VOSS Automate
Core Feature Guide

Release 25.3

December 03, 2025

Legal Information

- Copyright © 2025 VisionOSS Limited.
  All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20251203060110

Contents

1 What's New **1**
1.1 Core Feature Guide: Release 25.3 . . . 1

2 Introduction **7**
2.1 Overview . . . 7
2.2 Getting Started . . . 22

3 Quick Start Guides **96**
3.1 Customer Onboarding Quick Start Guide (Multiple Vendors) . . . 96
3.2 Microsoft Quick Start Guide for Automate . . . 107

4 Hierarchy Management **112**
4.1 Introduction to hierarchies . . . 112
4.2 Navigate the hierarchy . . . 116
4.3 View the Hierarchy . . . 118
4.4 Add a provider . . . 118
4.5 Resellers . . . 119
4.6 Customers . . . 121
4.7 Intermediate node . . . 128
4.8 Sites . . . 129
4.9 Site Defaults Doc templates . . . 133
4.10 Site defaults . . . 134
4.11 Delete a hierarchy . . . 147
4.12 Delete issues and purges . . . 148
4.13 Localization language . . . 150

5 Role Based Access **151**
5.1 Introduction to role-based access control . . . 151
5.2 Clone a role . . . 156
5.3 Delete unused roles . . . 156
5.4 Roles and Admins . . . 158
5.5 Role Configuration . . . 202
5.6 Privacy and Login Control . . . 308

6 App Integration and Detailed Settings **329**
6.1 Microsoft App Integration and Detailed Settings . . . 329
6.2 Webex App Integration and Detailed Settings . . . 412
6.3 Cisco UCM App Integration and Detailed Settings . . . 456
6.4 Cisco CUC App Integration and Detailed Settings . . . 815
6.5 Additional Apps - App Integration and Detailed Settings . . . 860
6.6 Data Sync Management - App Integration and Settings . . . 915
6.7 Dialplan Tools - App Integration and Detailed Settings . . . 959

7 Number Management **1023**
7.1 Introduction to number management in Automate . . . 1023
7.2 AudioCodes device number integration . . . 1025
7.3 Move number inventory instances . . . 1027
7.4 Number Inventory Management . . . 1028
7.5 E164 Numbers . . . 1066

8 Users & Services **1080**
8.1 Microsoft User Services . . . 1080
8.2 Webex User Services . . . 1138
8.3 Cisco User Services . . . 1147
8.4 Provisioning . . . 1259
8.5 Authentication . . . 1262
8.6 User Services . . . 1269
8.7 Sync & Purge Users . . . 1279
8.8 Self-provisioning . . . 1290
8.9 Move Users . . . 1293
8.10 Session Timeouts . . . 1303
8.11 User Accounts and Passwords . . . 1304
8.12 Self-service . . . 1308

9 Call Groups **1312**
9.1 Microsoft Call Groups . . . 1312
9.2 Webex Call Groups . . . 1333
9.3 Cisco Call Groups . . . 1334

10 Security Management **1349**
10.1 Microsoft Defender setup, sync and overbuild . . . 1349
10.2 Microsoft Defender for Office security management and policies . . . 1352
10.3 Microsoft Defender for Endpoint security management and policies . . . 1361

11 Insights Dashboards **1367**
11.1 Introduction to Microsoft Insights . . . 1367
11.2 Digital Experience Monitoring (DEM) Agent Installation . . . 1371

12 System Configuration **1378**
12.1 Customizations . . . 1378
12.2 System Monitoring . . . 1427
12.3 Email Setup . . . 1433
12.4 Customer Build Configuration . . . 1439
12.5 Preferences & Defaults . . . 1439
12.6 License Audit Setup . . . 1468
12.7 Entitlement Management . . . 1474

13 System Functions **1484**
13.1 Transaction Overview . . . 1484
13.2 Tools . . . 1485

14 Self-service Administration **1591**
14.1 Introduction to Self-service Administration . . . 1591
14.2 Self-service feature display policy . . . 1591
14.3 End User Access and Authentication . . . 1597
14.4 Themes and Branding . . . 1597
14.5 Self-service Login Banner . . . 1597
14.6 Personal Phones (Remote Destinations) . . . 1598

14.7 Dual Mode Phones - Mobile ID . . . 1598
14.8 Voicemail for Self-service . . . 1598
14.9 Links Page . . . 1598

15 Dashboard and Menu Reference **1599**
15.1 Introduction to the default reference menus and dashboards . . . 1599
15.2 Default menus . . . 1599
15.3 Default dashboards . . . 1620

16 Appendix: Glossary **1715**
16.1 Glossary . . . 1715

Index **1736**

1. What's New

1.1. Core Feature Guide: Release 25.3

- EKB-17419: Support contains filtering for drop down across entire data set. See: *Search in Automate*

  Added details for new "Contains" search and paginated scrolling in drop-downs.

- EKB-20180: Add the ability to navigate to related entities from dropdowns. See: *Guide to the Admin Portal user interface*

  Details added for ability to click a link at a drop-down to go to a related entity.

- EKB-20180: Add the ability to navigate to related entities from dropdowns. See: *Quick Add Groups*

  Details added for ability to click a link at a drop-down to go to a related entity.

- EKB-21907: Show "Licensed Applications" on License page. See: *Manage your Automate product license*

  Added details on the Licensed Applications list on the About page.

- EKB-22640: Model Instance Filter (MIF) for Teams user inconsistent. See: *Model instance filters*

  Added note clarifying post-filtering behavior when using "in" with UserPrincipalName and other CsOnlineUser filters during sync.

- EKB-22640: Model Instance Filter (MIF) for Teams user inconsistent. See: *Configure Automate for Microsoft services*

  Added note clarifying post-filtering behavior when using "in" with UserPrincipalName and other CsOnlineUser filters during sync.

- EKB-22640: Model Instance Filter (MIF) for Teams user inconsistent. See: *Microsoft tenant setup*

  Added note clarifying post-filtering behavior when using "in" with UserPrincipalName and other CsOnlineUser filters during sync.

- EKB-24170: Improve Action Search list details. See: *Use the Action search to navigate Automate*

  Updated Action search topic with improvements, specifically, matching of queries, and ability to sort, filter, and clear results.

- EKB-24268: Change External Breakout field to not required in Customer Dial Plan. See: *Customer HCS Dial Plan*

  Updated HCS Customer Dial Plan topic to make to note that *Default External Breakout Number* is now optional.

- EKB-24855: Support for scheduled dashboard data exports / delivery. See: *Manage dashboards and widgets*

Added details on the new dashboard export and scheduled export functionality.

- EKB-25420: Allow creation of Webex Workspaces for phones or conference devices. See: *Webex Workspaces*

  Updated "Add workspaces" to allow adding MPP phones or collaboration devices.

- EKB-25420: Allow creation of Webex Workspaces for phones or conference devices. See: *Webex Workspaces*

  Updated "Add workspaces" to allow adding MPP phones or collaboration devices.

- EKB-25422: Set default values for lineType and lineWeight when adding a line to a Webex device. See: *Webex devices*

  Added details on the default values applied when adding additional lines to a Webex-supported device.

- EKB-25422: Set default values for lineType and lineWeight when adding a line to a Webex device. See: *Webex devices*

  Added details on the default values applied when adding additional lines to a Webex-supported device.

- EKB-25437: Webex activation code cleanup fails. See: *Webex Workspaces*

  Added a note on enabling "Activation Code refresh" for Webex workspace on selected customers.

- EKB-25437: Webex activation code cleanup fails. See: *Webex Workspaces*

  Added a note on enabling "Activation Code refresh" for Webex workspace on selected customers.

- EKB-25699: Unreserve numbers does not clear Reservation Notes. See: *Number reservation*

  Docs updated for reservation notes field that is automatically cleared when unreserving a number.

- EKB-25719: Support for custom Reporter Resource fields. See: *Manage dashboards and widgets*

  Added notes on the custom creation of calculated fields for a reporter resource.

- EKB-25719: Support for custom Reporter Resource fields. See: *Introduction to Automate dashboards*

  Added notes on the custom creation of calculated fields for a reporter resource.

- EKB-25937: Enhance Number Inventory Audit to change numbers from Cooling or Reserved to Used status if they are used. See: *Number inventory audit*

  Updated topic Number inventory audit to include numbers in Cooling or Reserved status.

- EKB-25958: view/HcsDeleteSiteVIEW does not include option to delete data from Webex. See: *Delete a hierarchy*

  Updated hierarchy delete topic to add an option for the ability to delete data from Webex.

- EKB-26144: Enhance ModelFilterCriteria with hierarchy per criteria and overbuild usage. See: *Model filter criteria*

  Added details on the Model Filter Criteria for Overbuild setting to allow Target Hierarchy.

- EKB-26319: Cisco Device Mobility: IPv4 Subnet and IPv6 Subnet should not both be mandatory. See: *Device Mobility Info*

  Updated the Device Mobility Info topic for non-mandatory Ipv4 and Ipv6 fields.

- EKB-26335: Webex: Import of numbers does not work when Control Hub has "Webex Calling - Workspaces" license and not "Webex Calling - Professional". See: *Introduction to Cisco Webex App*

  Added details for macro that runs a dual check for two license types in syncs and provisioning workflows for Webex.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- EKB-26403: In a Chart widget, add min/max for yAxis. See: *Chart widgets*

  Added information on the min/max configuration for the chart widget y axis

- EKB-26436: "Next Available Line" should look local first, before looking up. See: *Manage number filters*

  "Use next available line" prioritizes numbers at the current site before checking higher levels of the hierarchy for available numbers.

- EKB-26436: "Next Available Line" should look local first, before looking up. See: *Onboard user (Cisco)*

  "Use next available line" prioritizes numbers at the current site before checking higher levels of the hierarchy for available numbers.

- EKB-26436: "Next Available Line" should look local first, before looking up. See: *Microsoft Quick User*

  "Use next available line" prioritizes numbers at the current site before checking higher levels of the hierarchy for available numbers.

- EKB-26436: "Next Available Line" should look local first, before looking up. See: *Cisco Quick User*

  "Use next available line" prioritizes numbers at the current site before checking higher levels of the hierarchy for available numbers.

- EKB-26436: "Next Available Line" should look local first, before looking up. See: *Webex Quick User*

  "Use next available line" prioritizes numbers at the current site before checking higher levels of the hierarchy for available numbers.

- EKB-26946: Adds a new permission, "Export Dashboard Data", to grant permissions to admins to export dashboard data. See: *Access profile permissions and operations*

  Added details on the Export Dashboard Data permission.

- VOSS-1464: System User Audit and cleanup process. See: *Settings*

  Added details on the new user audit feature

- VOSS-1507: Microsoft Defender for Office & Endpoint. See: *Microsoft tenant setup*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: Microsoft Defender for Office & Endpoint. See: *Microsoft Defender for Endpoint security management and policies*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: Microsoft Defender for Office & Endpoint. See: *Microsoft Defender for Office security management and policies*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: Microsoft Defender for Office & Endpoint. See: *Microsoft Defender setup, sync and overbuild*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: (EKB-24159: Create new Global settings for enabled services). See: *Global settings*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: (EKB-26263: Update Labels in Overbuild and Overbuild Overview to more accurately reflect the target models and add Defender models). See: *Model filter criteria*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- VOSS-1507: (EKB-26343: Add move support directly on data/ModelFilterCriteria). See: *Model filter criteria*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: (EKB-26263: Update Labels in Overbuild and Overbuild Overview to more accurately reflect the target models and add Defender models). See: *Overbuild for Cisco*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: (EKB-25879: Create an Overbuild tool for moving Defender device models). See: *Overbuild for Microsoft*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1507: (EKB-25879: Create an Overbuild tool for moving Defender device models). See: *Run overbuild*

  Added details on the new Microsoft Defender for Office & Endpoint functionality.

- VOSS-1536: Support for Webex Insights dashboards on VOSS Platform. See: *Webex Calls*

  Webex content updated for the new Webex Insights dashboards.

- VOSS-1536: Support for Webex Insights dashboards on VOSS Platform. See: *Webex Meeting Qualities*

  Webex content updated for the new Webex Insights dashboards.

- VOSS-1536: Support for Webex Insights dashboards on VOSS Platform. See: *Webex Meetings*

  Webex content updated for the new Webex Insights dashboards.

- VOSS-1537: Extend Wingman AI assistant capabilities. See: *Wingman*

  Added details on the new Wingman Enhancements.

- VOSS-1540: Support for Digital Experience dashboards on VOSS Platform. See: *Insights Assurance Arbitrators*

  Added details on the DEM dashboards available for Microsoft Insights

- VOSS-1540: Support for Digital Experience dashboards on VOSS Platform. See: *Introduction to Microsoft Insights*

  Added details on the DEM dashboards available for Microsoft Insights

- VOSS-1545: Configurable Microsoft Sync. See: *Datasync Builder*

  Added details for the vendor-agnostic Datasync Builder tool, templates, and profiles, which are also integrated with the MS tenant.

- VOSS-1545: Configurable Microsoft Sync. See: *Microsoft tenant setup*

  Added details for the vendor-agnostic Datasync Builder tool, templates, and profiles, which are also integrated with the MS tenant.

- VOSS-1545: Configurable Microsoft Sync. See: *Global settings*

  Added details for the vendor-agnostic Datasync Builder tool, templates, and profiles, which are also integrated with the MS tenant.

- VOSS-1545: Configurable Microsoft Sync. See: *Datasync builder templates*

  Added details for the vendor-agnostic Datasync Builder tool, templates, and profiles, which are also integrated with the MS tenant.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- VOSS-1545: Configurable Microsoft Sync. See: *Datasync profiles*

  Added details for the vendor-agnostic Datasync Builder tool, templates, and profiles, which are also integrated with the MS tenant.

- VOSS-1559: User based segmentation for Microsoft Teams call data. See: *Insights Assurance Arbitrators*

  Updated the docs for user hierarchy details now added to call records in Arbitrator and for syncs to push user hierarchies to Arbitrator call records.

- VOSS-1560: Microsoft Tenant App Registration Enhancements. See: *Datasync Builder*

  Changes when adding and editing a Microsoft tenant.

- VOSS-1560: Microsoft Tenant App Registration Enhancements. See: *Microsoft tenant setup*

  Changes when adding and editing a Microsoft tenant.

- VOSS-1560: Microsoft Tenant App Registration Enhancements. See: *Global settings*

  Changes when adding and editing a Microsoft tenant.

- VOSS-1560: Microsoft Tenant App Registration Enhancements. See: *Datasync builder templates*

  Changes when adding and editing a Microsoft tenant.

- VOSS-1560: Microsoft Tenant App Registration Enhancements. See: *Datasync profiles*

  Changes when adding and editing a Microsoft tenant.

- VOSS-1571: Finalize setup and experience of core framework for Insights only mode. See: *Role-based dashboards and menus*

  Updated role-based dashboards topic for the Insights Admin role.

- VOSS-1575: Role Management System Optimization. See: *Customers*

  Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the `data/Role` model.

- VOSS-1575: Role Management System Optimization. See: *Add a provider*

  Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the `data/Role` model.

- VOSS-1575: Role Management System Optimization. See: *Resellers*

  Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the `data/Role` model.

- VOSS-1575: Role Management System Optimization. See: *Sites*

  Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the `data/Role` model.

- VOSS-1575: Role Management System Optimization. See: *Introduction to role-based access control*

  Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the `data/Role` model.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- VOSS-1575: Role Management System Optimization. See: *Role Management*

  Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the `data/Role` model.

- VOSS-1590: Microsoft: Enhance update sync FTP/Move via Data Sync and Manual Move (Move User). See: *Global settings*

  Docs updated for flow through provisioning update sync for MS user moves, line configuration changes on MS move user and services, and global settings (FTP).

- VOSS-1590: Microsoft: Enhance update sync FTP/Move via Data Sync and Manual Move (Move User). See: *Flow through provisioning (FTP)*

  Docs updated for flow through provisioning update sync for MS user moves, line configuration changes on MS move user and services, and global settings (FTP).

- VOSS-1590: Microsoft: Enhance update sync FTP/Move via Data Sync and Manual Move (Move User). See: *Microsoft - Move user & services*

  Docs updated for flow through provisioning update sync for MS user moves, line configuration changes on MS move user and services, and global settings (FTP).

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Introduction

2.1. Overview

2.1.1. Welcome to Automate

Overview

Automate allows you to easily onboard customers and end users with collaboration services. The fulfillment procedures to achieve this objective may involve administrators at the provider, reseller, customer, and site levels of the hierarchy.

This guide provides information about provisioning Automate, including provisioning steps and interactions between Automate and the UC applications of vendors that Automate supports. This guide also describes user and subscriber management, including LDAP-related move and push operations.

This documentation includes several flowcharts to provide an overview of specific features and workflows for Automate. See the index (f) for a list of these flowcharts.

Related topics

- *Introduction to the default reference menus and dashboards*
- *Role-based dashboards and menus*

Multi vendor support

Automate supports provisioning and management of all unified communications (UC) applications, across multiple UC vendors (including Cisco, Microsoft, and Avaya), as single or multi vendor deployments:

Vendor	Solution
Microsoft	See *Introduction to Microsoft UC Integration* in the Core Feature Guide. Provides a single, integrated, synchronized interface for managing the existing Microsoft Teams collaboration service, through the web portal, bulk-loading, or the REST API. • Connects to adjacent service management platforms • Configurable deployment templates support automated business processes • Workflows for migrating users • End-to-end management of Microsoft Teams, UC and collaboration solutions • License management • Extends Microsoft Teams • Supports complementary systems and applications to work alongside Microsoft Teams, such as Cisco Call Recording or Contact Center.
Cisco	Provides for customized UC app management via the following capabilities: • Webex App management • Onboarding workflows • Cisco contact center support • Flow-through provisioning • Multiple MACD use cases and workflows • ServiceNow integration • Northbound notification • Generic drivers • Supports complementary systems and applications to work alongside Cisco UC apps
Avaya	Manage Avaya enterprise voice, extended into Microsoft Teams.

Related topics

- Multi vendor users in the Core Feature Guide
- Microsoft overview in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Accessibility

Automate supports Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. A full Voluntary Product Accessibility Template (VPAT) report is available from your account team.

To support accessibility, when using keyboard navigation, a black bar is enabled above the toolbar. When the cursor is in the URL box and the Tab key is pressed, this bar is displayed and has three menu items corresponding to three areas of the main user interface:

Home screen	From any form on the interface, return to the main user interface. This is equivalent to the Home button on the main toolbar, and can, for example be accessed by means of a screen reader shortcut.
Skip to content	On the main user interface, move the focus to the dashboard menu items. Press <Tab> to move the focus to the first dashboard link.
Skip to navigation	On the main user interface, move the focus to the menu bar. The first menu item receives focus.

The table provides examples of features in Automate that are assessed for accessibility to support users with disabilities, including those who require assistive technologies, such as users who are unable to use a mouse, or those who are visually impaired:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Title display in the browser	When choosing a menu option in the Admin Portal, the title displays in the browser to give screen reader users an overview of the page and to help them to move between open pages in their browser.
Buttons and images have alternative text	Buttons and images have accessible names and can be read by screen readers. For example, paginator buttons that allow a user to navigate to the first, next, previous, and last page on a form. The alternative text displays when the mouse pointer hovers over an image. Visually impaired users who are using screen readers can hear the alternative text read out. Users who have turned off images to speed up downloads or to save bandwidth can view the alternative text.
Heading elements appear in a sequentially-descending order	Headings are properly ordered and do not skip levels. This conveys the semantic structure of the page, making it easier to navigate and understand when using assistive technologies. For example, the Login page contains a level-one heading, and landmarks for the logo, input fields, and labels.
Elements meet minimum color contrast ratio thresholds and can be changed	Low-contrast text is difficult or impossible for many users to read. While some people need high contrast, for others, bright colors (high luminance) are not readable. A Chrome plugin can be installed (on the Chrome browser), which allows the user to change the default colors on a page.
Zoom capability	VOSS Automate supports zooming without losing any information or functionality.
Keyboard access and alternative visual focus	Many people cannot use a mouse and rely on the keyboard to interact with the Web. People who are blind and some sighted people with mobility impairments rely on the keyboard or on assistive technologies and strategies that rely on keyboard commands, such as voice input. In a browser that supports keyboard navigation with the Tab key (for example, Firefox, IE, Chrome, and Safari): 1. Click in the address bar, then put your mouse aside and do not use it. 2. Press the 'Tab' key to move through the elements on the page. 3. To move within elements such as select boxes or menu bars, press the arrow keys. 4. To select a specific item within an element such as a drop-down list, press the Enter key or Spacebar.
ARIA roles have allowable attributes	• Children of ARIA roles, such as form arrays, panel title bars, and tabs, are announced • Landmarks and IDs are unique • Table headers have text labels that are visible to screen readers • Interactive controls are not nested • Toggle fields have accessible names, for example, *Element: List checkbox*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Dynamic forms	• All buttons, including those used for pagination on dynamic forms, have discernible text labels that can be read by a screen reader • Links with the same name have a similar purpose to facilitate keyboard navigation and the use of screen readers
Breadcrumb navigation elements	Breadcrumbs have machine-readable labels to allow those using assistive technologies to understand the site structure, to facilitate navigation, and to provide context for their current location.
Pop-up dialogs	Form elements have accessible labels that properly identify the element, for example, a screen reader is able to announce a *Close* button as well as the header and content text on *Confirmation* dialogs and other messages, and on *Search* and *Hierarchy* pop-ups. Relationships between parent/child elements can be determined, for example, in the hierarchy tree.

Compatibility

Prior to install or upgrade, it is recommended that you review the latest Automate Compatibility Matrix for details on supported browsers and applications for your version.

Unicode limitations

Automate supports unicode characters only in the following fields:

- User Information
- Description
- Contact Information (Address, City, State, Postal Code, Country, Extended Name, External Customer ID, Account ID, and Deal IDs)
- Phone Label

Conventions used in this guide

Formatting conventions

The table describes formatting conventions in the Automate documentation:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Component	Formatting
UI buttons and labels	Uses the same capitalization as displayed in the user interface, formatted **bold**.
Dashboard, menu, and page names	Formatted **bold**
Asterisk '*' after field name, e.g. Userid *	Indicates that the field is mandatory.

Badges

Automate Help topics typically display one or more badges (below the topic title) to indicate that the Help content is relevant only to a specific deployment type (Enterprise or Provider), admin level (for example, Customer admin, HCS admin, or Provider admin), or vendor (for example, Microsoft or Cisco, hybrid or multi-vendor).

Note: Badges are typically used only for exceptions, that is, where functionality is available only for a specific deployment type, vendor type or vendor configuration, or where you must log in with a specific admin role.

Deployment badges

- provider

  Indicates that this functionality is only available in Provider deployments.

- enterprise

  Indicates that this functionality is only available in Enterprise deployments.

Vendor support badges

- Microsoft

  Indicates that this functionality is relevant for Microsoft.

- Cisco

  Indicates that this functionality is relevant for Cisco.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Vendor configuration badges

- hybrid

  Indicates that this functionality is relevant to hybrid vendor configuration.

- multi-vendor

  Indicates that this functionality is relevant to a multi vendor configuration.

Note: If no vendor configuration badge is used, assume single vendor, for example, Microsoft-only environment.

Admin role badges

Admin login roles are listed in order of highest access level to lowest access level. Provider and Enterprise admin are at the same level.

You can find more information about Automate roles and access levels in *Introduction to role-based access control*

- sys-admin

  Log in as sysadmin.

- hcs-admin

  Log in as HCS admin.

- reseller-admin

  Log in as Reseller admin.

- provider-admin

  Log in as Provider admin.

- enterprise-admin

  Log in as Enterprise admin.

- customer-admin

  Log in as Customer admin.

- site-admin

  Log in as Site admin

- self-service-admin

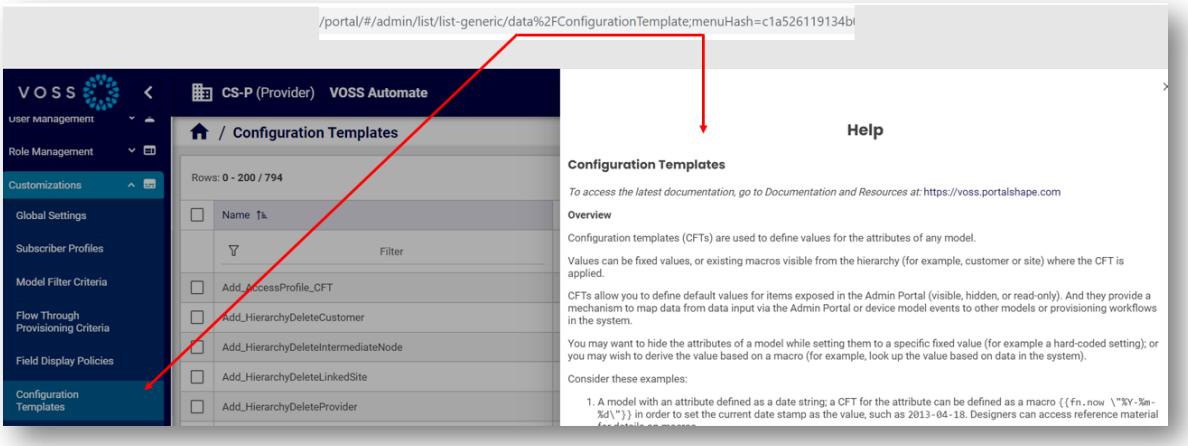
  Log in as Self-service admin

Copyright © 2025 VisionOSS Limited. All rights reserved.

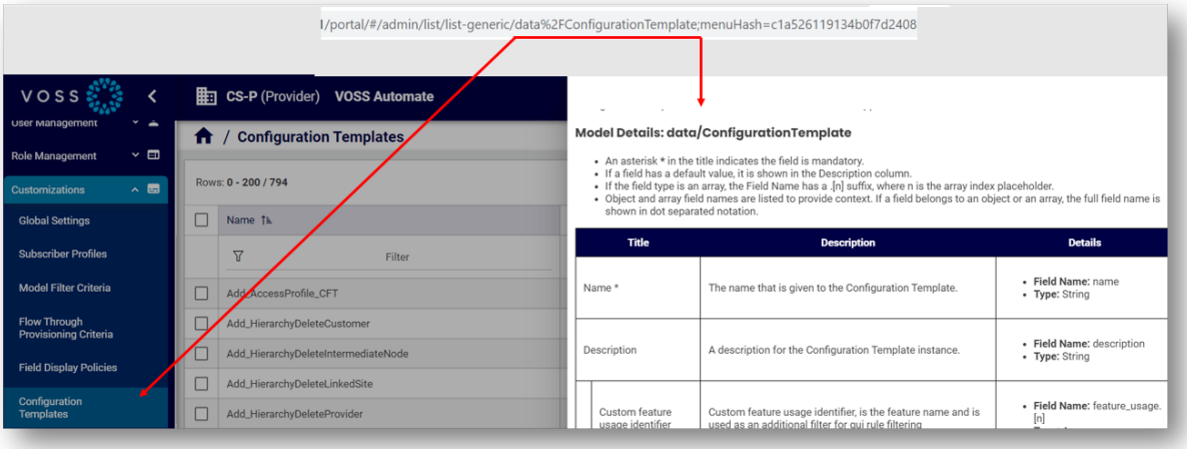
Context-sensitive Help files

The Automate Admin Portal ships with context-sensitive help files, which are associated with the relevant menu via the model type (visible in the URL).

The example shows the **Configuration Templates** page, the model type in the URL (*data/ConfigurationTemplate*), and the Help file topic title, *Configuration Templates*.



In addition to the help topic content, which may describe the feature, provide a task description, and additional details for the user interface, a default, auto-generated description is provided for the model. These model details may be further refined (filtered) via field display policies applied to the menu.



Where models are associated with two or more menus in the user interface, the help file may be a general topic for the model type, or the context of the help file that displays may relate only generally to the menu you're working with. In this case, it is recommended that you view the latest documentation for the menu or feature via the Documentation website via a link at the top of the context-sensitive help or via the *Documentation and Resources* tab at: https://voss.portalshape.com

For example, the `data/File` model is associated with the following menus:

- Audit Report Files
- File Management

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Manage Greeting Files
- MS-Teams MP3 Files
- MS-Teams WAV Files

2.1.2. Manage your Automate product license

Tip: *Use the Action search to navigate Automate*

Overview

This topic covers the licensing of the Automate software product. License enforcement is enabled on all Automate deployments, including production and lab environments.

Starting with Automate 21.4, a 7-day temporary license is issued for new installs or upgrades to allow administrators to carry out the required licensing. You must replace the temporary license with your new license token (license key) within 7 days from install or upgrade.

Important: You won't be able to log in to the system once the temporary license expires.

Each Automate deployment ships with a unique Deployment or Platform ID. The Platform ID is required to generate a license token. A license token is only valid for a deployment with the related Platform ID.

Licensing workflow

sys-admin

1. Obtain the license tokens (JSON Web Tokens) from VOSS. These tokens are used to license your product.
2. Choose a licensing method:
   a. Log in to Automate as `sysadmin` user.
   b. Go to the **Manage License** page in the GUI. Follow the steps described in *Add a license on Automate via the GUI*.

      Note: This method is *not* available for license renewal when the existing license token has already expired.

   c. From the system Command License Interface (CLI), as platform user:

      To update a license token from the system CLI, the following commands are available:

      - `license add token [<token string>]`
      - `license add file <token_file>`

      Follow the steps in the Product Licensing topic in the Platform Guide. Follow this method for expired license renewal.
3. When your license expires, follow the steps for your license type to renew it.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a license on Automate via the GUI

sys-admin

This procedure adds a new license token (license key) on Automate, via the GUI.

Note: You can also add a license via the CLI. See the Platform Guide.

1. Obtain your license token from VOSS.
2. Log in as the system administrator user (`sysadmin`), then go to **Manage License**.

   Note: You won't be able to log in to the system once your license expires. It is recommended that you renew and apply your license prior to the expiry date.

3. Review the **Manage License** form details. The table describes the fields on this form:

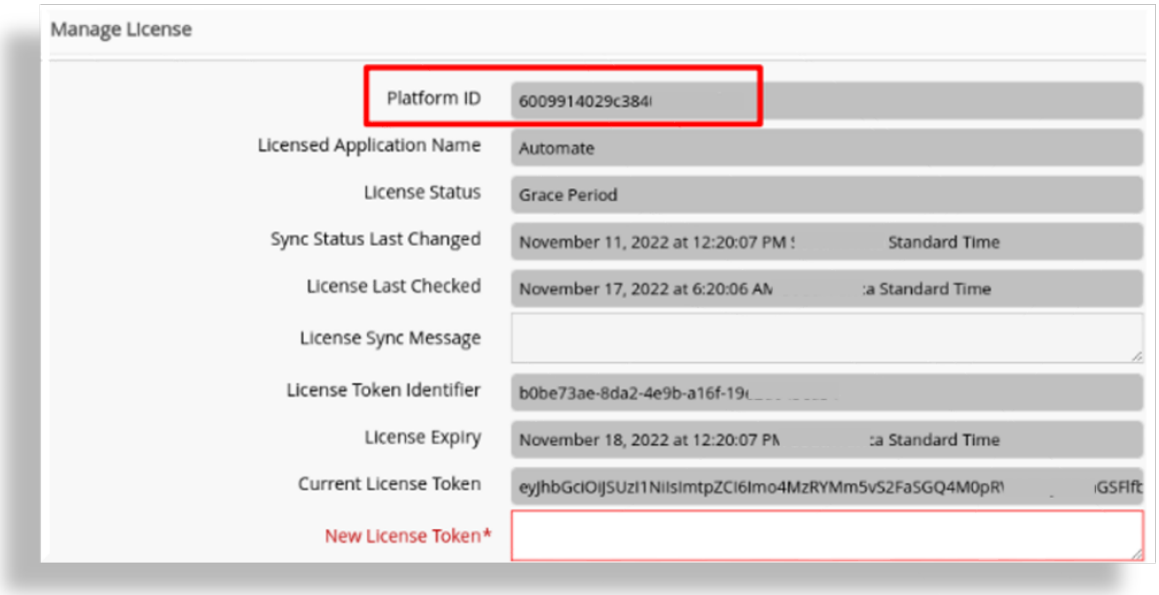
   Note: Date format of `<date-time>` is localized to the browser locale.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Platform ID	<platform ID> - The ID to submit when renewing a license.
Licensed Application Name	The name of your application, for example, “Automate”.
License Status	The status of your license. On install or upgrade, a 7-day temporary license is provided. It is important that you apply your new license before the expiry date. When a valid license exists, and is outside of the expiry alert period, the status is *Licensed*.
Sync Status Last Changed	<date-time>
License Last Checked	<date-time> - The last time the license was checked. Refer to the Product Licensing topic in the Platform Guide for details on the use of the `voss check-license` command, which is used to check your license with VOSS.
License Sync Message	The status messages of communication with the License service.
License Token Identifier	<token ID> - Used by VOSS Support.
License Expiry	<date-time>
Current License Token	The <token string> for your current license (the license that will expire or is due to expire).
New License Token	The <token string> for the new license that you obtain from VOSS. Once you paste the new license token into this field and save, it overwrites your current (expired) license.
Licensed Applications	The list of applications are shown, matching licensed application modes, for example: • Automate Collaboration • Insights Netflow • Insights Collaboration Assurance • Insights Collaboration Analytics For details on the available application modes, contact VOSS. The available licensed applications also enable related data sources that are available to dashboard widgets. For details, refer to the topic on License modes and data sources in the guide.

4. At the **New License Token** field, paste your new license token (the license token obtained from VOSS).

Copyright © 2025 VisionOSS Limited. All rights reserved.



5. Click **Save** to apply your new license token.

License expiry alert notifications

Automate sends alerts to Provider administrators in the Automate Admin Portal to notify these users that the system license will expire. The alert type depends on the number of days before the license expires:

Alert type	When sent?
Info	120 days prior to license expiry
Info	90 days prior to license expiry
Warning	60 days prior to license expiry
Warning	30 days prior to license expiry
Warning	Daily, from two weeks prior to license expiry

View your product license status

This section describes the ways in which you can access and view the status of your product license.

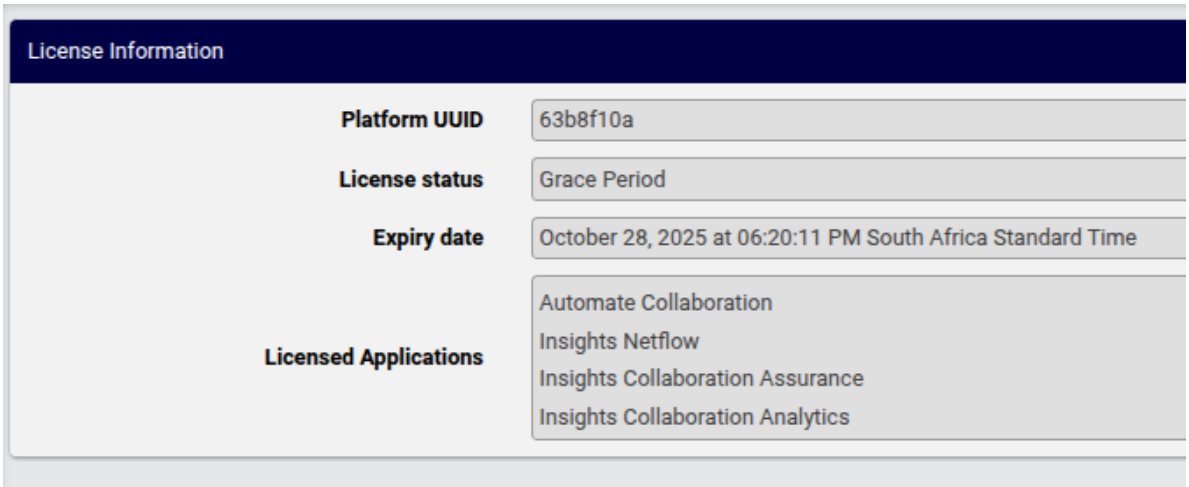
View your product license in the Automate GUI

You can access and view your product license in the Automate GUI via the About menu, Login screen, via alerts sent from the system, via the Licensing menu, and via the Dashboard link (as `sysadmin` user):

- About menu

  On the **License** sub-menu, the **License Information** is displayed, as show in the example below:

Copyright © 2025 VisionOSS Limited. All rights reserved.



- Login screen

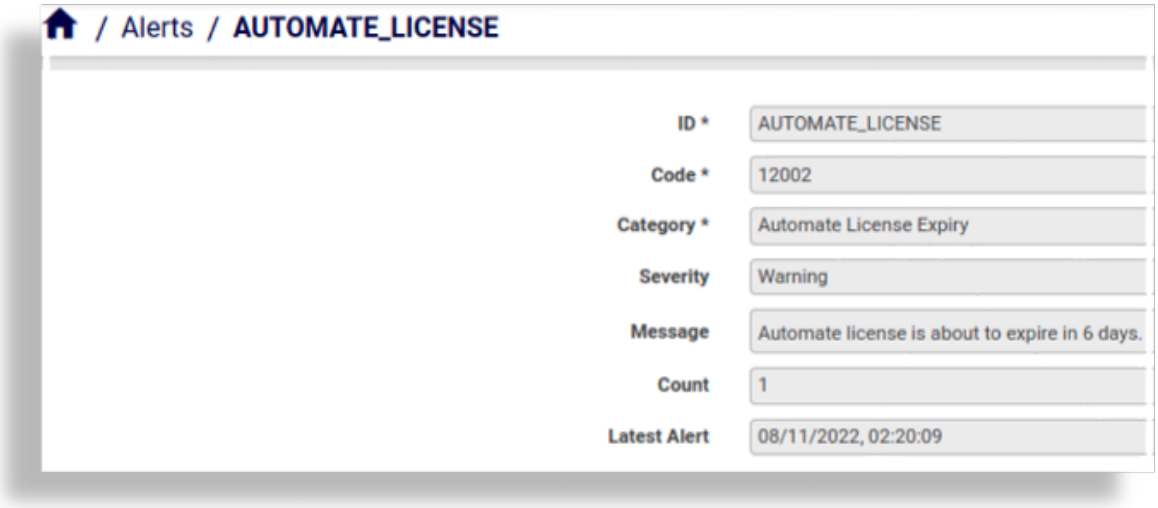
  You won't be able to log in to the system and access the Admin Portal GUI once your license expires. It is recommended that you renew and apply your new license before the expiry date. Your system administrator may log in via the CLI to update the license. Once the new license is applied, log in via the GUI is re-enabled. See the *Product Licensing* topic in the Platform Guide.

- Alerts

  When logging in during the license expiry notification period (up to 120 days prior to license expiry), Provider admins (and above) are shown license expiry notices.

  Once logged in, Provider admins (and above) can view pending license expiry notices via the toolbar Notifications icon. These alerts are also posted via the Notifications icon when Automate is unable to communicate with the license service.

  Alerts are generated if a license is within 120 days of expiry. The image shows an example of a license expiry warning:



  Example of license service error message:

```
"alert_id": "AUTOMATE_LICENSE",
"alert_severity": "ERROR",
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
"alert_category": "Automate License Service Error",
"alert_message": "Automate License Service communication error since <date-time>"
```

Note:

- Alerts can also be configured to send email messages - see the `notify` command in the Platform Guide.
- SNMP traps are also generated - see the License section under Notification Messages in the Platform Guide.

- Menu for `sysadmin` user

  The `sysadmin` user can view license expiry details via the **Manage License** page.

- Dashboard link for `sysadmin` user

  The `sysadmin` user can view license expiry details via the **Manage License** link on their Dashboard.

View your product license in the platform CLI

You can access your product license details via the Automate platform CLI:

- Login display, health display - only on unified nodes in a *unified node* topology and application nodes in a *modular cluster* topology.
- Use CLI command `license token list`, and view the output of this command. See further details in the Product Licensing topic in the Platform Guide.

Renew a license

You won't be able to log in to the system via the Admin Portal GUI once your license expires. It is recommended that you renew and apply your license before the current license expires.

Your system administrator will need to contact VOSS to renew the license. Provide the platform ID which is shown on the **Manage License** form.

2.1.3. Log in

Overview

Starting with Automate 24.1, "classic" admin portal view of the Automate GUI has been deprecated. On install or upgrade, the default view of the portal is set to the newer `admin` portal.

You can use the following URLs to log in:

- `https://{hostname}/`
- `https://{hostname}/portal/`

Important:

- The trailing forward slash `/` is required in the URL after `portal/`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Support is available for additional paths in the URL, for example, for use in a proxy path. The supported format is as follows: `https://{hostname}/{some}/{custom}/{path}/portal/`
- Users with a business admin role can use the URL, `https://{hostname}/business-admin/`, but this will *always* redirect to `https://{hostname}/portal/`.

Related Topics

- *Guide to the Admin Portal user interface*
- *Change your own password*

Log in for Standard Users

To log in as a standard user:

1. Go to either of:
   - `https://{hostname}/login`
   - `https://{hostname}/portal/login`
2. Enter your username, using either of these formats:
   - `{username}@hierarchy`
   - `{email address}`
   - `{username}`

Important: If logging in with just `{username}`, your username must be unique at the hierarchy level, else login fails. In this case, log in using either `{username}@hierarchy` or `{email address}`. Email address must be unique in the system.

Log in for LDAP Users

To log in as an LDAP user:

1. Go to either of:
   - `https://{hostname}/login`
   - `https://{hostname}/portal/login`
2. Log in, using either user ID (`{user ID}[@hierarchy]`), or your email address.
   - User ID (`{user ID}`) corresponds to the username mapping in User Field Mapping, for example, email address, user principal name, sAMaccountName. The login attribute name is configured in the authentication attribute of the LDAP device associated with the hierarchy. The authentication attribute value is obtained from the User Field Mapping, and is used to authenticate against LDAP. See *User field mapping*
   - `@hierarchy` is not required when the user ID corresponds to the user's email address (regardless of the login attribute name specified in the LDAP network connection). The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. Hierarchy level is the level at which the user is created.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Log in for SSO Users

To log in as SSO user:

1. Go to either of:
   - `https://{host name}/sso/{SSO login URI}/login`
   - `https://{hostname}/portal/sso/{SSO login URI}/login`
2. Log in using the relevant SSO identity provider credentials.

   The SSO URLs provided redirect to the Admin portal with endpoint: `/portal/`.

Related Topics

- SSO Users and Login in the Core Feature Guide
- LDAP Users and Login in the Core Feature Guide

2.2. Getting Started

2.2.1. Role-based dashboards and menus

Overview

New installs of Automate ship with a collection of pre-defined, default roles and associated elements to deliver a set of experience-based layouts for the Automate user interface:

- *Automate - Admin role*
- *Automate - Service Desk role*
- *Automate - Analyst role*
- *Automate - Self Service role*
- *Microsoft-only roles*
- *Insights - Admin role*

Automate also ships with these additional, special-purpose roles:

- **HcsAdmin** - This role is defined for the user who logs in on first install to create a provider admin, and optionally, to create admin users for the other hierarchies (customer, site, reseller) out of the cloned default roles created when adding a provider. Alternatively, the newly created provider admin user can now log in to create the other admin users out of the cloned roles at the provider level, and can hand over further configuration of each hierarchy to the relevant admin users, or configure Automate for all hierarchies.
- **selfservice** - Visible only to `sys` (System) administrators. This is the default *system resource* role for Self Service. Since critical data sync workflows and configuration templates make use of this system level role for provisioning new or updated users, do **not** modify or remove this role.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default roles

Each of the shipped, experience-based roles is assigned a GUI layout, comprising a Home dashboard (landing page), and a set of predefined dashboards and menus offering access to features designed for their user experience. The role-based layouts follow best practices and serve as a starting point for common personas. While they offer a strong foundation, you should customize them to fit your needs - for example, you'll be able to adjust actions and fields exposed via field display policies, customize naming conventions, and modify help text and descriptions to align with your user base. This ensures an optimized experience, reduces adoption challenges, and minimizes training requirements. Contact your account manager if you need guidance towards developing an operationally sustainable approach.

Roles are combined with a number of elements (such as permissions, menus, dashboards, access profiles, and themes) to define the look and feel of the system for particular user experiences. The `hcsadmin` user can clone and customize the pre-built layouts to create custom layouts.

Note: Some menus and pages have been renamed in 25.1. It is recommended that you use the toolbar *Search* functionality to search for models, functionality, and other entities so that you won't need to remember any particular menu paths. For example, to search for page by its name, use the *Action* search. Refer to *Use the Action search to navigate Automate*. For details on all the *Global* and *Filter* search, refer to *Search in Automate*

Hierarchy considerations

Automate's default roles can typically be assigned to users at any level in the hierarchy to pair the role capabilities with a given scope. For example, a specific customer in a Provider environment, or specific sub-unit in a business for Enterprise.

Dashboards may need to be adjusted to reflect the appropriate hierarchy level. For example, change group from Customer, which is useful for Provider, to perhaps, by Site.

GUI layouts in earlier versions of Automate

Earlier versions of Automate (pre-25.1) shipped with three sets of pre-built menus:

- Default menu layouts
- Best practice menus (enhanced menus)
- Menu layouts for a Business Admin role

Important: If you're upgrading to Automate 25.1 from an earlier version, your GUI layout remains unchanged unless you choose to configure your role and access profiles to switch to the new GUI layouts.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Automate - Admin role*
- *Automate - Service Desk role*
- *Automate - Analyst role*
- *Introduction to role-based access control*
- *Introduction to access profiles*
- *Menu layouts*
- *Introduction to Automate dashboards*
- *Use the Action search to navigate Automate*
- *Introduction to hierarchies*
- *Menu diff tool*
- For the full list of reference dashboards, see *Introduction to the default reference menus and dashboards*

Automate - Admin role

The *Automate - Admin* role is an experience designed for application administrators. This role provides broad access to setup, settings, and system actions. It serves as a model for advanced admins and offers insight into overall functionality.

Automate - Admin: Home dashboard

The **Automate - Admin** role's Home dashboard is *Automate - Admin Home*, which displays a selection of counters, quick actions, and charts curated for the role.

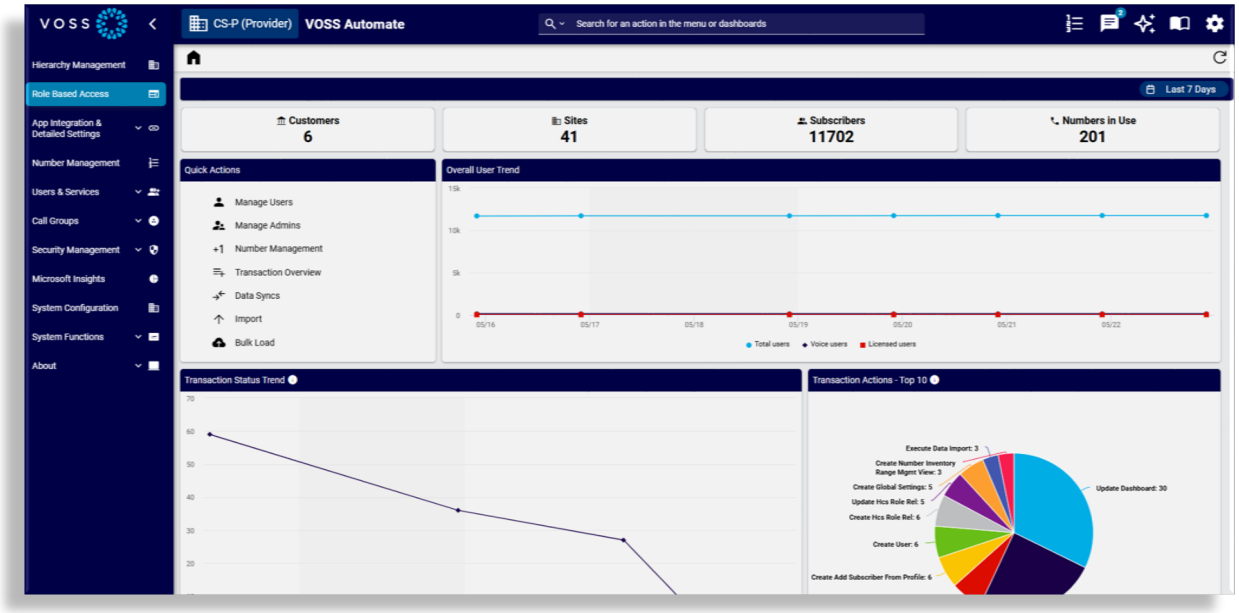
1. Menu layout
2. Counters
3. Quick Actions
4. Charts

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate - Admin GUI layout

By default, the *Automate - Admin* role is assigned a theme, a Home dashboard, a menu layout, and an access profile, and is available for a selection of hierarchies:

- Theme: *default*
- Home dashboard: Automate Admin Home
- Menu layout: *Automate - Admin*
- Access profile: *Automate - Admin*
- Hierarchies: Provider, Reseller, Customer, Hcs, Intermediate



Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate - Admin menus and dashboards

The Automate - Admin experience comprises a Home dashboard, menus, and a collection of experience-based, role-focused dashboards. To view the menu layout for this role, refer to:

- Menu: Automate - Admin in the Core Feature Guide

Related topics

- *Setting the default theme*
- *Introduction to access profiles*
- *Menu layouts*

Automate - Service Desk role

The *Automate - Service Desk* role is an experience tailored for users performing typical, day to day system operations, including set up and configuration, and requiring access to data for troubleshooting and other operational tasks. This role is suitable for help desk/service desk users, delegated administrators in Provider environments, or business sub-units in enterprises.

Automate - Service Desk: Home dashboard

The *Automate - Service Desk* role's Home dashboard is *Automate - Admin Home*, which displays a selection of counters, quick actions, and charts curated for the role.

1. Menu layout
2. Counters
3. Quick Actions
4. Charts

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate - Service Desk GUI layout

By default, the *Automate - Service Desk* role is assigned a theme, a Home dashboard, a menu layout, and an access profile, and is available for a selection of hierarchies:

- Theme: *default*
- Home dashboard: *Automate - Admin Home*
- Menu layout: *Automate - Service Desk*
- Access profile: *Automate - Service Desk*
- Hierarchies: Provider, Reseller, Customer, Hcs, Intermediate, Site

Automate - Service Desk menus and dashboards

The *Automate - Service Desk* experience comprises a Home dashboard, menus, and a collection of experience-based, role-focused dashboards. To view the menu layout for this role, refer to:

- Menu: Automate - Service Desk in the Core Feature Guide

Related topics

- *Setting the default theme*
- *Introduction to access profiles*
- *Menu layouts*
- *Introduction to Automate dashboards*

Automate - Analyst role

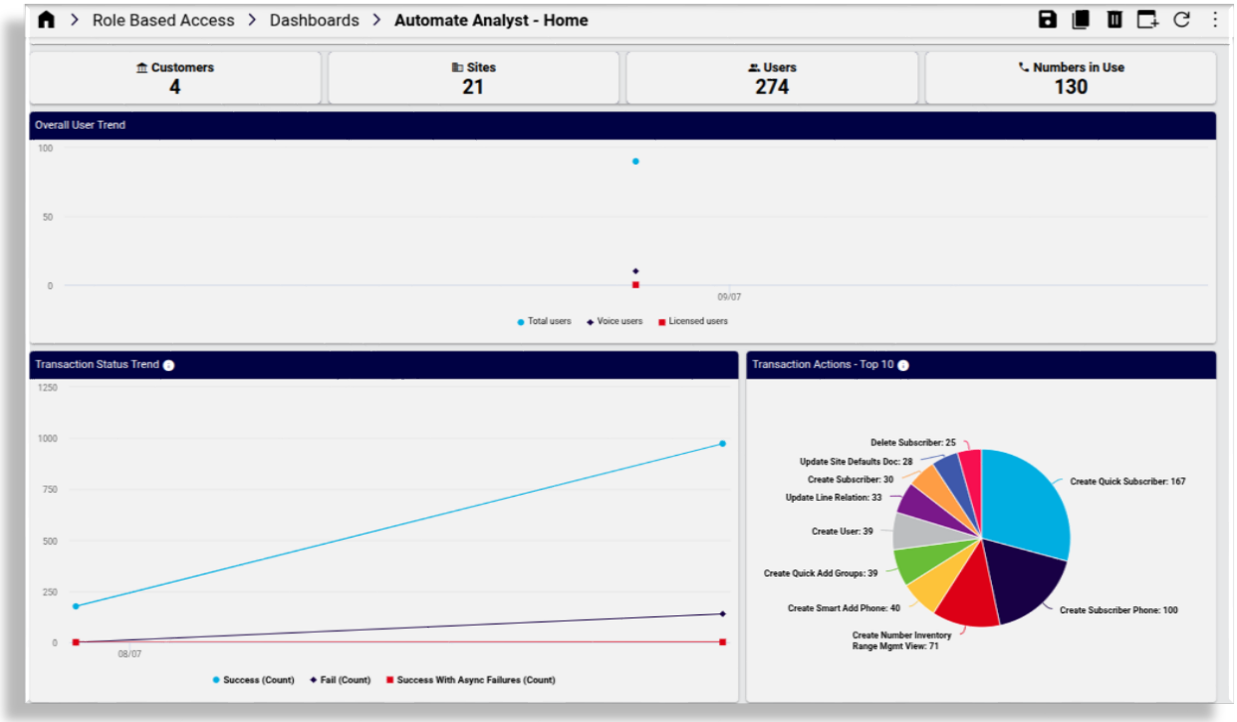
The *Automate - Analyst* role is an experience intended for users who need system visibility without making changes. It enables access to data for consuming dashboards, for performing searches, and for completing other analytical tasks, and is designed for stakeholders that need visibility of key metrics and information while offering more dynamic insights than traditionally static reports.

Automate - Analyst: Home dashboard

The Automate - Analyst role's Home dashboard is Automate - Analyst Home, which displays a selection of counters, quick actions, and charts curated for the role.

- Menu layout
- Counters
- Charts

Copyright © 2025 VisionOSS Limited. All rights reserved.



Automate - Analyst GUI layout

The default GUI layout for the *Automate - Analyst* role is assigned the following:

- Theme: *default*
- Home dashboard: Automate Analyst - Home
- Menu layout: *Automate - Analyst*
- Access profile: *Automate - Analyst*
- Hierarchies: Provider, Reseller, Customer, Intermediate, Site

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate - Analyst menus and dashboards

The *Automate - Analyst* experience comprises a Home dashboard, menus, and a collection of experience-based, role-focused dashboards. To view details for this menu layout, refer to:

- Menu: Automate - Analyst in the Core Feature Guide

Related topics

- *Setting the default theme*
- *Introduction to access profiles*
- *Menu layouts*

Microsoft-only roles

Microsoft-only roles ship with Automate, and while they're based on Automate's default, experience-based roles (including the *Automate - License Manager* role) these roles aren't enabled or assigned by default and are intended only as working examples for Microsoft-only deployments:

- *Automate - Admin - Microsoft Only*
- *Automate - Service Desk - Microsoft Only*
- *Automate - License Manager*

You can use Automate's customization tools to further refine these dashboards so that they are optimized for use cases in your organization:

- *Manage themes*
- *Menu layouts*
- *Introduction to Automate dashboards*
- *Introduction to access profiles*

Automate - Admin - Microsoft Only

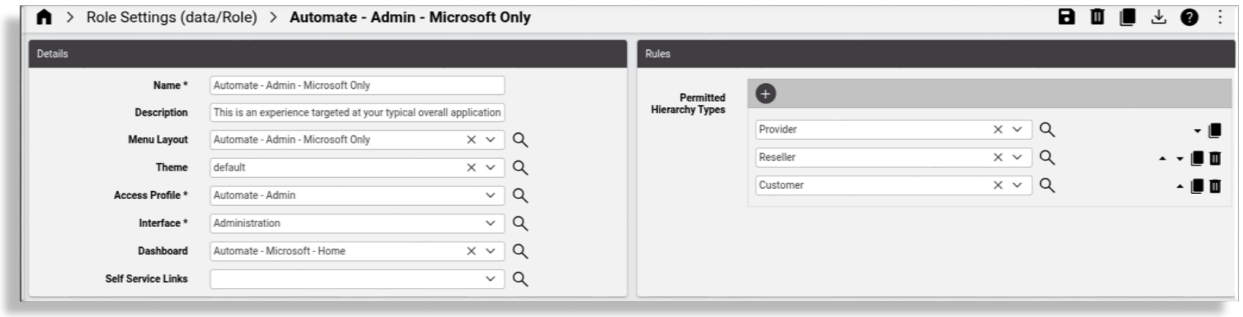
The *Automate - Admin - Microsoft Only* role ships with menus and dashboards customized for a Microsoft-only environment:

- Menu layout: Automate - Admin - Microsoft Only
- Theme: default
- Access profile: Automate - Admin
- Home dashboard: Automate - Microsoft - Home
- Permitted hierarchy types: Provider, reseller, customer

Copyright © 2025 VisionOSS Limited. All rights reserved.

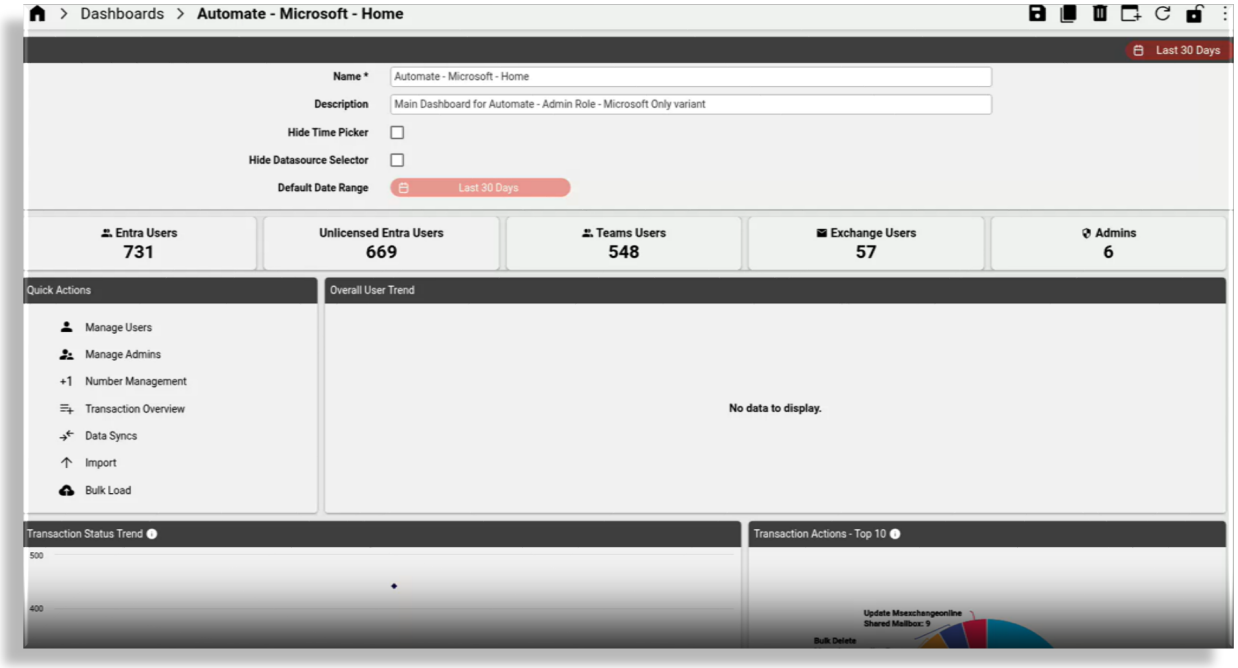
Role settings: Automate - Admin - Microsoft Only

The image displays the settings for the *Automate - Admin - Microsoft Only* role:



Home dashboard: Automate - Admin - Microsoft Only

The image displays the Home dashboard for the *Automate - Microsoft Only* role:

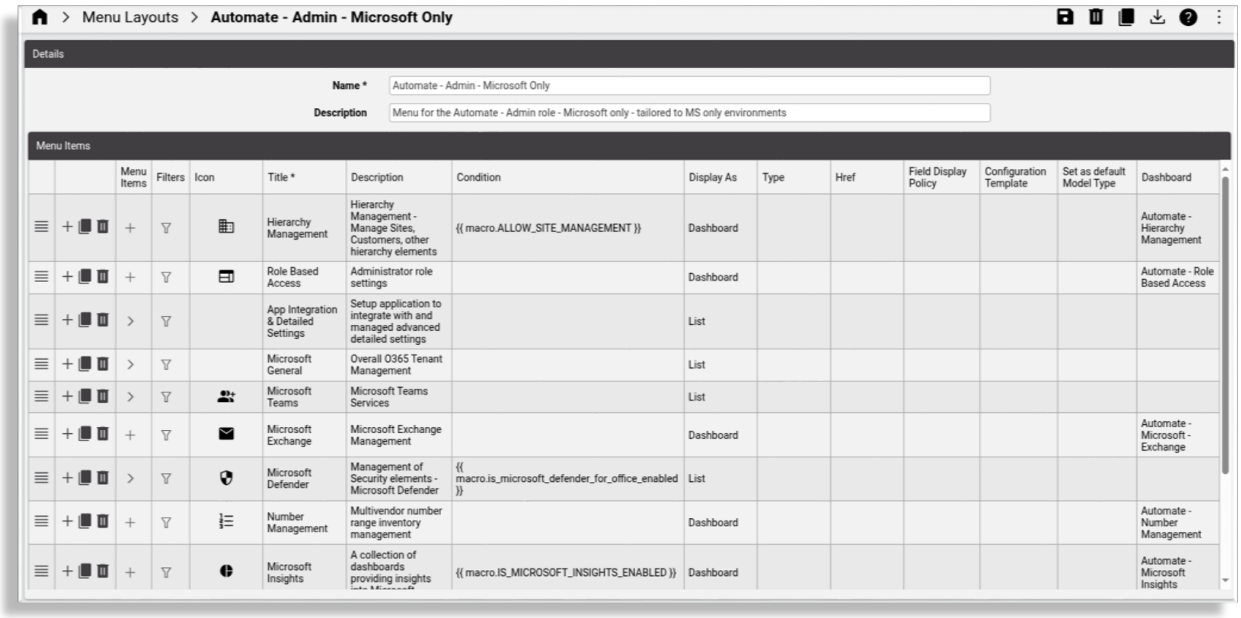


Menu layout: Automate - Admin - Microsoft Only

The image displays the menu layout settings for the *Automate - Admin - Microsoft Only* role. To view details for the menu layout, see:

- Menu: Automate - Admin - Microsoft Only in the Core Feature Guide

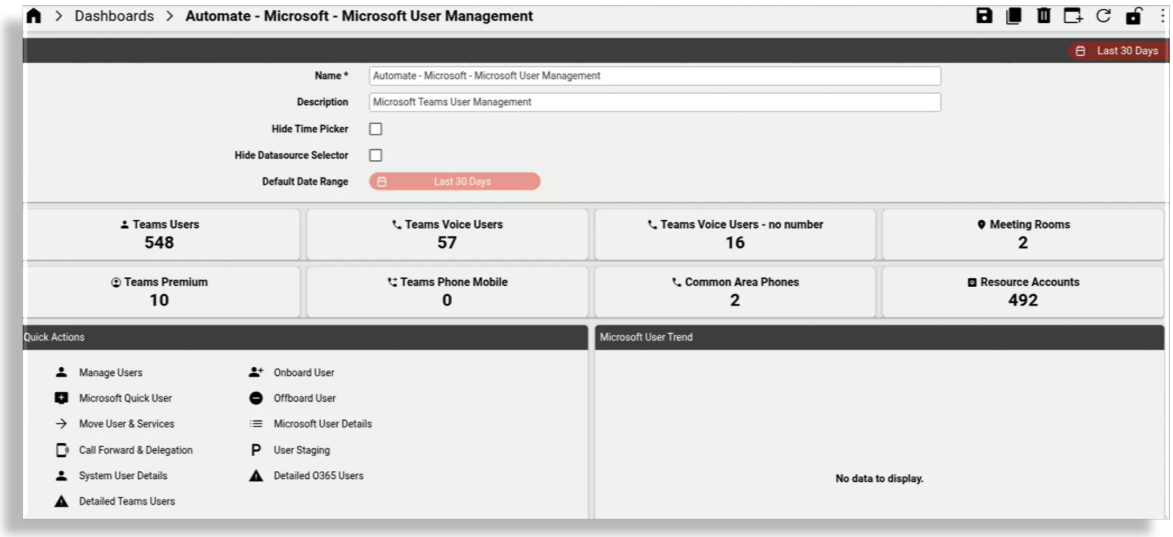
Copyright © 2025 VisionOSS Limited. All rights reserved.



Dashboards: Automate - Admin - Microsoft Only

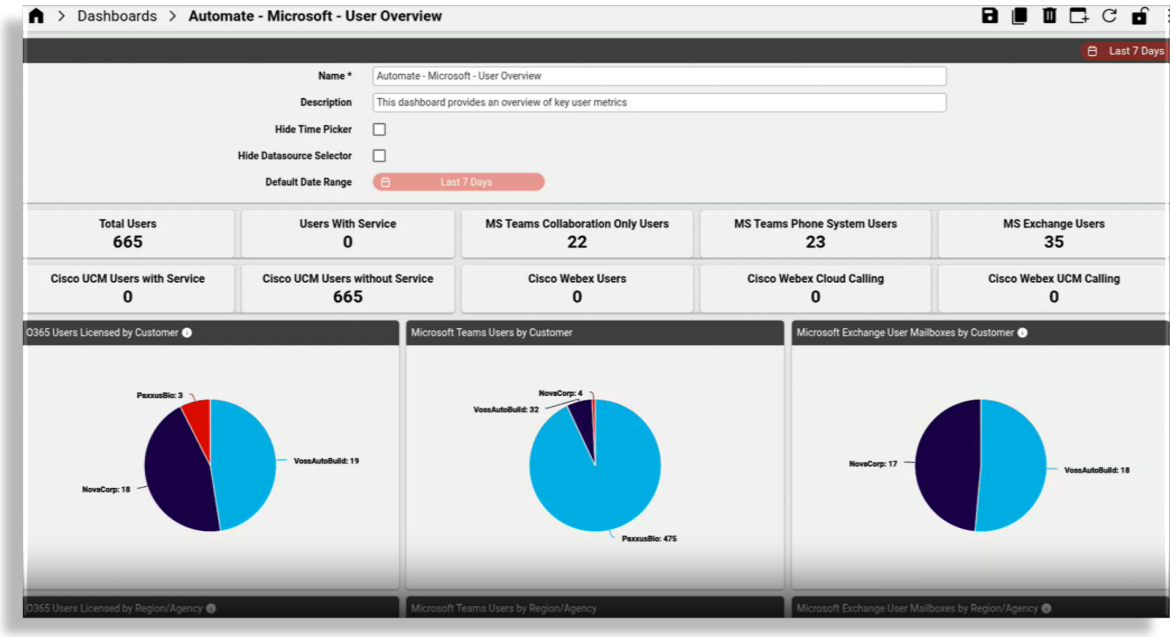
This section provides some examples of the dashboards that ship with the *Automate - Admin - Microsoft Only* role.

- The image displays the Microsoft-only *Microsoft User Management* dashboard that ships with Automate:

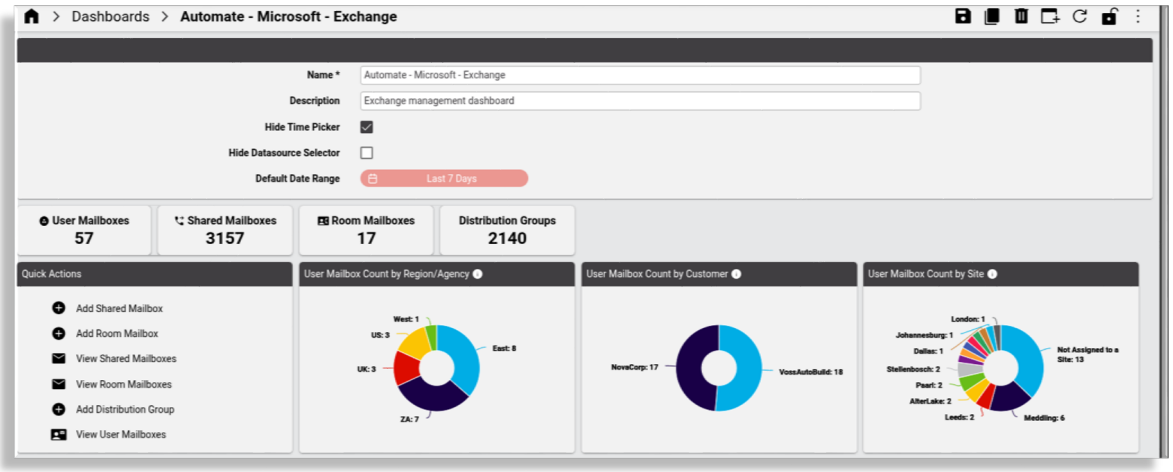


- The image displays the Microsoft-only *Microsoft User Overview* dashboard that ships with Automate:

Copyright © 2025 VisionOSS Limited. All rights reserved.



- The image displays the Microsoft-only *Microsoft Exchange* dashboard that ships with Automate:



Automate - Service Desk - Microsoft Only

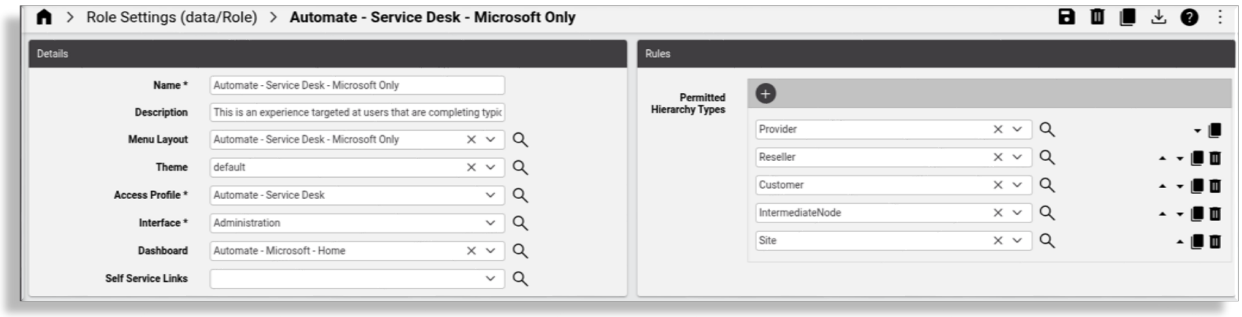
The *Automate - Service Desk - Microsoft Only* role ships with menus and dashboards customized for a Microsoft-only environment:

- Menu layout: Automate - Service Desk - Microsoft Only
- Theme: default
- Access profile: Automate - Service Desk
- Home dashboard: Automate - Microsoft - Home
- Permitted hierarchy types: Provider, reseller, customer, intermediate node, site

Copyright © 2025 VisionOSS Limited. All rights reserved.

Role settings: Automate - Service Desk - Microsoft Only

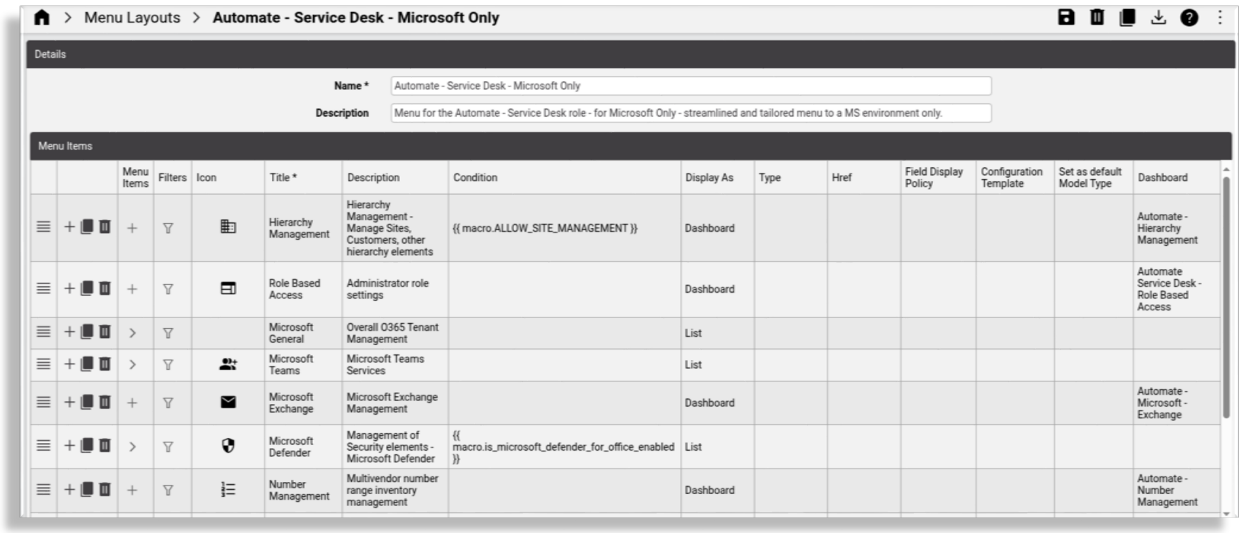
The image displays the settings for the *Automate - Service Desk - Microsoft Only* role:



Menu layout: Automate - Service Desk - Microsoft Only

The image displays the menu layout settings for the *Automate - Service Desk - Microsoft Only* role. To view details for this menu layout, see:

- Menu: Automate - Service Desk - Microsoft Only in the Core Feature Guide



Automate - License Manager

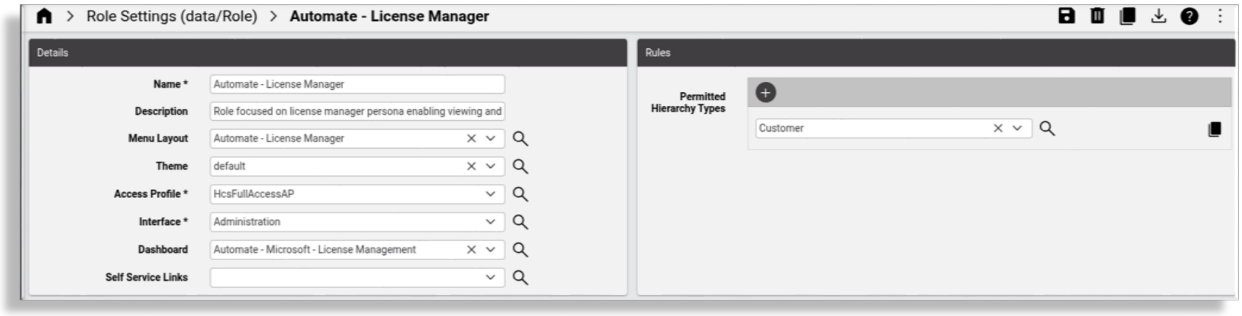
The *Automate - License Manager* role ships with menus and dashboards focusing on managing licenses and allocations for a license manager persona in a Microsoft-only environment:

- Menu layout: Automate - License Manager
- Theme: default
- Access profile: HcsFullAccessAP
- Home dashboard: Automate - Microsoft - License Management
- Permitted hierarchy types: Customer

Copyright © 2025 VisionOSS Limited. All rights reserved.

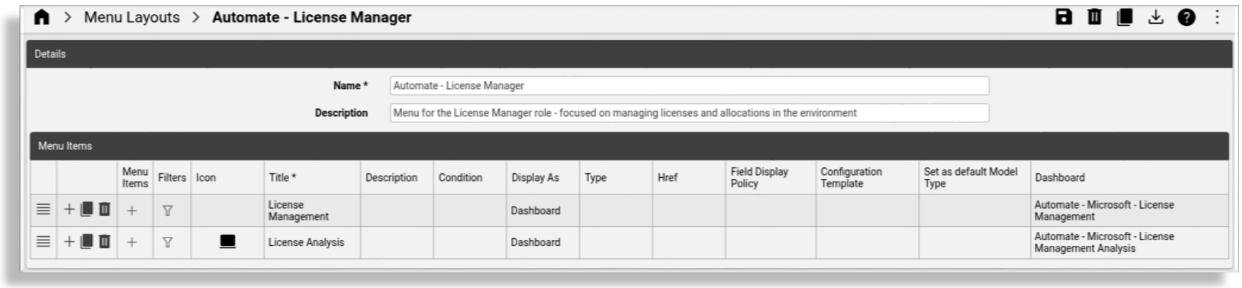
Role settings: Automate - License Manager

The image displays the settings for the *Automate - License Manager* role:



Menu layout: Automate - License Manager

The image displays the menu layout settings for the *Automate - License Manager* role.



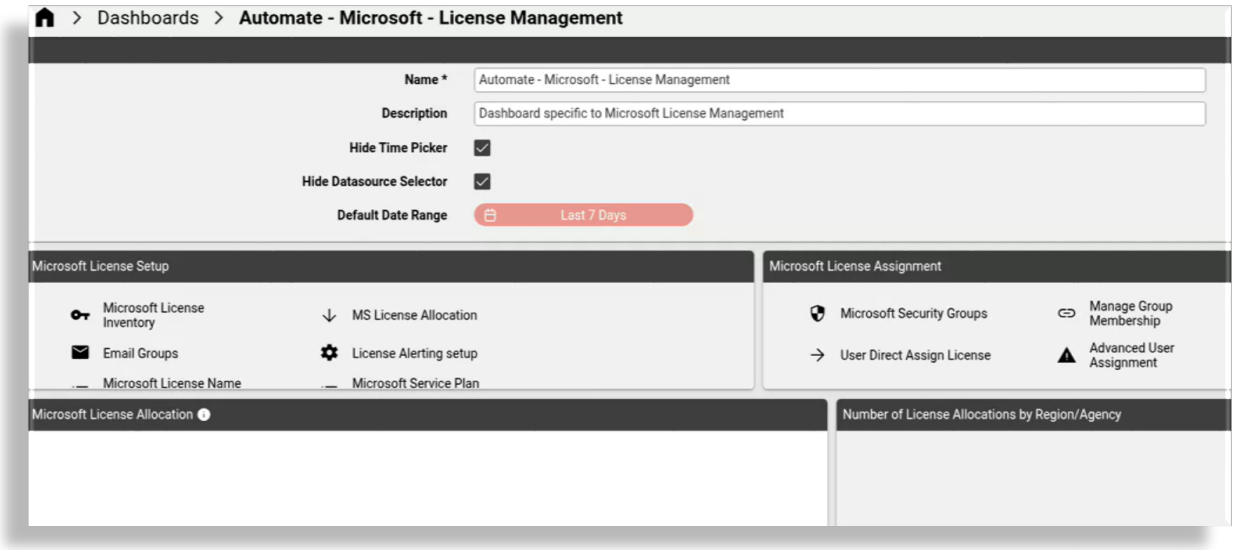
Dashboards: Automate - License Manager

The *Automate - License Manager* role ships with a menu with two pre-defined dashboards:

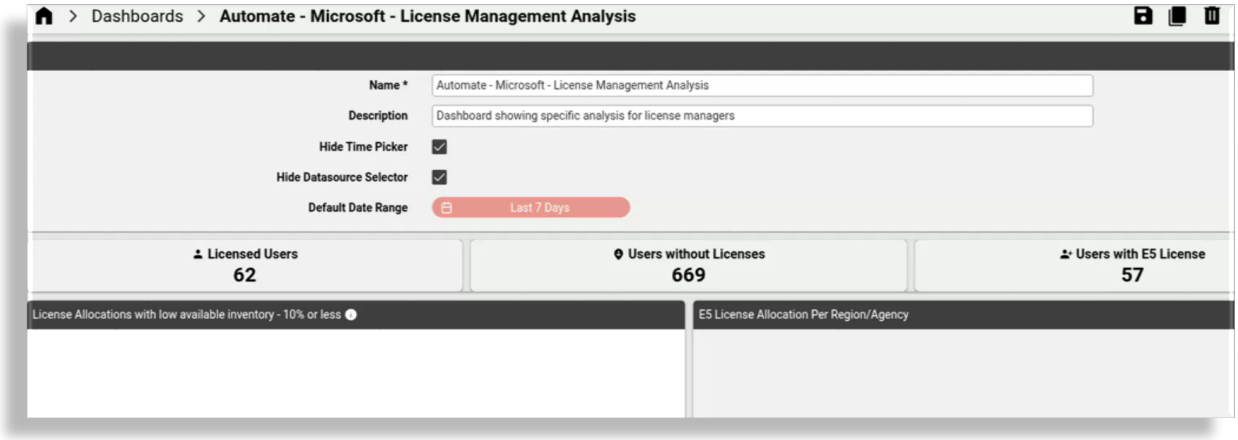
- Automate - License Manager: A menu providing access to two dashboards for managing licenses and license allocation in the environment:
  - License Management - a dashboard for managing licenses
  - License Analysis - a dashboard for analyzing licenses in your environment

The image displays the Microsoft-only *License Management* dashboard that ships with Automate:

Copyright © 2025 VisionOSS Limited. All rights reserved.



The image displays the Microsoft-only *License Analysis* dashboard that ships with Automate:



Automate - License Manager menus and dashboards

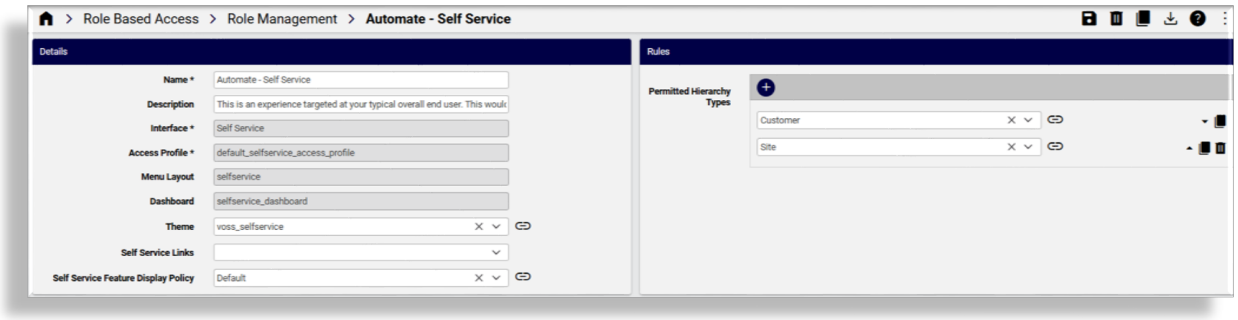
The Automate - License Manager experience comprises a Home dashboard, menus, and a collection of experience-based, role-focused dashboards. To view details for this menu layout, see:

- Menu: Automate - License Manager in the Core Feature Guide

Automate - Self Service role

The *Automate - Self Service* role provides an experience targeted at general end users that make use of the Self-service interface.

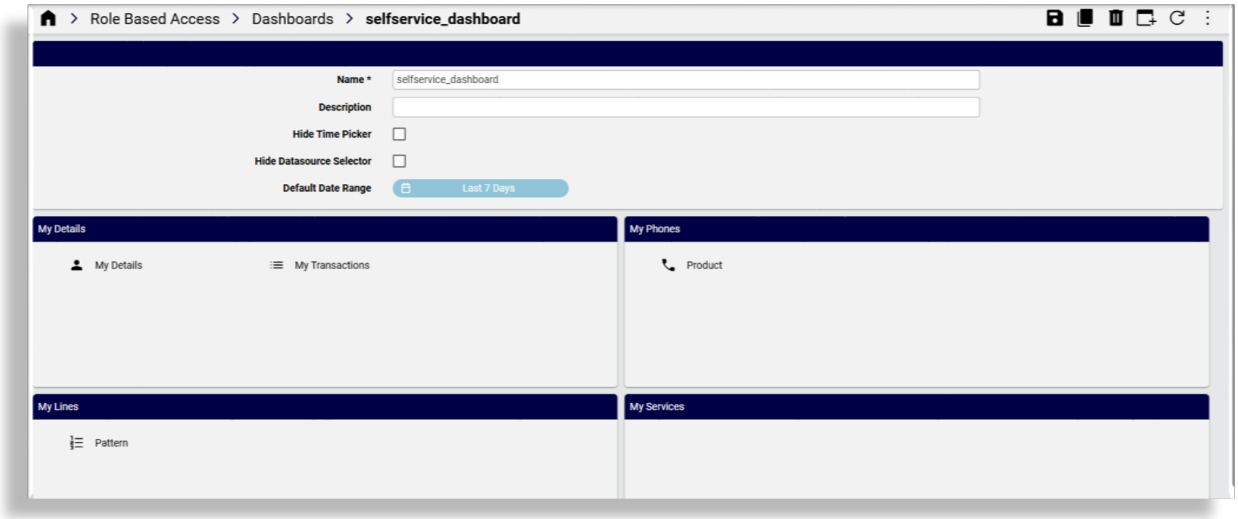
Copyright © 2025 VisionOSS Limited. All rights reserved.



- **Home dashboard**: selfservice_dashboard
- **Access profile**: default_selfservice_access_profile
- **Theme**: voss_selfservice
- **Interface**: Self Service
- **Hierarchies**: Customer, Site

Note: When setting the *Interface* on any role to Self Service, the following fields become read-only and are populated with the default values for a Self Service role. These fields are also read-only when editing an existing Self Service role:

- Interface
- Access Profile
- Menu Layout
- dashboard



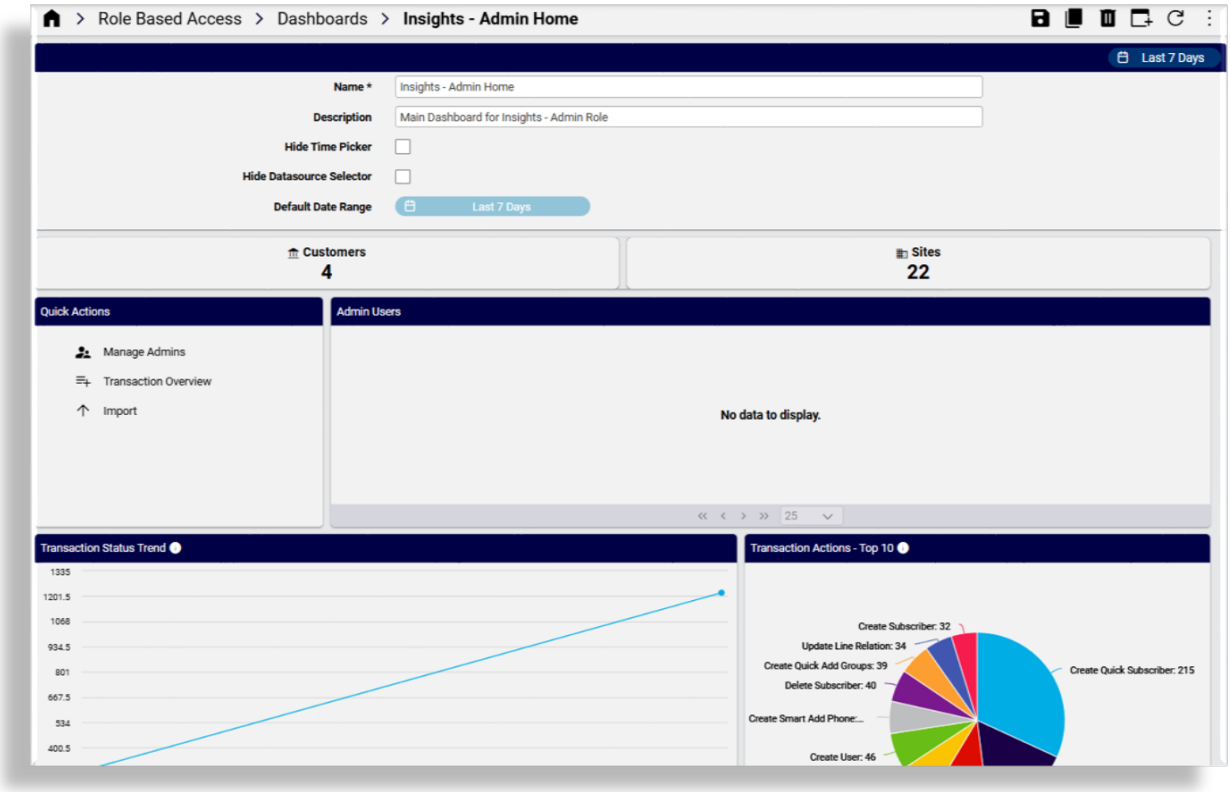
Copyright © 2025 VisionOSS Limited. All rights reserved.

Insights - Admin role

The *Insights - Admin* role provides an experience targeted at a typical, overall Insights application administrator. This role has wide access to the application setup and settings as well as a full range of actions in the system. These are typically advanced admins in the system but also provides a good guide and example of overall functionality in the system for other user types.

Insights - Admin: Home dashboard

The **Insights - Admin** role's Home dashboard is *Insights - Admin Home*, which displays a selection of counters, quick actions, and charts curated for the role.



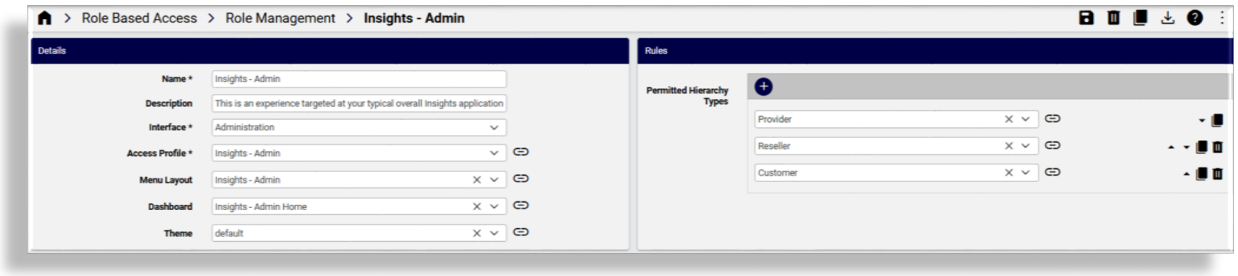
Insights - Admin: GUI layout

By default, the *Insights - Admin* role is assigned a theme, a Home dashboard, a menu layout, and an access profile, and is available for a selection of hierarchies:

- **Home dashboard**: Insights - Admin Home
- **Access profile**: Insights - Admin
- **Theme**: default
- **Interface**: Administration
- **Hierarchies**: Provider, Reseller, Customer

The image shows the *Insights - Admin* role settings:

Copyright © 2025 VisionOSS Limited. All rights reserved.



Insights - Admin menus and dashboards

The *Insights - Admin* experience comprises a Home dashboard, menus, and a collection of experience-based, role-focused dashboards.

2.2.2. Guide to the Admin Portal user interface

Tip: *Use the Action search to navigate Automate*

Overview

This topic is a guide to the standard functionality found in the Automate Admin Portal user interface toolbars, forms, and lists.

Note: Automate 25.1 ships with role-based GUI layouts, available by default on new installs, that can be enabled for different roles. For details, refer to *Role-based dashboards and menus*.

Related topics

- Role-based dashboards and menus, in the Core Feature Guide
- Introduction to Themes in the Core Feature Guide
- Theme Customization topics in the Advanced Configuration Guide
- Search in Automate in the Core Feature Guide
- *Working with lists*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Admin Portal toolbars

In the Automate Admin Portal, icons on the main toolbar are always available, regardless of the form or list you're viewing.

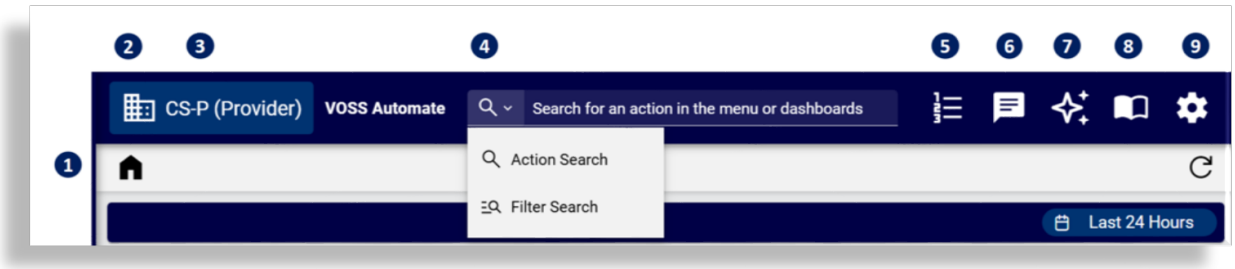
Important: Some icons (and related functionality) are available only if your access profile permissions allow it. For example:

- The **Transaction** icon is available only if you have read permissions on `tool/Transaction`
- The **Saved Searches** panel is available only if you have read permissions on `data/UserSavedSearch`
- You'll only receive alert notifications if you have read permissions on `data/Alert`
- The **Help** book icon displays only when you have access to the general help (Misc Permissions)

A form/list-based toolbar displays additional icons, depending on the model you're working with (which defines the content on the form or list you're viewing), and on your access profile and permissions. For example, if it's not possible or allowed that you move certain items, the **Move** icon won't display.

Main toolbar

The table describes the graphical controls and icons on the main Admin Portal toolbar:



The table describes the icons on the main toolbar in the Admin Portal:

Copyright © 2025 VisionOSS Limited. All rights reserved.

1. Home	The Home button displays a customizable dashboard that serves as a landing page. See "Automate Dashboards" for details. • The system displays a welcome message the first time a user logs in with a new account. • When a non-SSO or non-LDAP user logs in, a system message alerts the user to any failed login attempts. • When SSO or LDAP users log in, the system displays the last successful login time.
2. Organization Selection	Launches a hierarchy (organization) tree view that displays a tree or list of available nodes. See *Navigate the hierarchy* Note that the accent color is used for this element.
3. Hierarchy element	A hierarchy element displaying the highest hierarchy level. The associated child hierarchy element display in a similar field display box adjacent to the main hierarchy element. If there is more than one level or node at a specific hierarchy, you can search and navigate the hierarchy. See *Navigate the hierarchy*.
4. Search	The toolbar Search bar. Fill out search criteria to use the default search (Action search), or click the down arrow at the filter icon to choose an alternative search mode: • Action search - perform a fuzzy, free text, actions search, for example, *Modify Voicemail* or *Create user*. • Filter search - choose from a predefined list of entities • Global search - available only to users with appropriate permissions; allows querying of the API for models and search criteria
5. Transactions log	Displays the Opens the Transactions Log, where you can view a list of in progress and recent completed transactions, and drill-down to view transaction details. The pulsing counter above the icon indicates the number of transactions currently in progress. The spinner adjacent to the icon indicates that your transactions are in progress.
6. Messages	A notification indicator and menu for accessing the Transaction log and Alerts (if alerts are enabled). A pop-up notification displays when a transaction is done. You can click on the message to inspect transactions. Alert notifications display until all alerts are removed from the list.
7. Wingman	Opens Wingman Chat if enabled. Refer to *Wingman*.

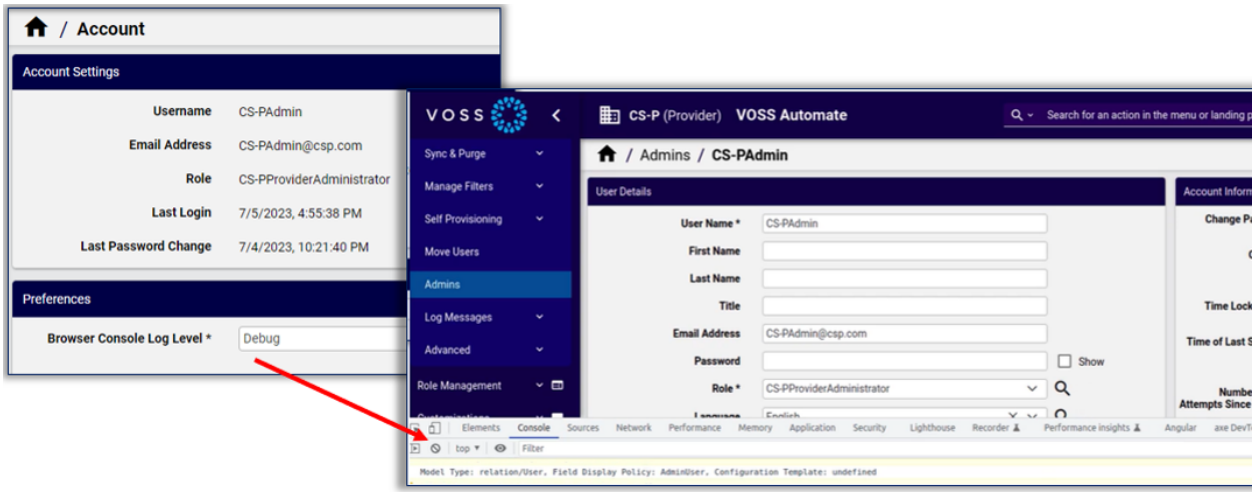
Copyright © 2025 VisionOSS Limited. All rights reserved.

8. Help	Opens the system online Help in a new browser tab.
9. Settings (Cog icon)	Provides a menu with items for: • The logged in user's **Account Settings** (read-only), **Quick Actions** to sign out or change password, and **Preferences** where you can set the **Browser Console Log Level**. If the **Browser Console Log Level** is set to `Debug`, your browser console (**Inspect** menu) provides additional details when selecting menu items and instances on the GUI, for example: `Model Type: relation/User, Field Display Policy: default, Configuration Template: undefined, Fixed Filters: undefined` This setting reverts to `None` (default) when you sign out. When set to `None`, the browser console **Inspect** menu does not show these details. See the note below this table for more information about this setting. • **About** form with version details - see: *About (system details)*. • **Sign out** button to log out the user.

Note: To view details for and of the following applied to any page in the GUI, on the **Preferences** page, set **Browser Console Log Level** to `Debug` and save your changes. Then open the page where you want to view these details, right click, and choose **Inspect** to open the browser console:

- Model
- Field display policy
- Configuration template
- Fixed filters

Copyright © 2025 VisionOSS Limited. All rights reserved.



Forms and lists toolbar

For certain models, such as Roles or Credential Policy, the list view or detail view of the record in the Admin Portal displays an additional toolbar with a number of controls.

The icons that display on this secondary toolbar depend on your access profile and based on the functionality available for data on the form or list (the model you're working with).

Standard icons

The table describes standard icons that typically display on all forms and lists.

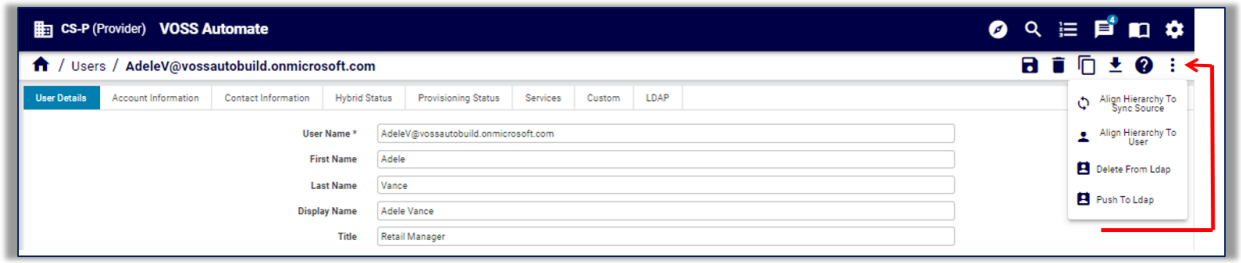
Copyright © 2025 VisionOSS Limited. All rights reserved.

Icon	Description
Filter	Allows you to filter items on a list.
Refresh	Manually refresh a list view to load updated data.
Plus icon (+)	Creates a new record from a list view.
Delete	From a list, remove an entry or the selected entries.
Move	You can move some model instances (by default, device models) from the current hierarchy to another hierarchy. When moving device models, the system won't allow you to move a device model instance to a hierarchy node with a different device. For data models, move is allowed if you edit the data model's definition in the Operations section.
Clone	Make a copy of the current item, and rename it to create a new instance.
Export	From search results or any list view in the system, it is possible to select the entities required and export them with all attributes. The selected data can be exported to: • A JSON file that is archived into .json.zip format for external use. • Excel - an export containing data and Excel columns for all fields as shown in the JSON export format. • Excel(formatted) - an export containing data and Excel columns as arranged by any Field Display Policies that apply.
Save	Saves a new or updated record.
Cancel	Cancels triggered events such as transactions or bulk loads. A Cancel icon on forms aborts the page or action.
Back	On forms, this icon returns to the original list page position. The browser's back button also carries out this action.
Help	Open the on-line help page for the current model.

Overflow actions menu

On forms and lists that allow multiple actions, icons for key actions (for example, Filter, Add, Create, Update, Delete), are always visible on the toolbar, whereas other available actions are accessible via a vertical ellipsis toolbar icon ( ), which displays a drop-down menu of the additional (overflow) actions available for data on the form or list.

The image shows non-key actions available in the overflow menu when viewing or updating a user, for example:



Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Accessibility support is provided for the overflow actions menu so that you can tab through the actions and press **Enter** or space bar to select an action in the menu.

The table lists actions that may be available in an overflow actions menu on a form or list, if relevant for the record and allowed for your access profile:

Action	Description
Bulk Load File	Only used via the **Bulk Load** page, when bulk loading a preselected file.
Bulk Modify	On the list view of certain items, the button displays a form to enter modifications to any selected list items and carries out a Bulk Modify. This is only available if your administrator has given you. the required permissions.
Configuration Template	For a form, create a Configuration Template for a model or carry out a task such as an advanced search.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Action	Description
Export Bulk Load Template	Export a model structure to a MS Excel bulk load file format. The file can be used as a template to bulk load instances of the model. Refer to the Bulk Load topic help.
Field Display Policy	Add a Field Display policy to a selected model. The detail view of a Transaction displays this button to show sub-transactions.
Execute	For an executable model such as a Provisioning Workflow, Macro, Wizard or for a script, run the execution.
Import	For supported Network Devices, carry out an import of data from the device.
Package	Create a package containing selected search results.
Refresh	Click this button on the Transaction list to refresh the list of transactions. This would for example update the Progress of the transaction.
Refresh User	On the **User Management** page, click **Refresh User** to align user data in relation/User with user data from source, caching from the UC application. This option is not exposed by default in the access profiles.
Replay	Transactions that have failed can, under certain circumstances, be replayed. This means that the transaction is re-submitted with the original request parameters.
Edit and Replay	Available for completed transactions. Similar to the **Replay** button, but allows you to first make changes to the previously submitted form before the transaction is resubmitted.
Reset Phone	Reset a phone.
Return	Return - From the detail display of a selected instance of a model, select this button to return to the list display of the model instances.
Tag	For a selected model instance, add a tag to it.
Tag Version	For a selected model instance, add a version tag to it.
Test Connection	For instances of models representing connection parameters such as connections to devices, click the button to test the connection.
Visualize	Deprecated.
Purge	Removes a record entirely.
JSON Editor	Update a JSON file.
Apply	Saves and updates the record.
Lock	Disables editing.
Reset	Clears the record.
Align Hierarchy to Sync Source	Used for managing users. See *User added as Microsoft Active Directory LDAP User*.
Align Hierarchy to User	Used for managing users. See *User added as Microsoft Active Directory LDAP User*.
Restart	
Vendor Config	
Wipe	

Copyright © 2025 VisionOSS Limited. All rights reserved.

Forms and lists

The Admin Portal displays information in forms (pages) and lists.

Detail	During input, mandatory fields are highlighted in a red frame.
List views of details	If the text in a column exceeds the defined column width, it is truncated with an ellipsis (. . .), except for any column showing the row entry hierarchy.

Tip: To easily copy data from a drop-down list or in a list view (provided you're using a mouse), highlight the value while keeping the mouse button pressed down and use the keyboard shortcut **CTRL-C** to copy, then release the mouse and paste the data where required.

Alternatively, a selected item (drop-down list selection box is active) from a drop-down list can be copied with **CTRL-C** and pasted into another input field using **Ctrl-V**.

Form controls

The following controls are typically available on forms.

Icon	Description
	Plus. Open another instance of the current form field or open a pop-up screen to add an item.
	Minus. Delete the current instance of a field from a form or open a pop-up screen to confirm.
	Down arrow. Move the selected instance on a form down in the order of field entries. In the case where a Position field is available, for example for Lines, the entered value determines the order in the object.
	Up arrow. Move the selected instance on a form up in the order of field entries. In the case where a Position field is available, for example for Lines, the entered value determines the order in the object.
	Collapse/expand icons. Collapse or expand all array items, for form arrays with multiple items. Arrays are collapsed by default. You can expand or collapse selected array items in a form array, or expand/collapse all from the form array header.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Icon	Description
	Left arrow. Right arrow. On multi-tabbed forms, navigate to the previous or next tab.
	Warning. Used, for example, if a mandatory field is not filled in.
*	Next to an input control on a form, the asterisk indicates that the field is mandatory.
[Browse]	Next to an input control on a form, a button to open a file selection dialog.
[V]	Drop-down input box. Typing into the box filters the drop-down list choices.
	URI link. A generated URI link you can click to open the related entity (`data`, `device` model) directly from the drop-down list.

Note: On some parts of the user interface, when adding or deleting items via pop-up screens, clicking the **OK** button typically completes the update; that is, you won't need to also click **Save** on the main form.

Switching form layouts

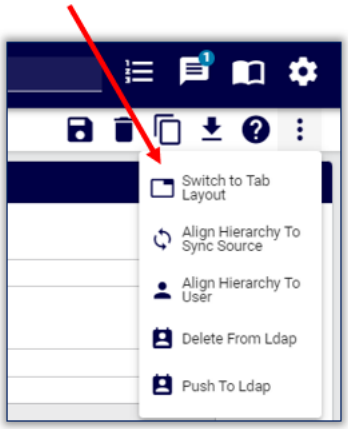
The layout of forms in Automate is defined via a number of field display policies (FDPs). For groups of fields, the default layout for the field display policies setting, **Display Groups As**, is *Panels*, except for the forms associated with the following models, which have their default layout as *Tabs*:

- `view/GlobalSettings`
- `data/SiteDefaultsDoc`
- `data/ucprep_UC_Profiles`
- `relation/DP_REL`
- `data/HcsDpDialPlanSchemaDAT`
- `data/HcsDpDialPlanSchemaGroupDAT`

On forms where you're able to change the layout (depending on your user type and the model type), you can click the layout change icon (**Switch to Panel Layout** / **Switch to Tab Layout**) to switch between a tab layout and a panel layout. The layout you choose is preserved when you log out and log in again.

On some forms, the action element to use for switching between tabs and panels may display in the overflow actions menu.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: This guide refers to the default layout for the model, unless otherwise specified.

Some form views do not have the action element available to switch between tabs and panel form views. For details and the list, see the “Display Groups As” topic at: *Field display policies*.

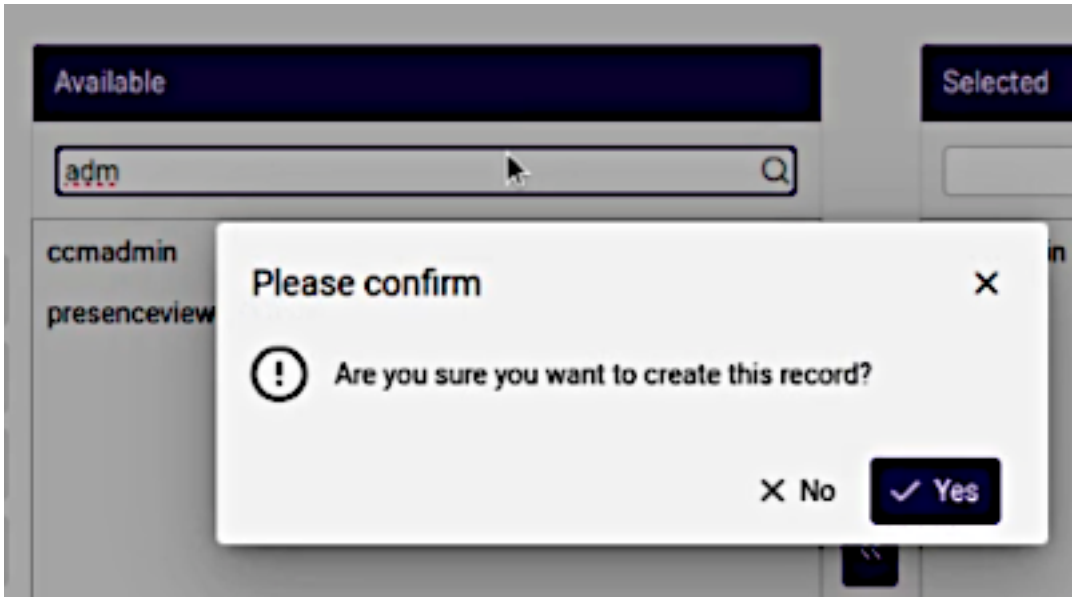
Related topics

- *Field display policies*

Pop-ups and slide out notifications

- A **Please confirm** pop-up notification appears in the middle of an add or edit form of the interface if the **Enter** key is used in the input field. This notification thus allows for the confirmation of the data currently entered or edited prior to saving the form.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- A **Cached** slide-out notification at the top right of the interface displays when the locally cached data of a resource is used.

  This slide-out notification can be minimized to a narrow bar on the side of the screen.

Navigate to related entities from drop-downs

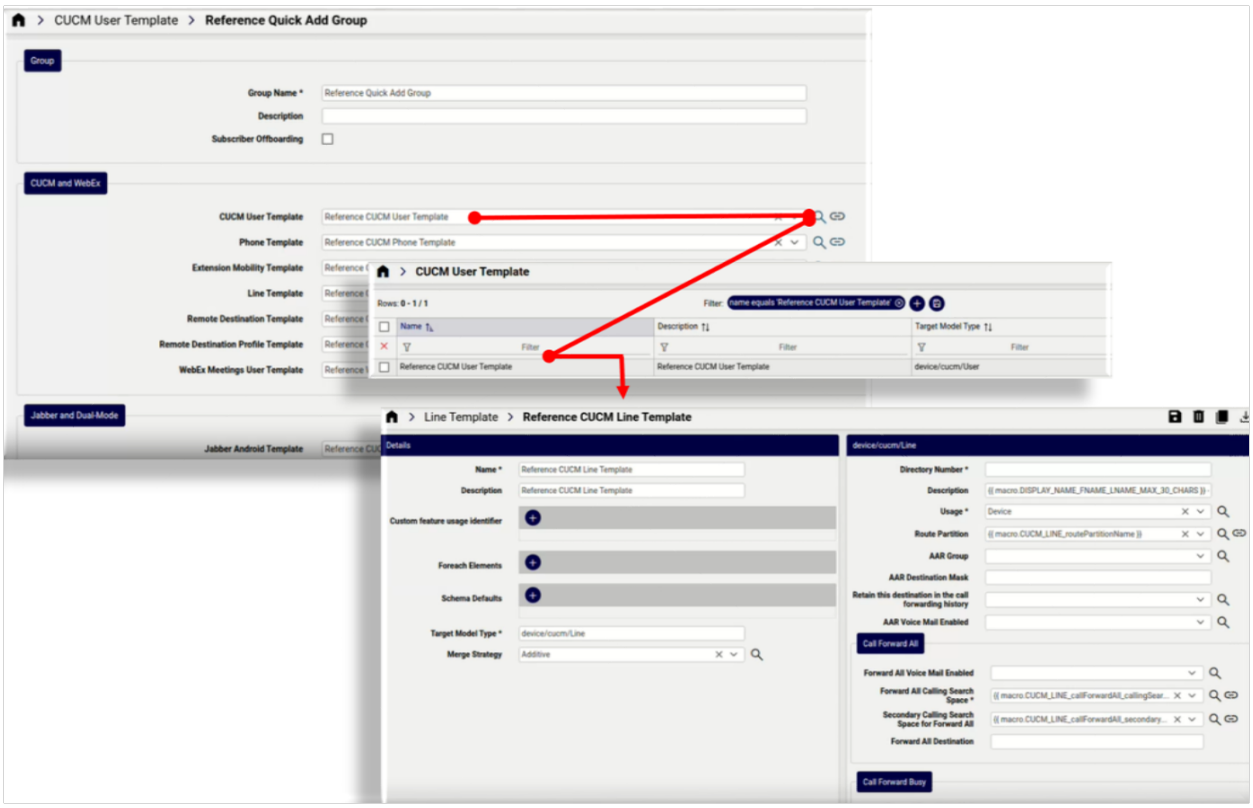
Automate provides clickable links adjacent to drop-down fields that reference related entities, that is, drop-downs that have a direct URI link, or a macro that uses a model type:

Note: The links are not relevant for drop-downs that have functions in the macro since that does not allow the system to determine the underlying model type.

- These links allow direct navigation to the relevant configuration template (CFT) or model type at the same hierarchy.
- The system determines the target model and attribute, then applies a filter to show the correct list view.
- Link icons are shown only when the field is populated and accessible to the user.

This feature applies broadly across drop-downs in the GUI, particularly in Quick Add Groups, to streamline admin workflows for provisioning tasks.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Sessions and authentication

Since Automate sessions are cookie based, it is possible to share the same session across different tabs or windows of the same browser. However, it is not possible to have different authentication sessions in different tabs. In other words, login as different users in different browser tabs is not supported.

On-line help

To access the full online help website from the Automate Admin Portal, press the toolbar Book icon. To access help for a page you've viewing in the system, click the **Help** icon.

The page-level (context) help also includes a **Full HTML Help** link for the entry on the online help website and the model help (as seen in the GUI tooltips).

Note:

- To access the online help website URL, you may need to request that the website be made accessible by your network administrator.
- Your view of the system help depends on your hierarchy level, role-based access permissions, and the field display policies applied to your system.

Copyright © 2025 VisionOSS Limited. All rights reserved.

About (system details)

The **About** menu provides details for your system, including version, patches, and adaptations.

Note: The **About** toolbar icon provides only version details.

Version

- Release: Installed product release version.

  The version naming convention is:

  - new: *<YY>.<num>*, for example: 19.3 is the 3rd release of 2019.
  - legacy: *<major>.<minor>.<revision>*, where major=YY,minor=num,revision=revision of num.
- Patch Bundle: The installed Patch Bundle (PB) number, if any.
- Build Number: Product build number.
- Release Date: Date when this version was released.
- Deployed Mode: Current deployment mode type, for example:
  - Provider
  - Enterprise

Note: You can use the toolbar Copy icon to copy version release text to the clipboard.

Patches

If any patches have been installed on the system, these are listed under the **Patches** menu. Details of installed patches are also provided for reference and enquiries, for example:

- **Version**: in this context, the patch version (there can be multiple versions of the same patch).
- **Defect IDs**: Automate internal IDs for reference
- **Models**: any models and model **Instances** added or affected by the patch

Adaptations

If any adaptations are installed on the system, these are listed. Select an adaptation from the list to see more details, for example:

- **Adaptation Tag(s)**: the tags can be used to find all models that are a part of the adaptation, using a search query such as

```
(tag IS <tag1>) or (tag IS <tag2>)
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

where `<tag1>` and `<tag2>` are the names of tags.

Note: The search for models is carried out from the user hierarchy and down.

- **Upgrade Risk**: an indication of the impact of an adaptation on an existing system:
  - High: Core changes
  - Medium: Standalone adaptation using core workflows
  - Low: Standalone feature

License

This menu provides details for your current license, including the platform UUID, license status, and expiry date. See also, *Manage your Automate product license*.

License counts

This menu provides a chart with details, for example:

- Weekly Automate license usage totals trends
- A chart showing the breakdown of the Automate license usage by metric
- License information table
- A table showing the full data set of license audit details
- A table showing the Microsoft user information fields
- Counters for Automate Platform license usage totals

For details, see the Licensing and User Data Export Guide. To modify the dashboard, refer to the topic on managing dashboards and widgets.

2.2.3. Manage items

Tip: *Use the Action search to navigate Automate*

Editing items

Edit on GUI forms

Provided you have the necessary user and model permissions, you can edit and save items directly on the GUI forms. Note the following:

- Displayed field names are customizable and provide tooltips according to a Field Display Policy for the model.
- Form GUI rules control the default field availability and pre-populated values.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- When opening a form, form details are initially rendered using cached data. Save is disabled while non-cached data loads, and is enabled once the non-cached data has been loaded.
- Most forms provide a Help button for editing guidance.

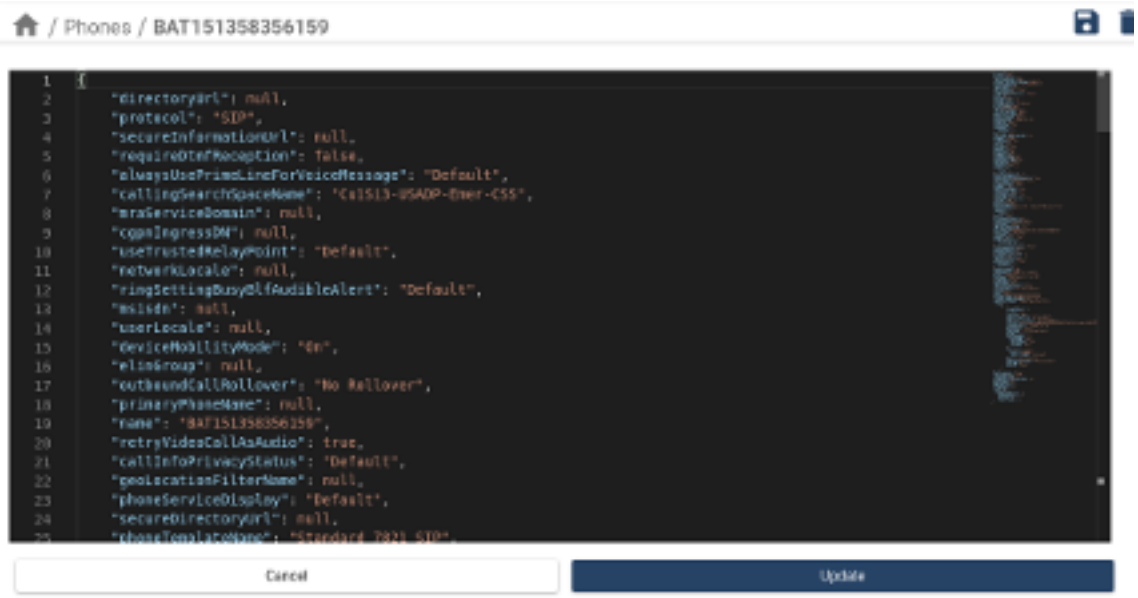
Edit in the JSON editor

You can edit items in the JSON editor if your high-level administrator has enabled the **Json Editor** permission for your access profile. See *Access profile permissions and operations*.

If you have the required permissions, the **JSON Edit** button displays on the toolbar. <>

Note: The JSON Editor is available only in the new Admin Portal. See *Conventions used in this guide*.

1. Navigate to a page that provides access to a JSON editor, for example, transactions, or phones.
2. Click the **JSON Edit** button to open the JSON editor.
3. Edit the JSON format data on the form.
4. Click **Update** to update data on the GUI input form.
5. Click **Save** to commit your changes.



Important: Accessibility options in the JSON editor

When using the JSON editor with a screen reader application, note the following:

- Pressing **ALT+F1** enables accessibility options.
- Pressing the **Escape** key closes the accessibility help dialog.
- Pressing **Ctrl+M** enables and disables editor tabbing.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Pressing **SHIFT+TAB** while inside the editor allows you to move focus to various components and controls inside the editor. For example, to update modified data, press **SHIFT+TAB** until focus reaches the **Update** button; then, press the **Enter** key to update the data.

At the time of writing (21.2), the JSON editor does not support the use of the **TAB** key on its own to move focus from one component to another within the editor. The workaround is to use **SHIFT+TAB** for navigation within the editor.

Create a clone

You can create copies (clones) of certain items, such as roles, credential policies, devices, and phones. Cloning provides a quick way to create new items, based on data from the cloned item.

You can create a clone wherever you see a **Clone** button in the Admin Portal. For example, you can't create a clone in the list views. Saving a new cloned item creates the clone.

If an item refers to other items, only the current item is cloned, and not the referenced items. For example, when cloning a phone, referenced device models (Phone and Remote Destination) aren't added to the clone.

On the cloned item, you will need to edit the cloned key field(s), such as *Name*, and provide new values to create the new item in the system. If you don't change a key field value, the system displays the following error message: "Error, Duplicate Resource Found."

To clone an item:

1. Log in to the Admin Portal.
2. Choose the hierarchy level of the item to be cloned.
3. Choose the item you want to clone.
4. Click **Clone**. The page refreshes and the form displays the cloned item.
5. Edit the required details.
6. Click **Save** to create the new item.

Selecting items

You can select one or more existing items in a list to delete or modify these items at once.

- To delete or modify one item in a list view, click on the relevant item, and click the action, for example, the Delete button.
- To delete or modify multiple items in a list view, select the checkbox for each item. If the list view spans multiple pages, you can select items on each page before performing the bulk action. The table header displays the number of selected items. Once you have all the items selected, click the action, for example, Export.

Note:

- Actions such as **Export Bulk Load Template**, **Field Display Policy**, and **Configuration Template** apply to the *type of item* and are not affected by the item selection.
- Actions such as **Bulk Modify** depend on whether your administrator has given you the required permissions.

When selecting items, note the following:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Items selected across multiple pages remain selected until the transaction (or export) is complete, at which time all selected items are cleared.
- Items selected while on a specific menu, for example, Users, are automatically cleared as soon as you select a different menu.
- Items selected across multiple pages are automatically cleared when you select the 'All' checkbox in the header of the first column (on any of the list pages).
- Manually clear selected items on one or more pages by selecting and then clearing the checkbox located on the left of the *first* column in the header row.

Where the Admin Portal user interface provides a list of check boxes, a "toggle all" checkbox allows you to quickly select or deselect of all checkboxes.

Transfer boxes

Side-by-side transfer boxes (Available / Selected) are used on various forms in the system, such as Audit Number Inventory, Re-skill Agents (Contact Center) and Upload Multiple Files to MOH Clusters.

Transfer boxes allow you to choose a selection of items for processing in a transaction. For example, you may want to perform an audit on numbers from selected sites only.

The initial list of items in an **Available** transfer box displays up to 5000 results. You can then specify a case-insensitive *contains* filter to return relevant results, even when the list of items exceeds 5000.

Bulk delete and modify

When more than one item is selected from the list view of items, the selected items can be deleted in bulk by using the **Delete** button on the button bar.

If your administrator has given you the required permissions, you can also bulk modify certain items, for example Roles.

Select the check boxes of the items you want to modify and choose the **Bulk Modify** action on the button bar. The input form for the item is opened. Values entered on this form (which is an update template) are modified for all selected items when you choose the **Bulk Modify** action.

Note: When opening the form for the bulk modify, boolean flags do not take a value by default.

To unset a boolean field:

- After opening the form for bulk modify, toggle the field to on (set) and then off (unset) again. This forces the value in the boolean field to be set with a value of false (or unset).

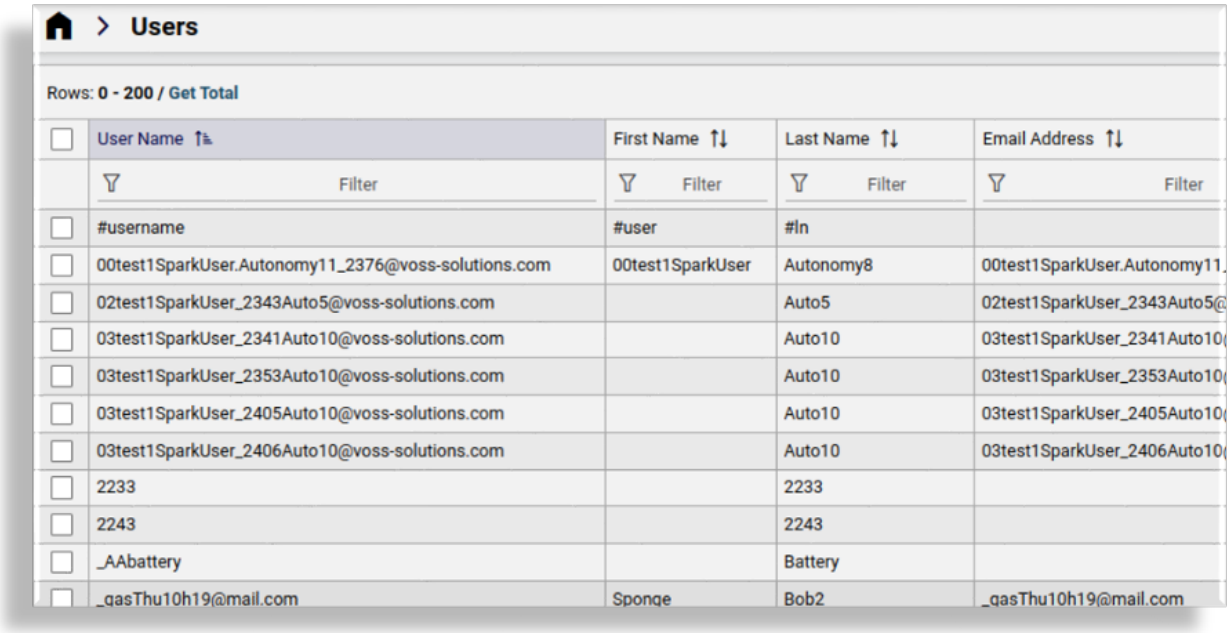
2.2.4. Working with lists

Overview

Summary views of resources and services are shown in lists in the Automate Admin Portal. For example, you can view a list of components in your system hierarchies, or to view a list of customers, sites, users, subscribers, servers, or device types.

The lists include functionality that allows you to sort, order, and filter items, and to navigate across multiple pages.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related Topics

- *Guide to the Admin Portal user interface*

Get total

A **Get Total** link is available at the top of list and filtered views to show the total number of rows in a list in the case where there are more than the default 200 rows shown on a page. Pagination controls will then be adjusted accordingly.

The purpose of this control is to speed up the initial display of long lists.

Refresh lists

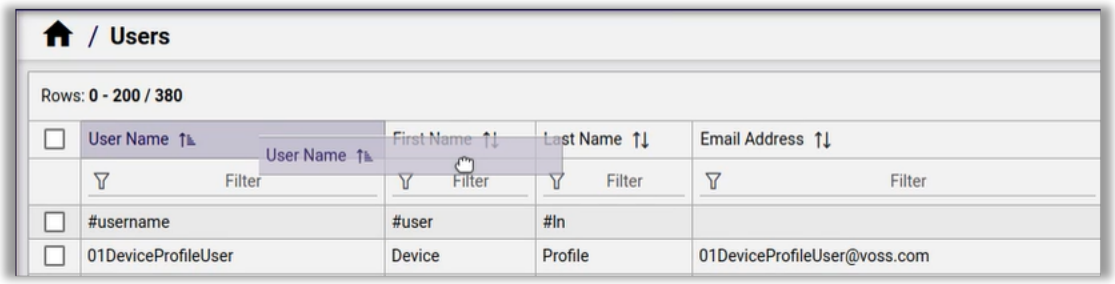
The Automate toolbar **Refresh** icon allows you to refresh the list view any time, for example, you may want to reload list items once a transaction completes related to the items you're viewing on a list.

Note: If you have a filter applied to the list, refreshing the list displays the new item if it matches any applied filters. In the scenario described above, if you have a filter applied to only show phones containing the characters *123*, the refreshed list view will show any new phones containing these characters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Reorder columns

Automate allows you to select and drag a column to a new position in the list view, to rearrange the order of the columns. The updated column order is retained for you in your browser's local storage, until that storage is cleared.



Sort and order lists

Columns in the list views may contain string values or numeric values. The default sort order is on the first column, either alphabetically (descending) for string value columns, or numerically (descending) for numeric value columns.

To sort the list based on values in a column, click on any column header. Click again to change the direction of the sort order. An up/down arrow in the column header indicates the sort order.

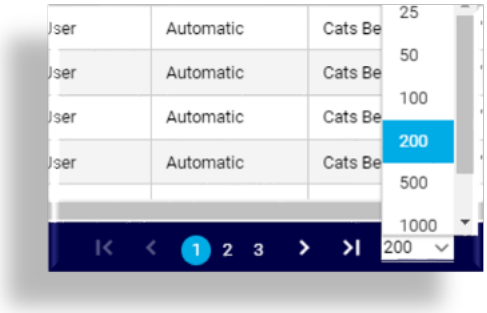
When sorting:

- Cells with no value move to the top or bottom of the list, depending on the sort order (ascending or descending).
- Upper case letters letters sort before lower case letters.
- Any column can be sorted, provided no filter is applied.
- Applying a filter to two or more columns disables sort.
- Leading spaces in field values are dropped from the list view. This may affect the sort order.
- Values in the **Located At** column are sorted according to the string value, and not the hierarchy path.

Navigate lists

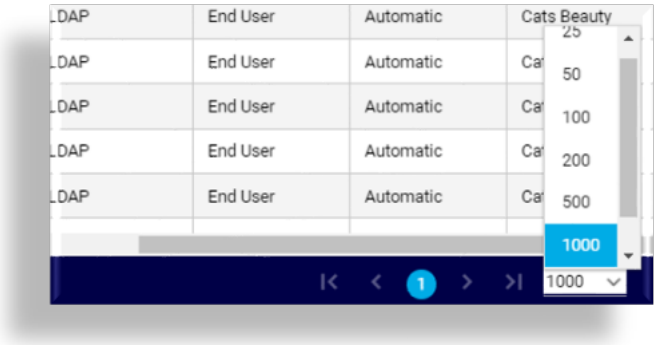
Lists with many items may display across two or more pages.

- To navigate across a multiple page list, click the right/left arrow to scroll to the next/previous page, or click a page number.

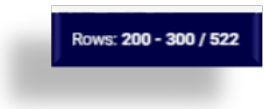


Copyright © 2025 VisionOSS Limited. All rights reserved.

- To view more items per page, specify the number of items to display on each page, from 25 to 2000. This includes lists of transactions, logs and sub-transactions.



- The header row displays the number of the rows you're viewing out of the total.



Note: Search results that display as lists return a maximum of 1,000 items. A system message at the bottom of the list indicates this limitation. Change the search criteria for result lists exceeding 1000 items.

Filter lists

This topic describes filtering on resource and service summary lists. For details around filtering transactions, sub-transactions, and log lists, see *Filter Transactions*.

A filter remains active until you remove it or until your user session ends (even if you navigate away from the page). If you're not seeing all data on a list, clear the filter by clicking the X icon adjacent to the **Filter** button, or open the dialog and remove filters.

Note: In the Admin Portal, when opening a list via a menu, and you create and apply a filter to this list, the filter is not retained for this list when you open the same list from a dashboard. The filter is retained for the list only when opening the list from a menu (any menu where that list is available).

The same applies for lists that you launch from a dashboard, when you create and apply a filter to the list you opened from the dashboard. In this case, the filter is only retained on the list when you open that list from a dashboard (any dashboard where that list is available)

To speed up the initial display of long lists, a **Get Total** link is available at the top of list and filtered list views where there are more than the default 200 rows shown on a page. Pagination controls will then be adjusted accordingly.

The Automate Admin Portal provides two options to filter a list view:

- Advanced filter
- Quick filter

Copyright © 2025 VisionOSS Limited. All rights reserved.

To filter lists in the Admin Portal:

1. Log into the Admin Portal.
2. Open a list view for a resource or service.
3. Add or modify filter criteria. The table describes the options:

Note: You can also sort the columns of filtered lists.

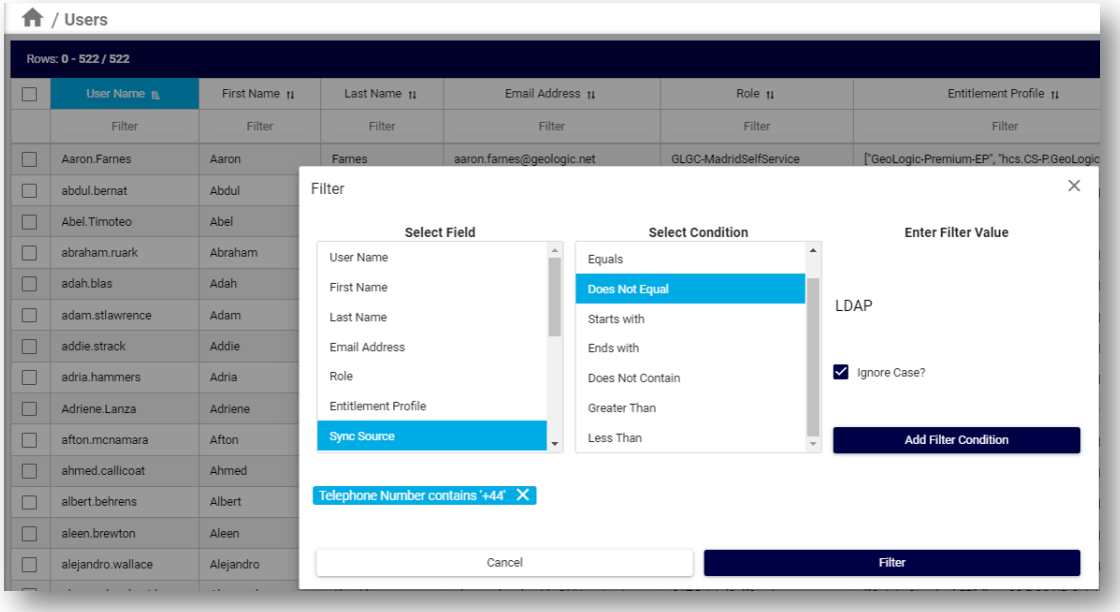
Filter option	Description
Advanced filter	1. Click the toolbar Filter icon to launch the **Filter** dialog. 2. Specify filter criteria: • Select a field and a condition, and enter a filter value. • To run a case-insensitive search, clear **Ignore Case**, else, leave the checkbox selected (default). • Click **Add Filter Condition**. To filter for empty rows in a specific column containing string values, choose **Equals** with "None" as value. To filter for non-empty rows in a specific string value column, choose **Does Not Equal** with "None" as value. Note that this condition does not apply to columns containing numeric or boolean values. To filter for strings that optionally contain or match string values, choose **Equals** and then the options can be joined with `[OR]`. For example: `Ben[OR]Jerry` will filter on values containing or matching `Ben` or `Jerry`. 3. To add another filter, click **Add Another Filter**, then repeat the steps above to select another field and condition. 4. Click **Filter**. 5. View filter criteria you added. • The filter is applied to the list. • Filter criteria is added to the top of the page (as well as in the Filter field at the top of the relevant column). • To add more filter criteria, click the Plus icon (+) adjacent to the criteria at the top of the page to open the **Filter** dialog, or click in the Filter field for the relevant column to add new criteria. • To edit individual filter criteria, click on the filter to open the **Filter** dialog, or edit the criteria in the Filter row for the relevant column. • To remove a filter, click the Delete icon (x) for the relevant filter criteria at the top of the page, or click the red X icon in the row to remove all filters. 6. To save your filters as a search, click the Save icon adjacent to the filters. Saved searches are added to the user **Account** (from your **Settings** icon), under **Saved Searches**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

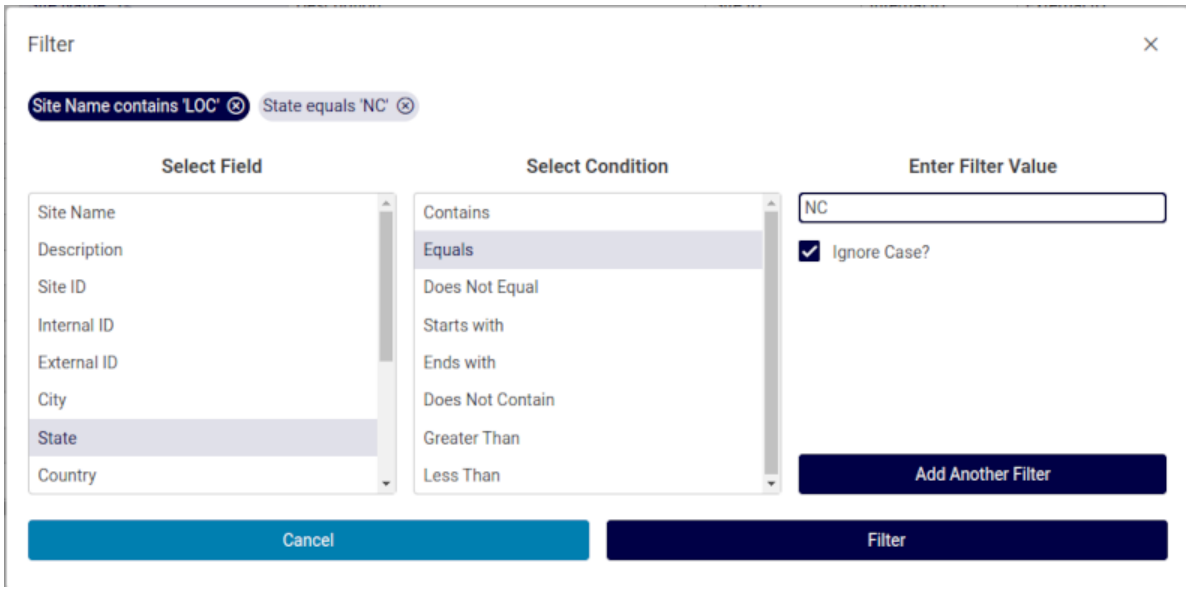
Filter option	Description
Quick filter	1. Click in the **Filter** field below the header of the column you want to filter on. 2. Type in filter criteria (one or more characters; or using `[OR]` to join these) • The filter is applied to the list. • Filter criteria is added to the top of the page (as well as in the Filter field at the top of the relevant column). • To add more filter criteria, click the Plus icon (+) adjacent to the criteria at the top of the page to open the **Filter** dialog, or click in the Filter field for the relevant column to add new criteria. • To edit individual filter criteria, click on the filter to open the **Filter** dialog, or edit the criteria in the Filter row for the relevant column. • To remove a filter, click the Delete icon (x) for the relevant filter criteria at the top of the page, or click the red X icon in the row to remove all filters. 6. To save your filters as a search, click the Save icon adjacent to the filters. Saved searches are added to the user **Account** (from your **Settings** icon), under **Saved Searches**.

Filter Examples

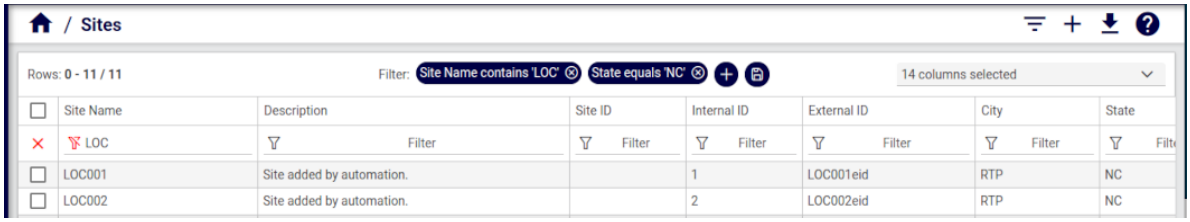
- Specify advanced filter criteria in the **Filter** dialog.



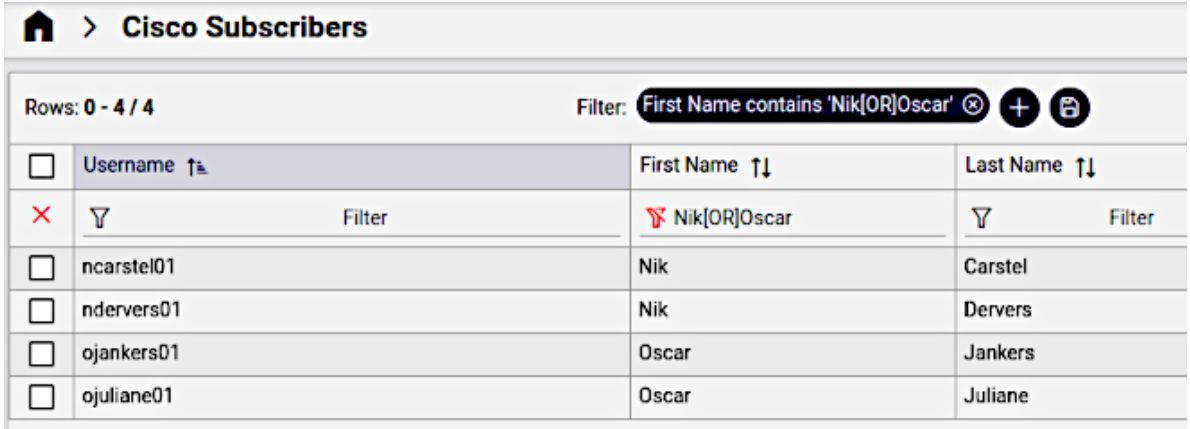
Copyright © 2025 VisionOSS Limited. All rights reserved.



- Advanced and quick filter criteria you add displays at the top of the page, and to the top of the relevant column/s.

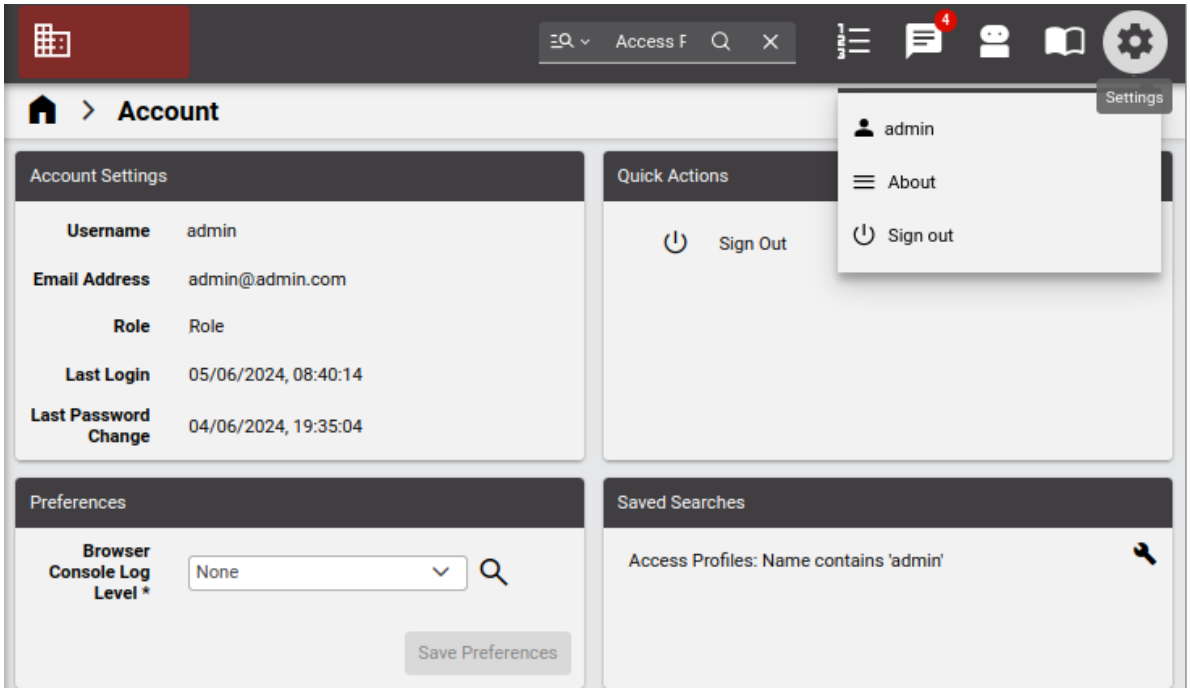


Showing the use of `[OR]` in a quick filter:



- Advanced and quick filter saved searches display on the user **Account** (from your **Settings** icon), under **Saved Searches**.

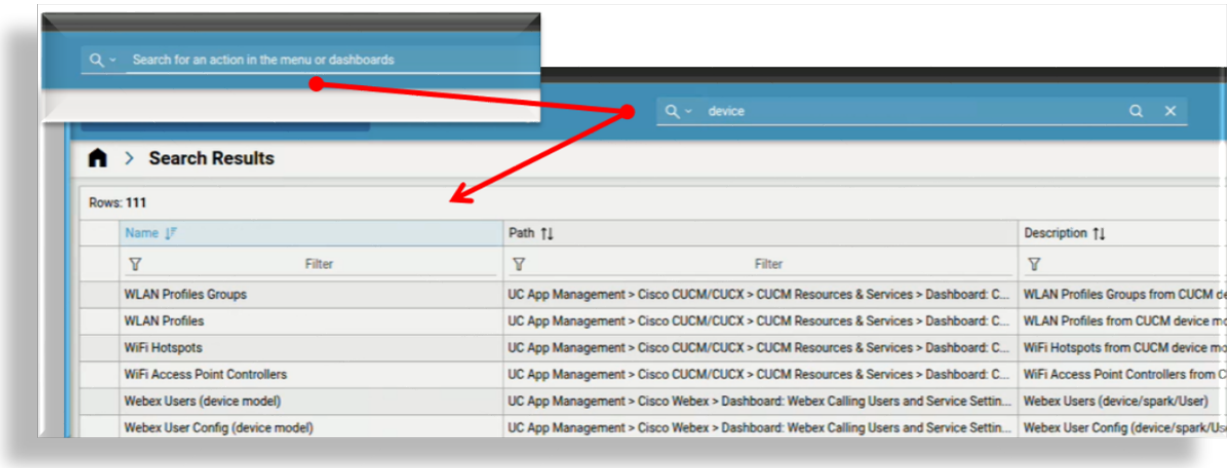
Copyright © 2025 VisionOSS Limited. All rights reserved.



2.2.5. Use the Action search to navigate Automate

Overview

Automate's toolbar **Action search** helps you to quickly find functionality, dashboards, and menu items in the Automate GUI. It's the default search method and is especially useful when searching for functionality in a role-based dashboard layout.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Search in Automate in the Core Feature Guide

How to use Action search

1. Type the name of the page, dashboard, or action you're looking for,
2. Press **Enter** or click the **Search** icon.
3. Select the relevant result to open the page.

Result handling

Action search uses title text from menus, dashboards, and actions, and also matches against model names, even if those names aren't visible in the result string. This improves relevance but may occasionally surface unexpected results. To ensure clarity, queries that match only the underlying model type (without a friendly label) are excluded from results.

The result set includes functionality that makes it easier to manage large result sets and to quickly locate a desired action:

- **Sortable and filterable column headers**: You can sort results alphabetically or reverse-alphabetically.
- **Keyword filters**: Enter filter criteria to narrow down long result lists.
- **Clear filters**: Reset filters to view the full result set again.

Result formats

- Menu entries appear as: *Menu > Submenu*
- Dashboard entries appear as: *Dashboard: Name*

Search tips

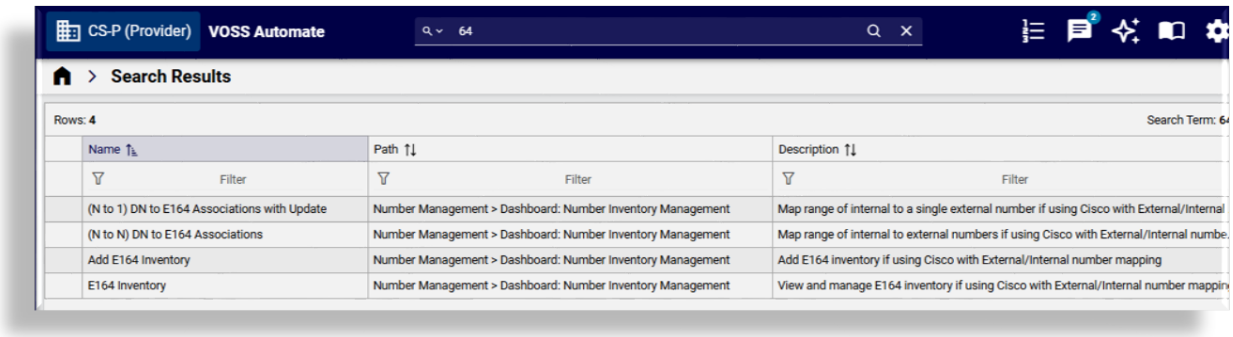
To improve your Action search results:

- Use singular keywords, for example, "phone" instead of "phones", or *add subscriber* instead of *add subscribers*.
- Avoid filler words like "the", "a", or "an".
- Use specific verbs like "create", "add", "update", "edit", "delete", or "remove".

  Note: Verbs in the search phrase return results that match the same word in a menu or dashboard, based on your role permissions.

- Include device names, such as "Cisco UCM", to find related models and actions.
- Abbreviations are supported. For example, "QAS" finds "QAS - MS Teams" and "Quick Add SIP Gateway".
- Include digits to find menus with numbers in their names, for example, "E164 Inventory".

Copyright © 2025 VisionOSS Limited. All rights reserved.



Example use cases

- Searching for “SIP Gateway” filters out unrelated models unless explicitly named.
- Typing “Cisco” and sorting results helps quickly locate all Cisco-related actions and dashboards.
- Filtering by “add” or “edit” helps isolate tasks based on operation type.

Best practices for admins

To ensure meaningful search results with Action search:

- Use familiar and descriptive terms when naming menus, dashboards, and actions.
- Configure dashboards based on user roles for faster access.
- Action search can be used to locate tasks not visible in dashboards or menus.
- Regularly review naming conventions to align with user expectations and improve discoverability.

2.2.6. Search in Automate

Overview

Automate provides three search types via a **Search** field on the GUI toolbar:

Search Mode	Description
Action search	Default. Searches for entries or actions available on the menus and dashboards.
Filter search	Choose from a predefined list of entities to launch a **Filter** dialog, where you can add additional criteria to filter results.
Global search	Performs a search based on all or part of a search term that queries the API for the relevant model and search criteria.

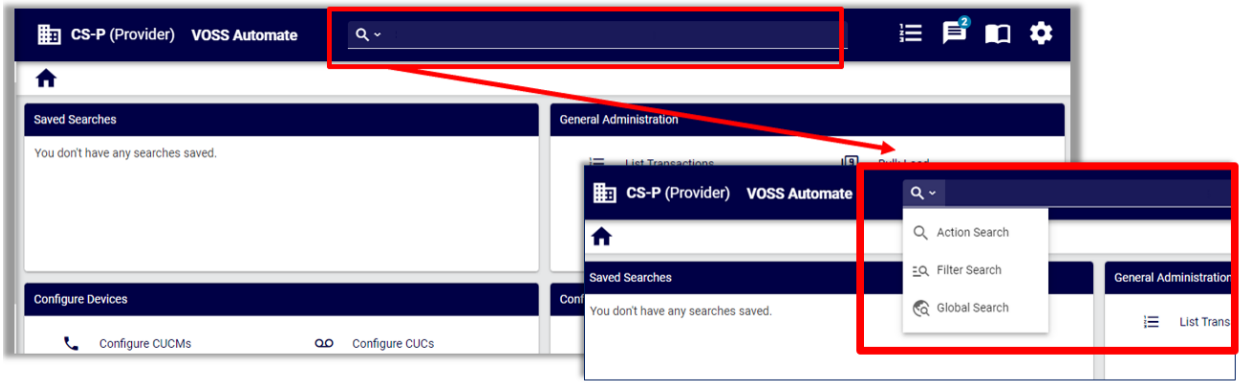
For further details, see:

- *Action search*
- *Filter search*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *Global search*

For details on using Wingman for chat, see: *Wingman*. To toggle between search modes, click the down-arrow at the search icon. The last used search mode and search criteria text is retained during the current session in the browser and when you log out and log in again.



Related topics

- *Working with lists*
- *Searchable fields*
- *Case-insensitive search fields*
- *Use the Action search to navigate Automate*

Search types

Action search

Action search is the default search mode in Automate. It is a case-insensitive, fuzzy, free text search that includes the *contains* condition. Search results are based on the menus and dashboard links for your role, as well as on the menu or dashboard path (where to find the entry), and descriptions (when populated).

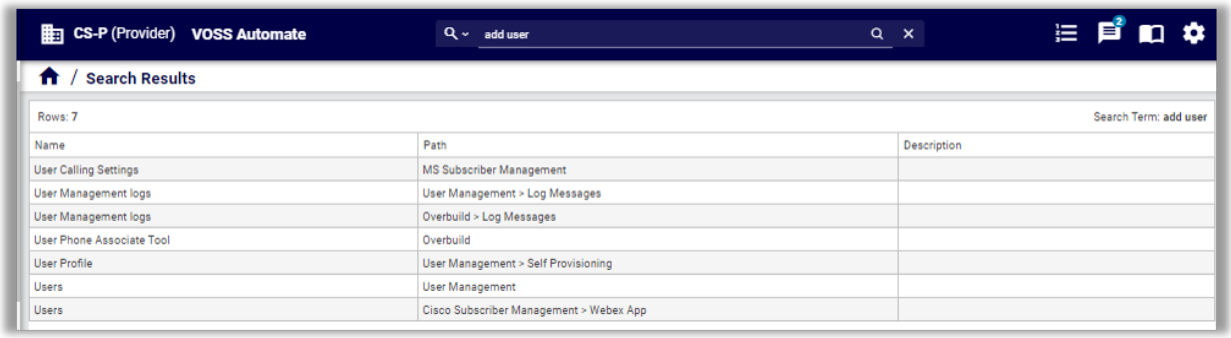
You can use the Action search to fill out a search phrase or single word to navigate quickly to a relevant form, view, or list. All relevant items are returned.

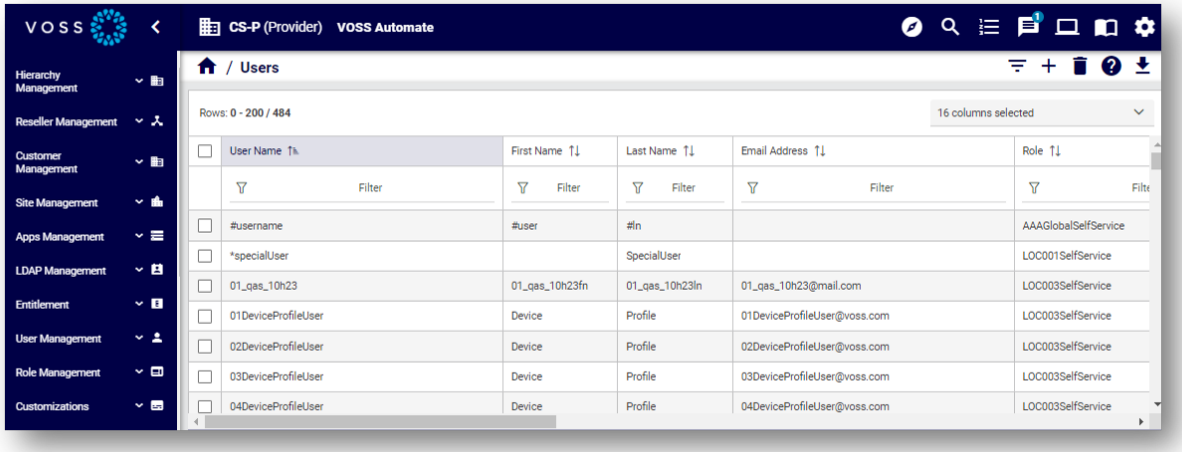
- When searching for *user*, results include *Phones* because *Phones* is an item included under the (Cisco) *User Management* menus.
- When searching for *settings*, the search result includes the macro entry for **Emergency and CLI Settings**, since the word *settings* is included in the name.

Including *add* in your search phrase generates results for *create* and *add*.

You can click on a search result to open it in the system.

Copyright © 2025 VisionOSS Limited. All rights reserved.





Related topics

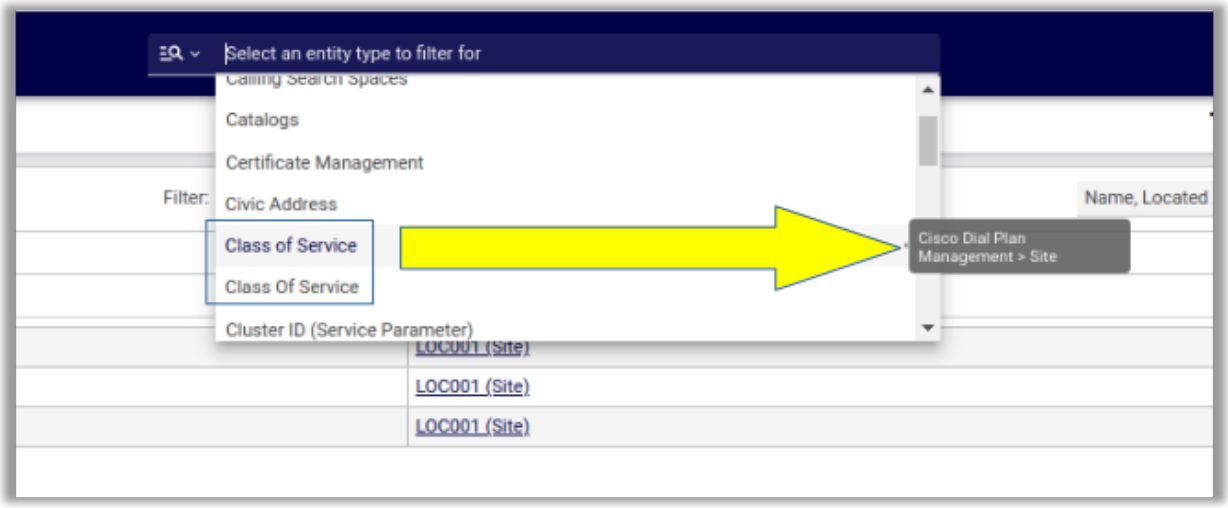
- *Use the Action search to navigate Automate*

Filter search

In a **Filter search** you choose from a predefined list of entities (based on your role) to launch a **Filter** dialog, where you can further refine the criteria to filter results.

Tooltips for the entity display the path to the entity. Where duplicate entities appear in the list, the tooltip indicates the difference.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Select an entity to open a **Filter** dialog, where you can refine search criteria, if required.

For further details around using a filter search, see *Filtering lists in the Admin Portal* in *Working with lists*.

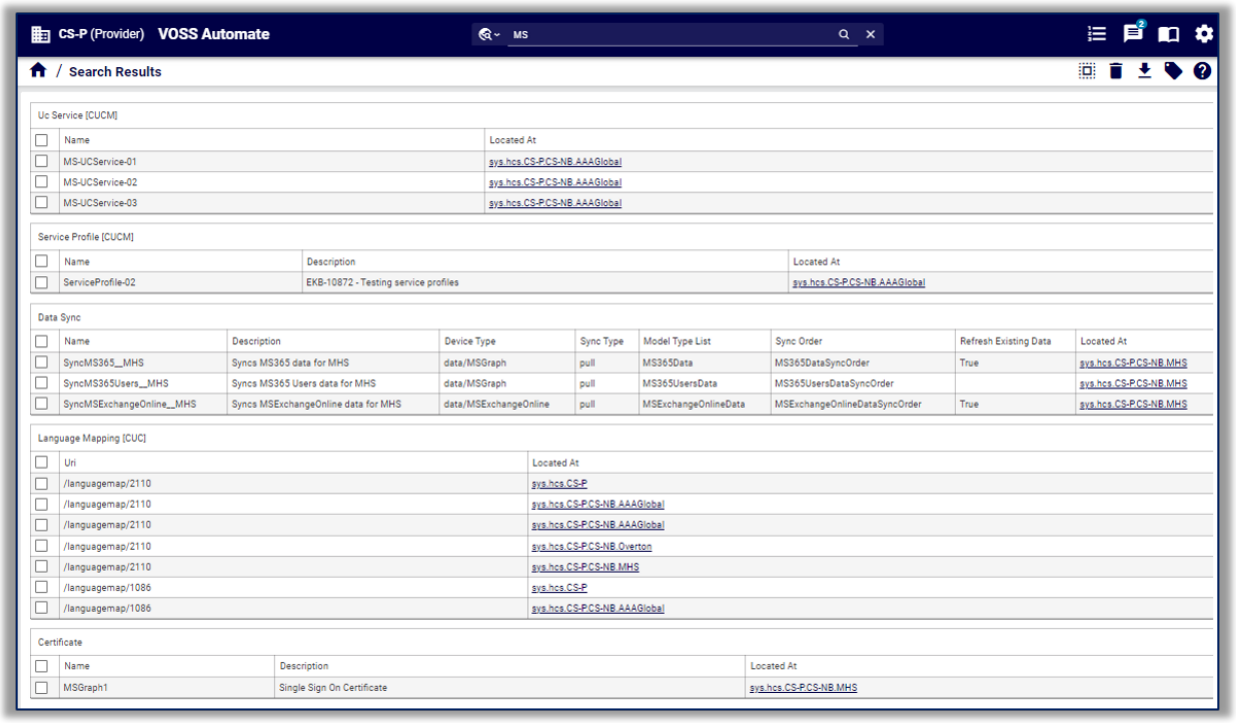
Global search

Note: The Global search from the **Search** bar is only available to a user with a role that has an access profile with **Permitted Type** containing `tool/*` (and no restriction on `tool/Search`) or **Type Specific Permissions** containing `tool/Search`. Otherwise, the search bar is hidden.

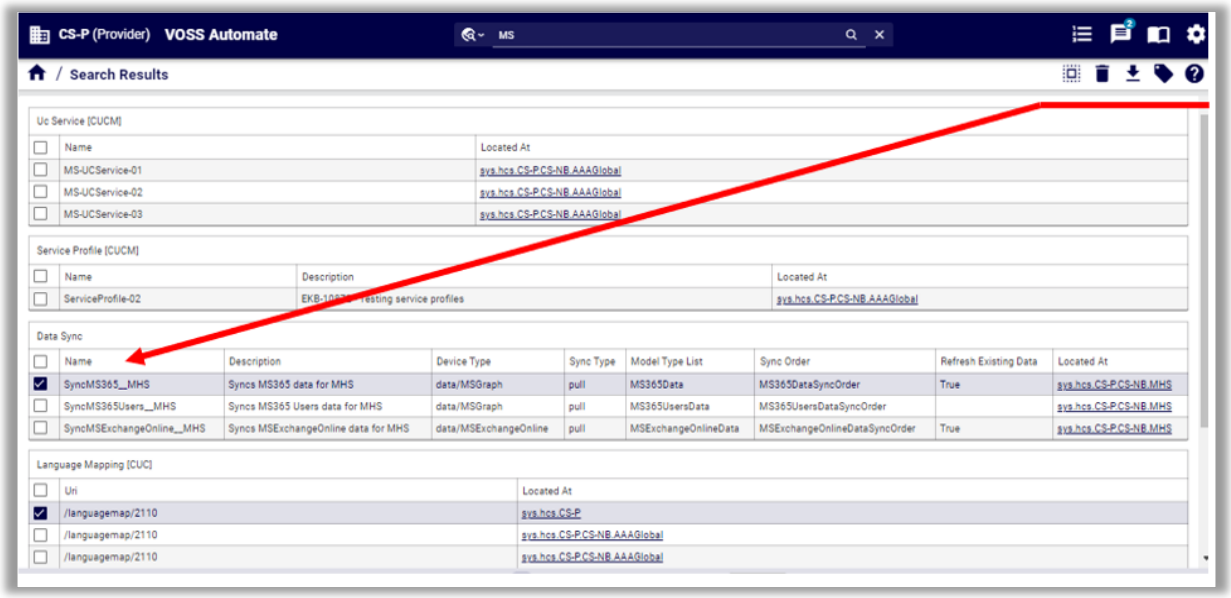
For details on Access Profiles, see: *Introduction to access profiles*.

A Global search from the **Search** bar performs a search based on all or part of a search term that queries the API for the relevant model and search criteria. Results display as a list of links, showing the models.

Copyright © 2025 VisionOSS Limited. All rights reserved.



You can select the checkbox adjacent to a search result (one or more), then click a toolbar action, such as **Delete**, or select an option from the **Action** drop-down (for example, **Export** or **Tag**. Actions allowed on search results are permissions-based, depending on your access profile, with caveats on the number of items, relations, and device models:



- In a global search the maximum number of rows the system returns is 2000. The page size limit is 200 rows.
- Search results are returned for your current hierarchy and below.
- Click on a search result to open it and view its details.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- From a selected search result, you can click on the **Search Results** breadcrumb to see all results again.
- Search results for a simple string search matches the *contains* condition in the text of a component.
- Simple search strings match values in data and device models (relations instances are not returned). To search the relation model instances, specify the model as a part of the query.
- Case-insensitive searches on field names are supported on several models. See *Case-insensitive search fields*.
- You can search on the summary attributes of any models, and for some models you can also search on a subset of their attributes. See: *Searchable fields*.
- Selecting a data or device model instance returned in a search displays the full model details; that is, without a Field Display Policy applied.

Constructing search queries for Global search

Search syntax

For Global search, you can construct search queries to search for specific items, based on Automate search syntax filters.

Search queries can contain:

- Model type and model name references
- Model attribute and nested model attribute references
- Key words
- Brackets, for grouping
- Query string, using valid query string characters, as follows:
  - alphanumeric characters
  - Any of:

    ```
    !@#$%^&*-_=+<,.>/?\|[{]}~`
    ```

  - To search for single quote in a string, wrap the string in double quotes
  - To search for double quote in a string, wrap the string in single quotes

Search queries are carried out on models, so you can specify the model type and the model name in a query, using the syntax `type/name` as the full reference to a model type (for example, relation, data, or device) and model name (for example, Countries).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Search keyword types

Various keywords can be used to construct a search query. Available keywords are categorized by type, either of the following:

- Specification - WITH
- Matching - IS, LIKE
- Grouping - AND, OR

Keyword	Description and Examples
WITH	Restricts the search to look for only specific data types. In the example below we have specified the data type Countries and so only countries will be returned. `((data/Countries WITH country_name LIKE Kingdom) AND (data/Countries WITH country_name LIKE Unite ))`

IS	For a result to be returned the data attribute must match exactly the 'input'. In the example below the 'input' is Spain and only a Country with the attribute country_name Spain will be returned. If 'North Spain and South Spain existed they would not be returned. In the example below we have specified the data type Countries and so only countries will be returned. If we had not specified a data type then the search would cover all data types looking for an attribute country_name.
	`country_name IS Spain`
	
	`data/Countries WITH country_name IS Spain`
	Another example with a model tag as reference:
	`tag IS "feature"`

CONTAINS	Matching is done by substring and is the default parameter. For a result to be returned, the data attribute must contain 'input'. In the example below, the 'input' is 'Sw' and the search would find both 'Sweden' and 'Switzerland'. `data/Countries WITH country_name CONTAINS Sw`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Keyword	Description and Examples
LIKE	Matching is done by fuzzy search. For a result to be returned, the data attribute must nearly match 'input'. In the example below, the 'input' is 'swe' and the search would find both 'Sweden' and 'Switzerland'. `data/Countries WITH country_name LIKE swe`
AND	This grouping term allows you to combine different searches and only finds a result where both conditions are met. The example below the search would find 'United Kingdom' but not the 'Kingdom of Bhutan' as in this case the second condition (LIKE Unite) is not true. `((data/Countries WITH country_name LIKE Kingdom) AND (data/Countries WITH country_name LIKE Unite ))`
OR	This grouping term allows you to combine different searches and matches a result where any one or both of the conditions are met. The example search below would find 'United Kingdom', 'United States' and 'Kingdom of Bhutan'. `((data/Countries WITH country_name LIKE Kingdom) OR (data/Countries WITH country_name LIKE Unite))`

Search examples

Where the attribute of a model is nested in an object, the reference to the attribute in the search query requires a model type specification.

For example, for a model `data/User` with an attribute in a nested object called `account_information`, the query should take the model type (`data`) specifier:

```
data/User WITH data.account_information.credential_policy IS Default
```

The following query *will not* yield results:

```
data/User WITH account_information.credential_policy IS Default
```

Brackets should be used in a query with matching and grouping operators. In a query containing no model references, brackets are evaluated first. The order of bracket evaluation is inner to outer brackets.

Example Queries (line breaks added):

```
(((data/Countries WITH pstn_access_prefix IS 9) AND
  (data/Countries WITH emergency__access_prefix IS 112))
 OR (data/Countries WITH international_access_prefix IS 00))
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Search string format

The string to search for can be specified with the following properties:

- Multi-word and quotes

  When searching for a multi-word string value like “United States”, the value must be enclosed in either single quotes: `'United States'`, or double quotes: `"United States"`.

  When single word or multi-word values contain a single or double quote, the string needs to be enclosed in double or single quotes respectively, for example: `"L'Amour"`.

- Case sensitivity

  Use the appropriate operator (LIKE)

In a query containing model references, brackets and grouping keywords, the query is evaluated in the order shown in the table below.

Order	Element	Description
1	WITH	Model reference is evaluated first.
2	brackets	Brackets evaluate before grouping keywords.
3	AND	AND grouping evaluates before OR grouping.
4	OR	Evaluates last.

A number of attributes from the meta data of a model can also be searched:

- `__device_pkid`: if a device pkid is known, then for example:

  `device/cucm/Line WITH __device_pkid IS 55c32b59a6165451e04f392a`

- `pkid`: if a pkid is known, then for example:

  `data/CallManager WITH pkid IS 55c32b59a6165451e04f392a`

- `tags` (can also use “tag”): if the tag name is known, then for example:

```
((data/FieldDisplayPolicy WITH tag IS feature_tag_add_customer) AND
 (data/FieldDisplayPolicy WITH tags IS applicationendtoend))
```

Note: Only lower-case tags are searchable.

“Contains” search in drop-down lists

On forms where you select values from pre-populated, editable drop-down lists, Automate allows you to run a case-insensitive “contains” search to filter across the entire result set for the drop-down. Paginated scrolling is supported for large result sets.

To run a “contains” search in a drop-down list:

1. Start typing any value in a drop-down field.
2. Select the relevant option from the result set.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2.2.7. Searchable fields

All models can be searched for by using their summary attributes. In addition, a number of models can also be searched on by a subset of their attributes.

Below is the list of these models and their searchable fields:

- `device/cuc/AlternateExtension`
  - `DtmfAccessId`
  - `IdIndex`
  - `UserObjectId`
  - `ObjectId`
- `device/cuc/Callhandler`
  - `templateObjectId`
  - `DisplayName`
  - `ObjectId`
  - `DtmfAccessId`
  - `Language`
  - `TimeZone`
  - `VoiceName`
  - `RecipientSubscriberObjectId`
- `device/cuc/CallhandlerMenuEntry`
  - `DisplayName`
  - `CallHandlerObjectId`
  - `TouchtoneKey`
  - `TransferType`
  - `TransferNumber`
  - `Action`
- `device/cuc/CallhandlerOwner`
  - `TargetHandlerObjectId`
  - `ObjectId`
- `device/cuc/CallhandlerTransferOption`
  - `URI`
  - `TransferOptionType`
  - `CallHandlerObjectId`
  - `TransferOptionType`
  - `Extension`
  - `Action`
  - `TransferType`

Copyright © 2025 VisionOSS Limited. All rights reserved.

- device/cuc/Greeting
  - GreetingType
  - CallHandlerObjectId
- device/cuc/HtmlDevice
  - DeviceName
  - DisplayName
  - SubscriberObjectId
  - ObjectId
  - SmtpAddress
  - CallbackNumber
- device/cuc/PagerDevice
  - DeviceName
  - PhoneNumber
  - DisplayName
  - ObjectId
  - SubscriberObjectId
- device/cuc/PhoneDevice
  - DeviceName
  - PhoneNumber
  - DisplayName
  - ObjectId
  - SubscriberObjectId
- device/cuc/SmsDevice
  - DeviceName
  - DisplayName
  - SubscriberObjectId
  - ObjectId
  - SmppProviderObjectId
  - RecipientAddress
  - SenderAddress
- device/cuc/SmtpDevice
  - DeviceName
  - PhoneNumber
  - DisplayName
  - SubscriberObjectId
  - ObjectId

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - SmtpAddress
- device/cuc/User
  - Alias
  - FirstName
  - LastName
  - DtmfAccessId
  - EmailAddress
  - TimeZone
  - templateAlias
  - ObjectId
  - MailboxStoreObjectId
  - CallHandlerObjectId
- device/cuc/UserPassword
  - Alias
  - UserObjectId
  - CredentialType
- device/cuc/UserPin
  - Alias
  - UserObjectId
  - CredentialType
- device/cucm/DeviceProfile
  - class
  - description
  - lines
  - loginUserId
  - name
  - phoneTemplateName
  - product
  - protocol
  - services
  - softkeyTemplateName
- device/cucm/EnterpriseFeatureAccessConfiguration
  - pattern
  - routePartitionName
- device/cucm/Line
  - alertingName

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - description
  - asciiAlertingName
  - pattern
  - routePartitionName
  - shareLineAppearanceCssName
  - callPickupGroupName
  - presenceGroupName
  - usage
- device/cucm/Phone
  - callingSearchSpaceName
  - class
  - description
  - devicePoolName
  - digestUser
  - lines
  - locationName
  - name
  - ownerUserName
  - phoneTemplateName
  - presenceGroupName
  - primaryPhoneName
  - product
  - protocol
  - subscribeCallingSearchSpaceName
  - ip_address
  - status
- device/cucm/PhoneButtonTemplate
  - name
  - basePhoneTemplateName
- device/cucm/PhoneSecurityProfile
  - description
  - name
  - protocol
  - phoneType
- device/cucm/PhoneType
  - PhoneType

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - ProtocolTemplates
  - PhoneNamePrefix
- device/cucm/RemoteDestination
  - destination
  - name
  - ownerUserId
  - remoteDestinationProfileName
  - dualModeDeviceName
  - ctiRemoteDeviceName
- device/cucm/RemoteDestinationProfile
  - devicePoolName
  - description
  - class
  - lines
  - name
  - primaryPhoneName
  - product
  - protocol
  - userId
- device/cucm/RoutePattern
  - routePartitionName
  - pattern
  - destination
  - description
- device/cucm/RoutePlan
  - dnOrPattern
  - partition
- device/cucm/TransPattern
  - pattern
  - routePartitionName
  - calledPartyTransformationMask
- device/cucm/User
  - userid
  - mailid
  - firstName
  - lastName

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - associatedDevices.device
  - lineAppearanceAssociationForPresencesdepartment
  - lastName
  - primaryDevice
  - primaryExtension
  - phoneProfiles
  - status
  - userIdentity

2.2.8. Case-insensitive search fields

Case-insensitive searches and macro lookups can be carried out for some model types and fields.

This topic lists these models and their field name case variants:

- data/NormalizedUser
  - username
  - mail
- data/User
  - username
  - sso_username
  - email
  - username_avaya_system_manager
  - username_broadworks
  - username_cuc
  - username_cucm
  - username_hcmf
  - username_ldap
  - username_microsoft
  - username_ms_365
  - username_ms_ldap
  - username_ms_teams
  - username_open_ldap
  - username_uccx
  - username_webex_teams
  - username_zoom
- device/avayaes/Agent
  - Name

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - name
- device/avayaex/User
  - LoginID
  - loginid
  - FirstName
  - firstname
  - LastName
  - lastname
  - EMail
  - email
- device/avayaol/User
  - FirstName
  - firstname
  - LastName
  - lastname
  - UserName
  - username
- device/avayasm/User
  - loginName
  - loginname
  - userName
  - username
  - givenName
  - givenname
  - middleName
  - middlename
  - surname
- device/azureadonline/MsolUser
  - UserPrincipalName
  - userprincipalname
- device/cuc/Callhandler
  - DisplayName
  - displayname
- device/cuc/GlobalUser
  - alias
  - Alias

Copyright © 2025 VisionOSS Limited. All rights reserved.

- device/cuc/User
  - alias
  - Alias
  - emailaddress
  - EmailAddress
- device/cuc/UserPassword
  - alias
  - Alias
- device/cuc/UserPin
  - alias
  - Alias
- device/cucm/Phone
  - ownerUserName
  - ownerusername
- device/cucm/RemoteDestination
  - ownerUserId
  - owneruserid
  - name
  - dualModeDeviceName
  - remoteDestinationProfileName
  - ctiRemoteDeviceName
- device/cucm/RemoteDestinationProfile
  - userid
  - userIdname
- device/cucm/TodAccess
  - ownerIdName
  - owneridname
- device/cucm/User
  - userid
  - mailid
  - userIdentity
- device/ldap/user
  - samaccountname
  - sAMAccountName
- device/msgraph/MsolUser
  - UserPrincipalName

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - `userprincipalname`
- `device/msteamsonline/CsOnlineUser`
  - `UserPrincipalName`
  - `userprincipalname`
- `device/pexip/Conference`
  - `primary_owner_email_address`
- `device/spark/User`
  - `email`
- `relation/HcsAdminUserREL`
  - `hcsUname`
- `relation/HcsUserREL`
  - `username`
- `relation/SparkUser`
  - `email`
- `relation/Subscriber`
  - `userid`
  - `mailid`
- `relation/SystemUser`
  - `username`
- `relation/UccxAgent`
  - `userID`
- `relation/User`
  - `username`
  - `email`
- `relation/Voicemail`
  - `Alias`

2.2.9. Wingman

Overview

Automate provides a **Wingman Chat** AI assistant in the Admin portal that can be activated by a user from any form.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Enabling Wingman Chat

Wingman Chat is enabled by default, and can be disabled and enabled `sysadmin` users and admins with access to the `data/Settings` model.

For details, see *Enable Wingman chat*:

- See **Enable Wingman Chat** in the *Settings* topic in the Advanced Configuration Guide.

Wingman requires internet access (to Microsoft Azure) and supports connecting via a web proxy. This can be configured by `sysadmin` users and admins with access to the `data/Settings` model and the **Web Proxy** menu. For details, see *Wingman web proxy* and *Set up a Web Proxy*.

Note:

- A user role should also be associated with an **Access Profile** that has **Wingman Chat** enabled under the **Miscellaneous Permissions**. From release 24.1, default administrator roles have this permission enabled and an upgrade to 24.1 enables this permission on all existing access profiles.
- In order to first use Wingman, an initial manual sync step is required - See: Insights Analytics in the Platform Guide.

For details on Access Profiles and the required administrator level to manage these settings, see:

- The Access Profiles chapter in the Core Feature Guide

Using Wingman

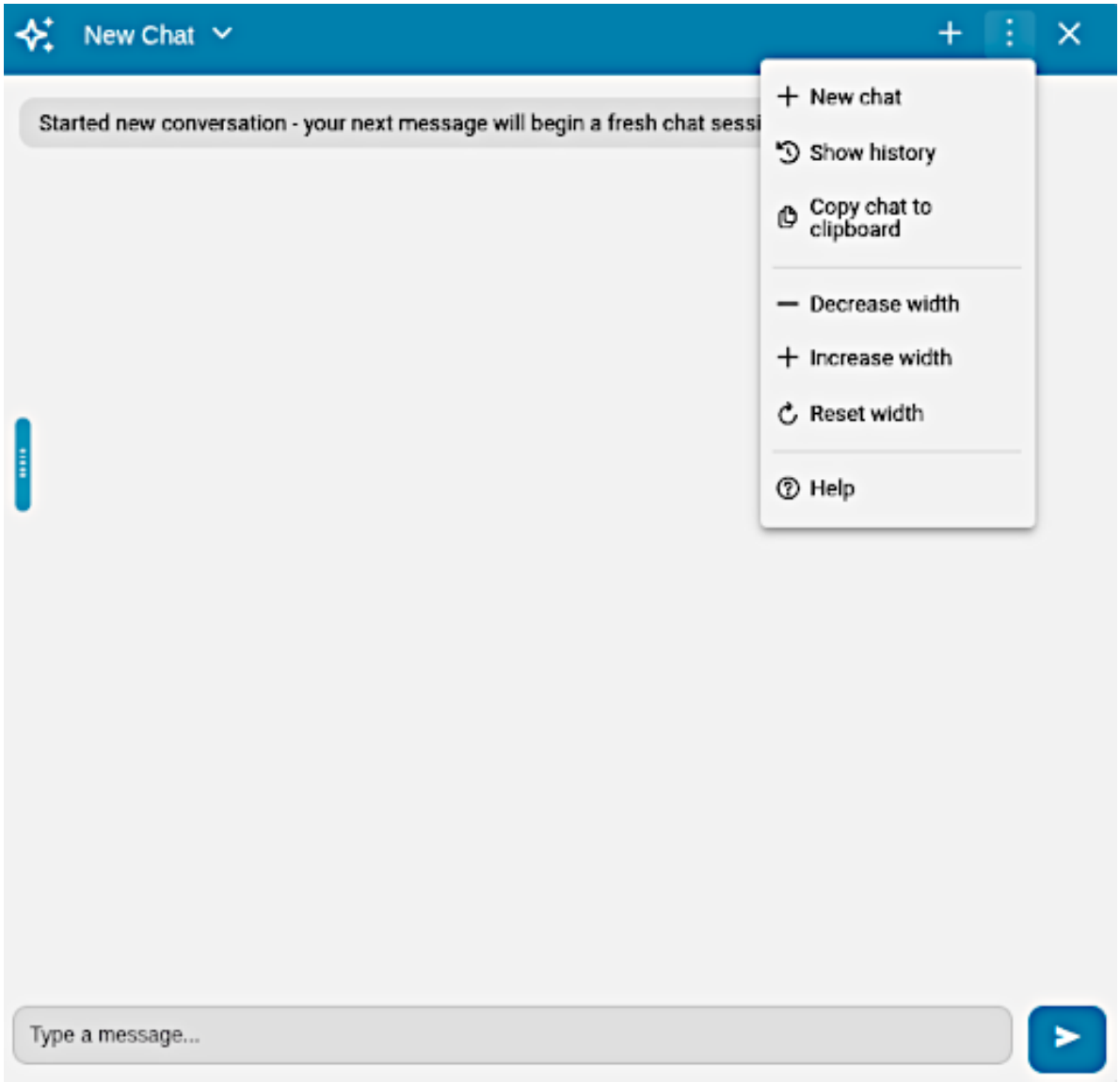
Note: While we strive to ensure and will continue to improve on chatbot accuracy in future releases, the correctness, completeness, or reliability of all results and documentation links is not guaranteed.

---

1. Click the **Wingman** icon on the Automate Admin Portal toolbar to launch the chat pane.

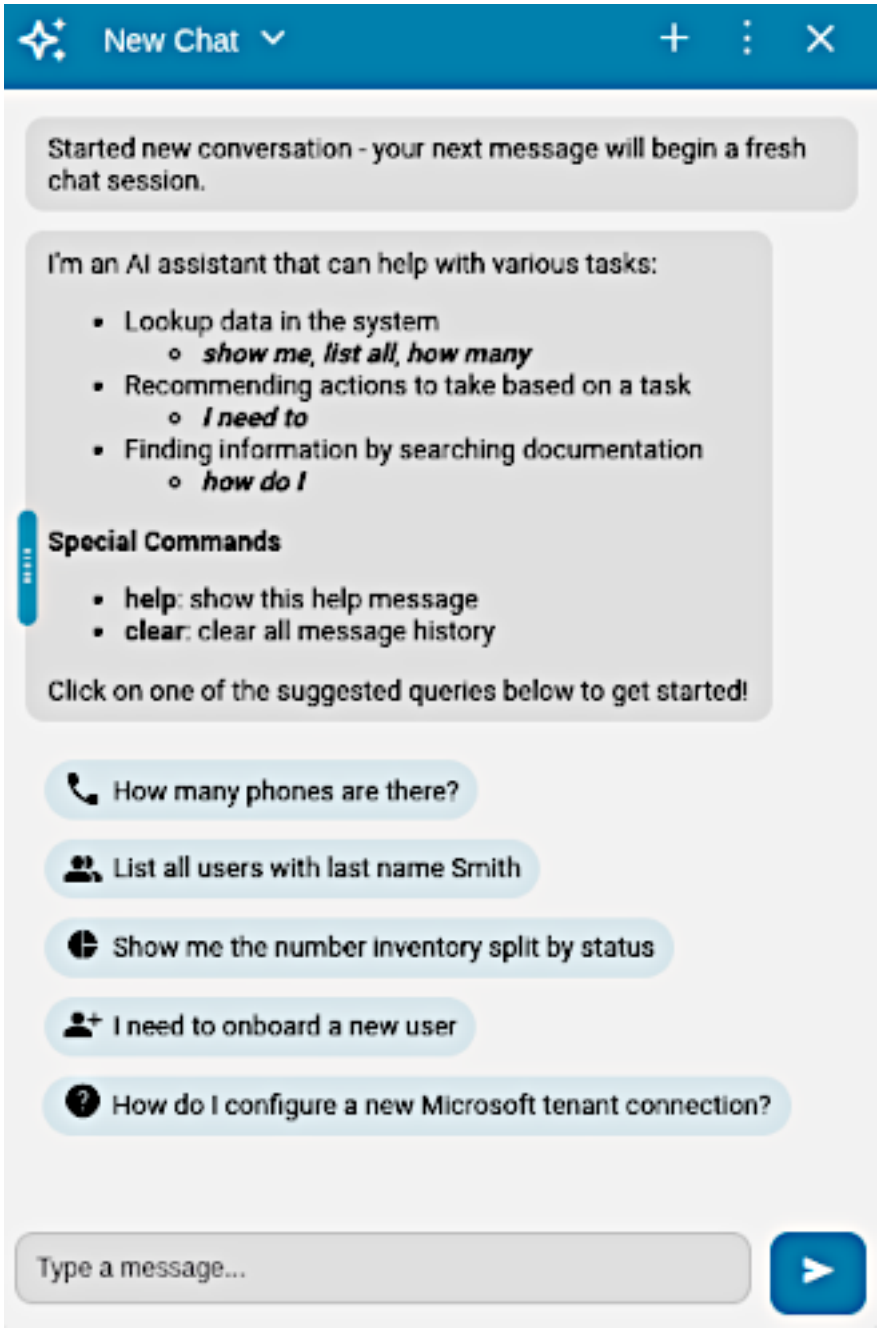
2. In the chat pane, select the Menu icon (3 dots) adjacent to the **New Chat** title to display chat history, size and help options for using Wingman Chat:

Copyright © 2025 VisionOSS Limited. All rights reserved.



You can also resize the chat pane by dragging the resize button in the left frame. The help menu item opens a list of instruction types and examples that can be selected to test the Wingman response.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.

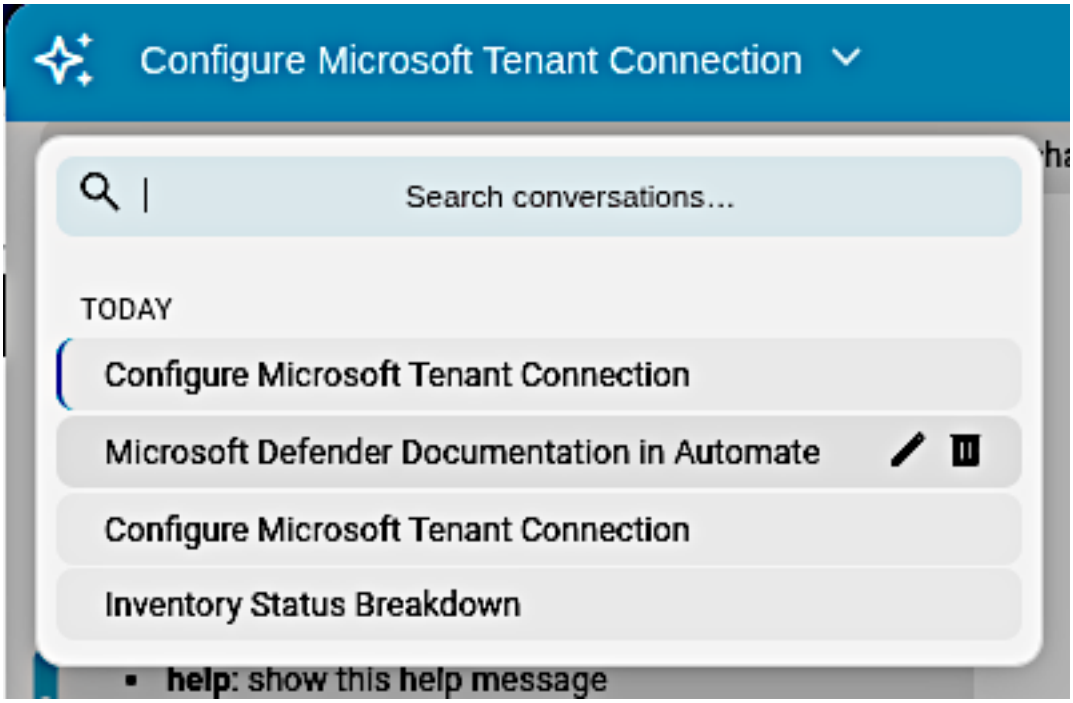
Conversation context and chat history

Wingman retains the *context* of the current conversation when follow-up questions are asked. For example, if a question is: “many phones?”, then a follow-up question: “by site” will be interpreted *within the context* of phones, in other words, “how many phones by site”.

A user’s *chat history* (up to 100 conversations) is available to the user in the **Chat History** drop-down.

This user chat history is persistent across sessions and is grouped in **TODAY**, **THIS WEEK** and **OLDER** lists.

Chat history entries can be searched and managed (deleted and re-used), allowing for access to useful and repeatable queries.



Wingman task types

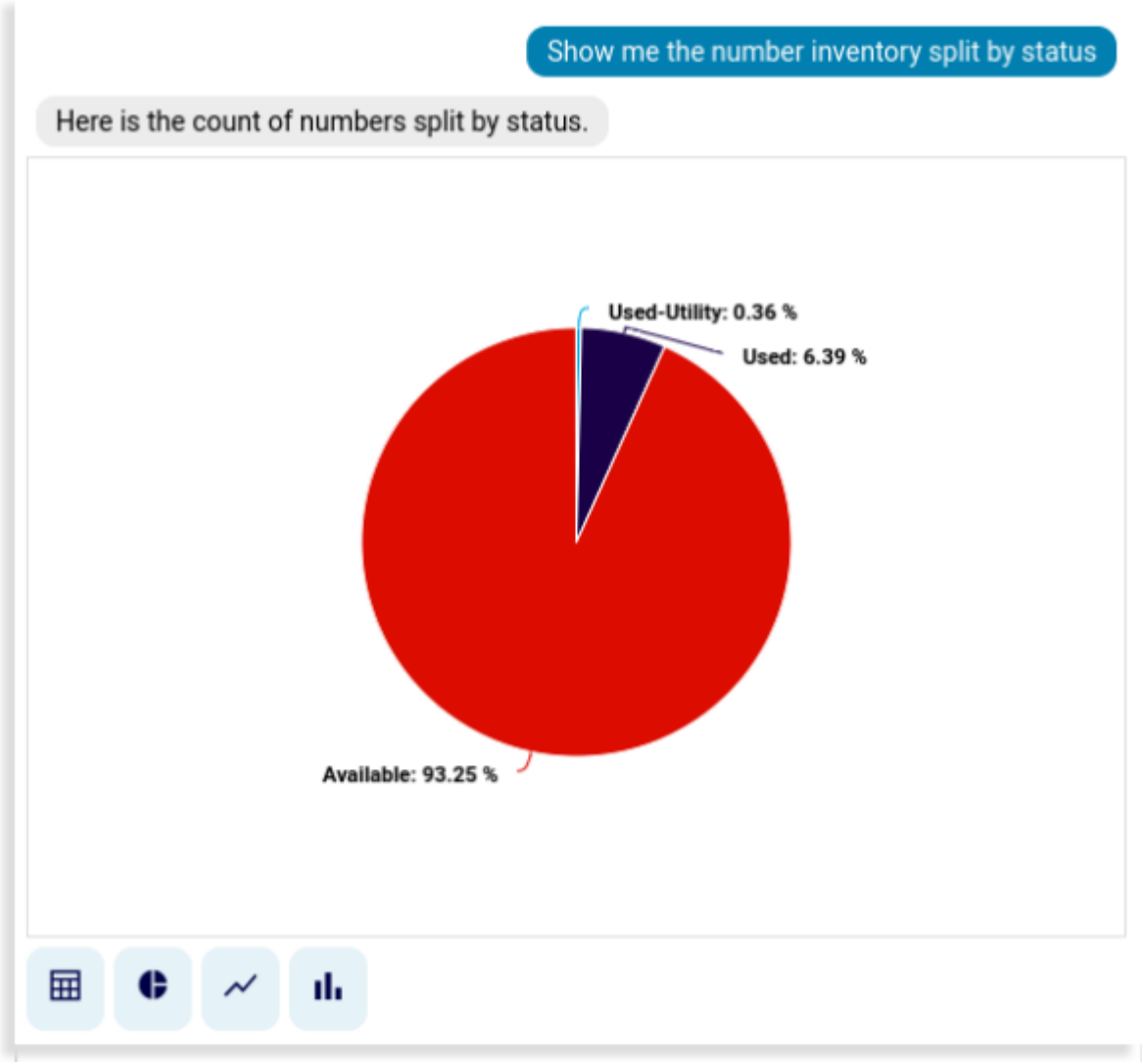
Three types of tasks can be carried out - each selected by using an appropriate *prefix phrase* in your chat input:

Show me/List all/How many/Troubleshooting

Look up data on the platform.

- For “Show me” questions, the reply can be rendered in a chart.

Copyright © 2025 VisionOSS Limited. All rights reserved.



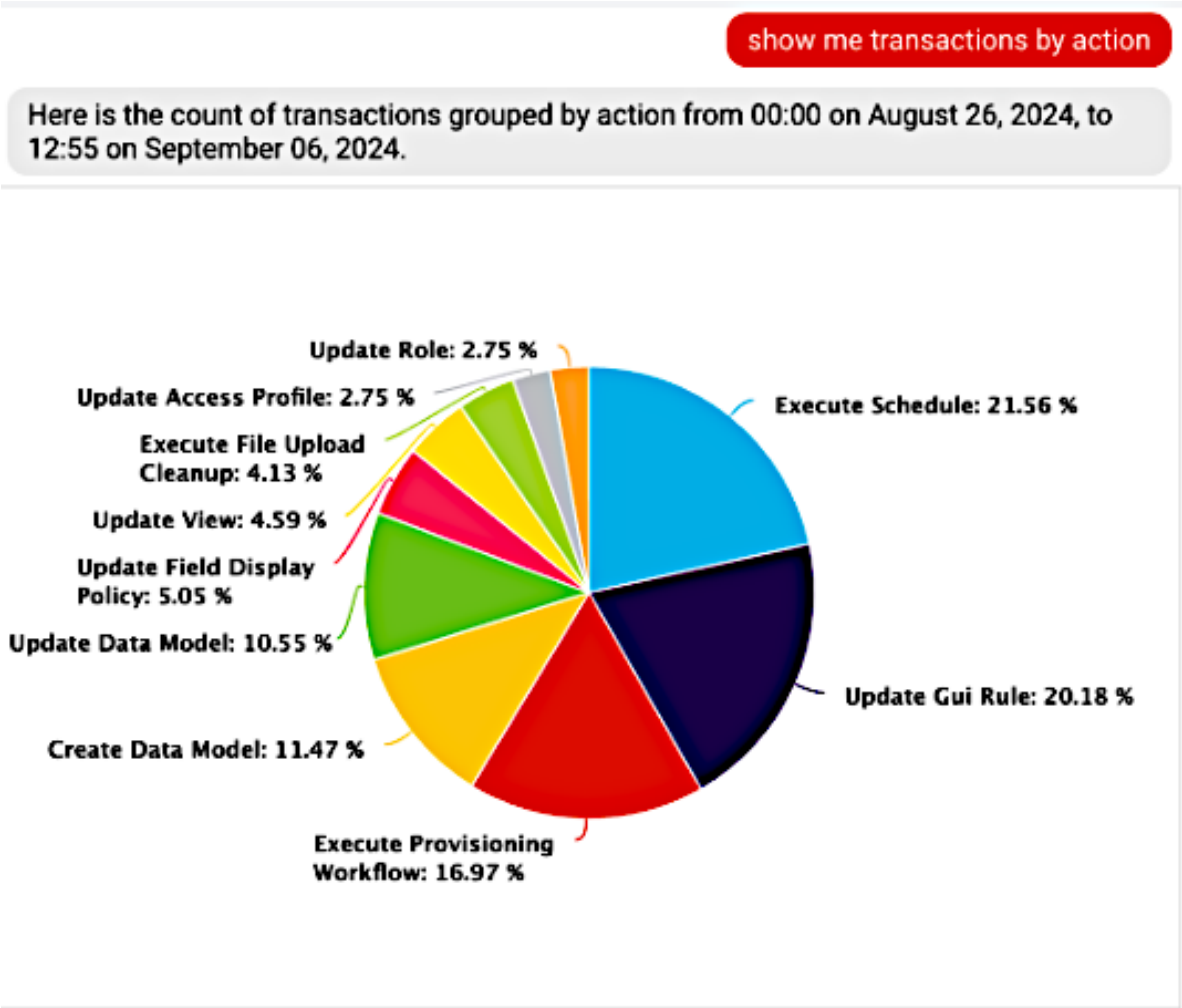
Date ranges can also be included into questions, for example: “show me transactions for this week”. The list below provides an indication of the calculation of the date range based on the phrase in the question:

- today: from 00:00:00 (UTC) to 23:59:59 (UTC) of the current day.
- yesterday: from 00:00:00 (UTC) to 23:59:59 (UTC) of the previous day, in other words, the full 24 hour period of the previous day.
- last week: from 00:00:00 (UTC) last Monday to Sunday 23:59:59 (UTC).
- last month: from 00:00:00 (UTC) of the first day of the preceding month to 23:59:59 (UTC) of the last day of the preceding month.
- last year: from 00:00:00 (UTC) of the first day of the previous year to 23:59:59 (UTC) of the last day of the previous year.
- this week: from 00:00:00 (UTC) of the first day of the current week to 23:59:59 (UTC) of the last day of the current week.
- this month: from 00:00:00 (UTC) of the first day of the current month to 23:59:59 (UTC) of the last day of the current month.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- this year: from 00:00:00 (UTC) of the first day of the current year to 23:59:59 (UTC) of the last day of the current year.
- since <specified date>: from 00:00:00 (UTC) of the specified date to 23:59:59 (UTC) of the current day.
- since <phrase>: Match start date time to the phrase, but end date must be today's date time. Examples:
  - since last week: from 00:00:00 (UTC) last Monday to today's date.
  - since yesterday: from 00:00:00 (UTC) to 23:59:59 (UTC) of the previous day to today's date.

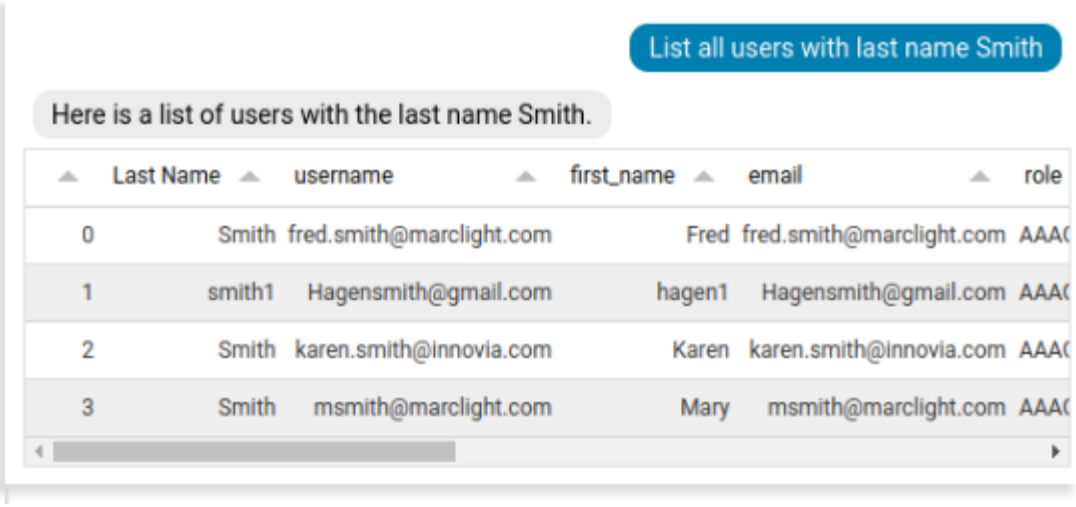
When queries are made without an explicit date range, the default behaviour is "since last week", for example, if a query was made on September 6th, 2024 at 12:55 UTC:



Icons below replies show options to change the chart or output format.

- For "How many" questions, Wingman by default responds by showing a bar chart with the count of the data found.
- For "List all" questions, Wingman by default responds by showing a table with the data found.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- Questions can also be asked about *transactions*, for example:
  - Are there any failed transactions?
  - Why did it fail?
  - Which transactions are there?
  - Show me the logs of all severities
- *Troubleshooting* questions can be asked whereby Wingman will follow a detailed playbook to provide a structured problem diagnosis and report. For example, a question such as:

  "Investigate bad call for user Angela Hill over 365 days"

  This will return a detailed report for the period as well as troubleshooting steps and possible solutions, as shown in the images below:

Copyright © 2025 VisionOSS Limited. All rights reserved.

A user reported a bad call

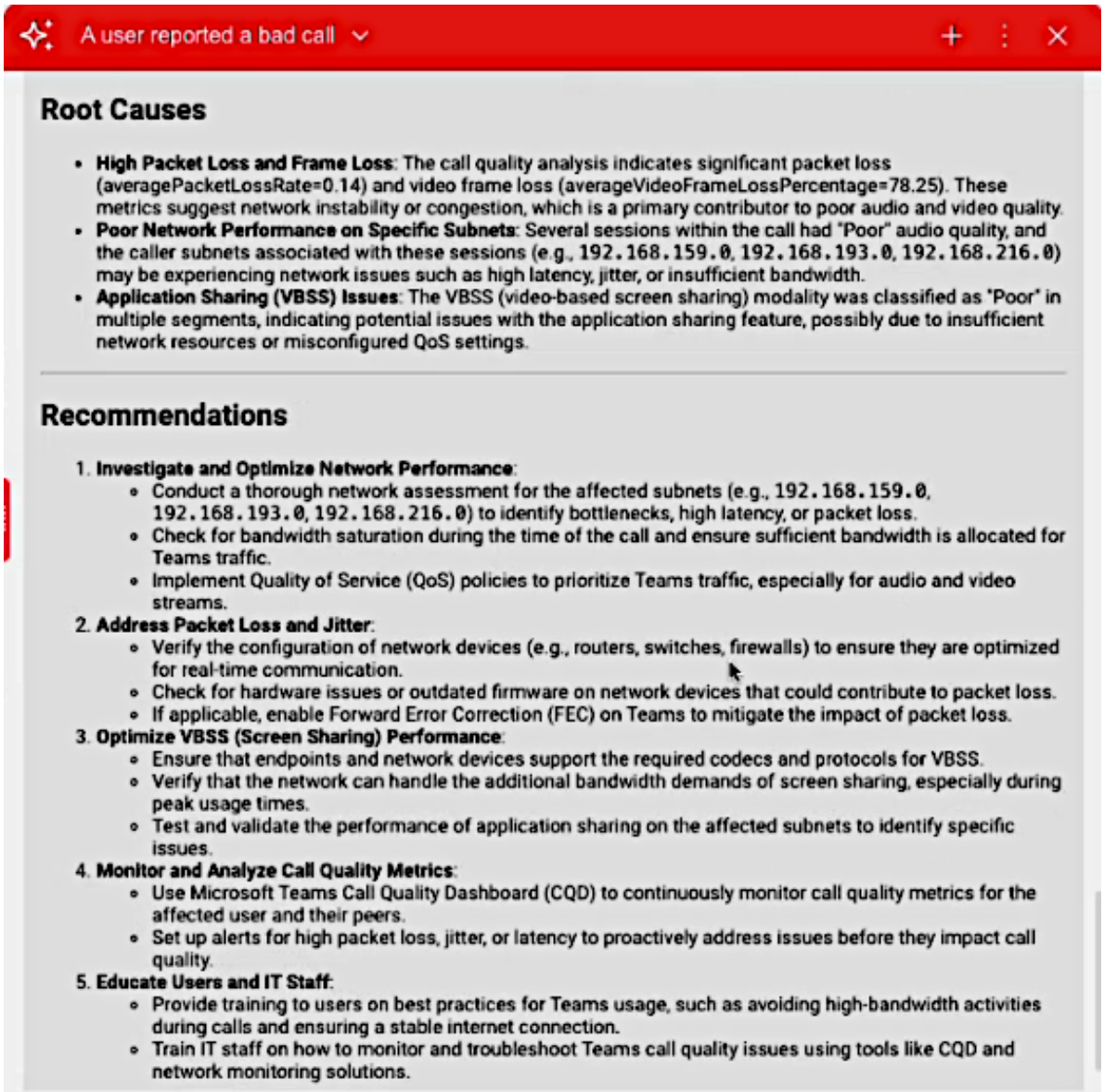
Summary

The analysis followed the 'Teams Call Quality Diagnosis' playbook, which is designed to diagnose poor teams calling experience for a specific user by analyzing call records, network conditions, and comparing against baselines. 5 steps were executed to gather and analyze relevant data.

Detailed Findings

- **Step 1**: [{'organizer_userprincipalname': "b'Angela.Hill@visionoss-dev.info'", 'organizer_displayname': "b'Angela Hill'", 'organizer_id': "b'9fba6ba7-def2-4b71-82d8-305988930508'", 'tenantname': "b'muted874-b877-4b29-b2d9-e521b8067muted'"}]
- **Step 2**: [{'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'startdatetime': "b'2025-09-02T16:45:50.643Z'", 'enddatetime': "b'2025-09-02T17:17:50.643Z'", 'duration': 1920, 'audio_quality': "b'Poor'", 'video_quality': "b'Na'", 'session_failure_count': 0, 'participant_count': 29, 'modality': "b'audio,videoBasedScreenSharing'", 'quality_info': "b'Audio classified as Poor: packetUtilization=99544.00, averageRoundTripTime=0.28, averagePacketLossRate=0.14, averageJitter=0.00, VBSS classified as Poor: averageVideoFrameLossPercentage=78.25'"}]
- **Step 3**: [{'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'83c7167c-4db2-470d-9557-c7985912902b'", 'caller_subnet': "b'192.168.12.0,192.168.176.0,192.168.202.0'", 'callee_subnet': "b''", 'audio_quality': "b'Good'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'daf466fa-f5b7-4caa-b60b-fd35caff076d'", 'caller_subnet': "b'192.168.126.0,192.168.176.0,192.168.241.0'", 'callee_subnet': "b''", 'audio_quality': "b'Good'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'93aa1856-aee9-432c-b949-19b3a6fd191a'", 'caller_subnet': "b'192.168.159.0,192.168.193.0,192.168.216.0'", 'callee_subnet': "b''", 'audio_quality': "b'Poor'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'56d578e6-c70c-4b31-a870-812623a22c80'", 'caller_subnet': "b'192.168.196.0,192.168.210.0,192.168.227.0'", 'callee_subnet': "b''", 'audio_quality': "b'Poor'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'65fac80f-140a-49c4-b866-eda6469144db'", 'caller_subnet': "b'192.168.209.0,192.168.238.0,192.168.58.0'", 'callee_subnet': "b''", 'audio_quality': "b'Good'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'3c5f3033-0b18-4b53-a4d6-264074874835'", 'caller_subnet': "b'192.168.12.0,192.168.176.0,192.168.252.0'", 'callee_subnet': "b''", 'audio_quality': "b'Good'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'8826ff20-1f06-4e46-b623-f549131cb6a2'", 'caller_subnet': "b'192.168.198.0,192.168.233.0,192.168.48.0'", 'callee_subnet': "b''", 'audio_quality': "b'Poor'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'0252301c-2ab6-4ab1-a80b-2db57307e424'", 'caller_subnet': "b'192.168.24.0,192.168.244.0,192.168.25.0'", 'callee_subnet': "b''", 'audio_quality': "b'Good'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'c3aa2a15-968d-445d-9019-5460dc656e9d'", 'caller_subnet': "b'192.168.128.0,192.168.145.0,192.168.4.0'", 'callee_subnet': "b''", 'audio_quality': "b'Poor'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'c3b05e69-05a6-4c7b-8547-3a582296ae51'", 'caller_subnet': "b'192.168.17.0,192.168.32.0,192.168.76.0'", 'callee_subnet': "b''", 'audio_quality': "b'Good'", 'video_quality': "b'Na'", 'failure_reason': "b''", 'failure_stage': "b''"}, {'callid': "b'cb9e7de3-d8ba-42c6-9d7d-f47cad907645'", 'sessionid': "b'05e317fc-fb0c-43d3-ac3e-effd2a3988b4'", 'caller_subnet':

Copyright © 2025 VisionOSS Limited. All rights reserved.



A user reported a bad call

Root Causes

- **High Packet Loss and Frame Loss**: The call quality analysis indicates significant packet loss (averagePacketLossRate=0.14) and video frame loss (averageVideoFrameLossPercentage=78.25). These metrics suggest network instability or congestion, which is a primary contributor to poor audio and video quality.
- **Poor Network Performance on Specific Subnets**: Several sessions within the call had "Poor" audio quality, and the caller subnets associated with these sessions (e.g., `192.168.159.0`, `192.168.193.0`, `192.168.216.0`) may be experiencing network issues such as high latency, jitter, or insufficient bandwidth.
- **Application Sharing (VBSS) Issues**: The VBSS (video-based screen sharing) modality was classified as "Poor" in multiple segments, indicating potential issues with the application sharing feature, possibly due to insufficient network resources or misconfigured QoS settings.

Recommendations

1. **Investigate and Optimize Network Performance**:
   - Conduct a thorough network assessment for the affected subnets (e.g., `192.168.159.0`, `192.168.193.0`, `192.168.216.0`) to identify bottlenecks, high latency, or packet loss.
   - Check for bandwidth saturation during the time of the call and ensure sufficient bandwidth is allocated for Teams traffic.
   - Implement Quality of Service (QoS) policies to prioritize Teams traffic, especially for audio and video streams.
2. **Address Packet Loss and Jitter**:
   - Verify the configuration of network devices (e.g., routers, switches, firewalls) to ensure they are optimized for real-time communication.
   - Check for hardware issues or outdated firmware on network devices that could contribute to packet loss.
   - If applicable, enable Forward Error Correction (FEC) on Teams to mitigate the impact of packet loss.
3. **Optimize VBSS (Screen Sharing) Performance**:
   - Ensure that endpoints and network devices support the required codecs and protocols for VBSS.
   - Verify that the network can handle the additional bandwidth demands of screen sharing, especially during peak usage times.
   - Test and validate the performance of application sharing on the affected subnets to identify specific issues.
4. **Monitor and Analyze Call Quality Metrics**:
   - Use Microsoft Teams Call Quality Dashboard (CQD) to continuously monitor call quality metrics for the affected user and their peers.
   - Set up alerts for high packet loss, jitter, or latency to proactively address issues before they impact call quality.
5. **Educate Users and IT Staff**:
   - Provide training to users on best practices for Teams usage, such as avoiding high-bandwidth activities during calls and ensuring a stable internet connection.
   - Train IT staff on how to monitor and troubleshoot Teams call quality issues using tools like CQD and network monitoring solutions.

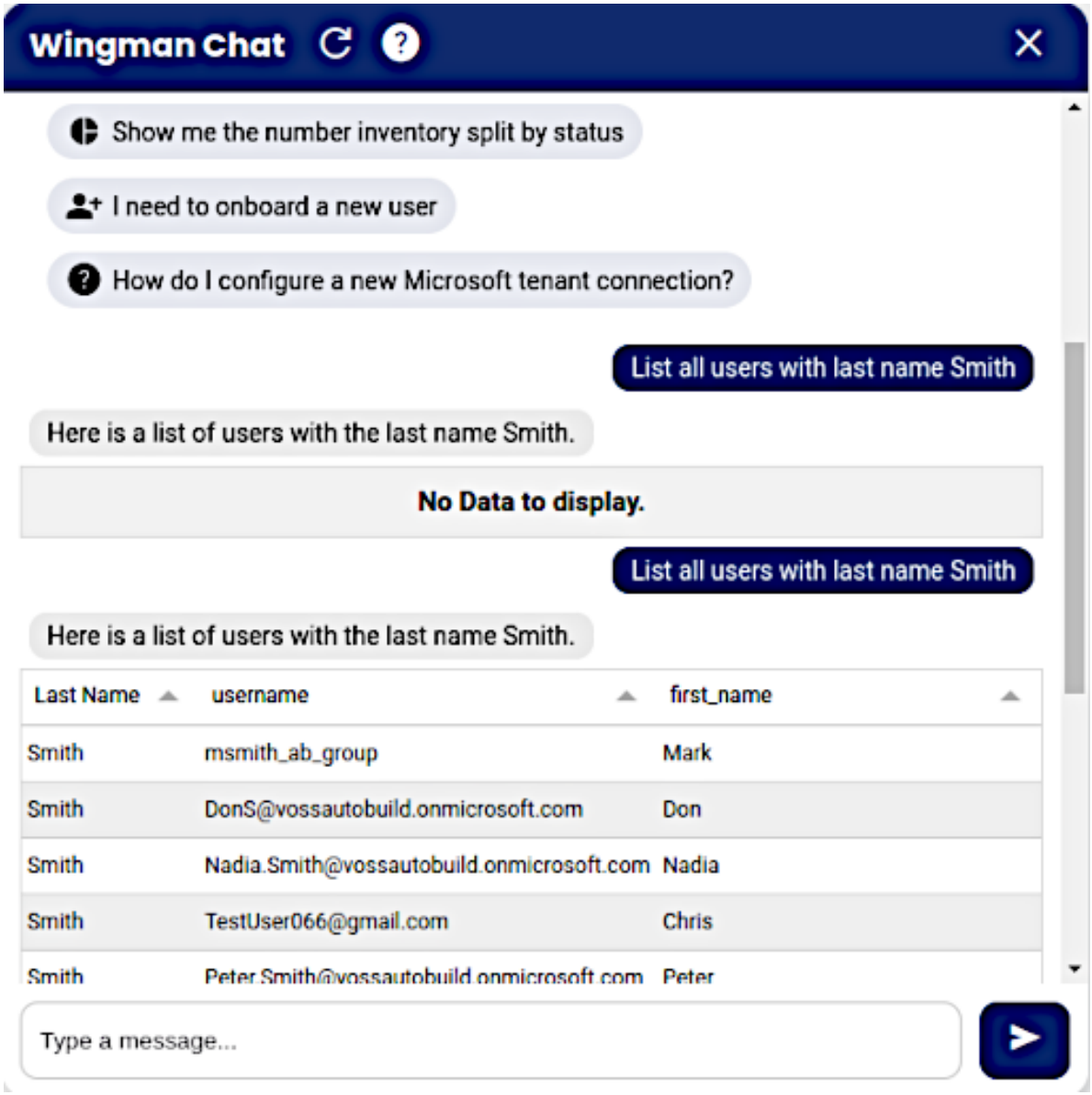
Note:

- Wingman will use the permitted dashboard resources in a user's access profile as valid data lookup options.
- Data sources are: *Wingman data sources*. If a question does not refer to these sources, Wingman responds with the friendly names of these sources as available data sources.
- Count results (in tables or charts) are dependent on the *hierarchy* at which the user is, as well as the user role permissions when using the Wingman chat interface.

  The example below shows responses where an admin user navigates down to a site level hierarchy and asks: "List all users with last name Smith" (result: **No Data to display.**) and then navigates to a

Copyright © 2025 VisionOSS Limited. All rights reserved.

provider level and repeats the question (result: table):

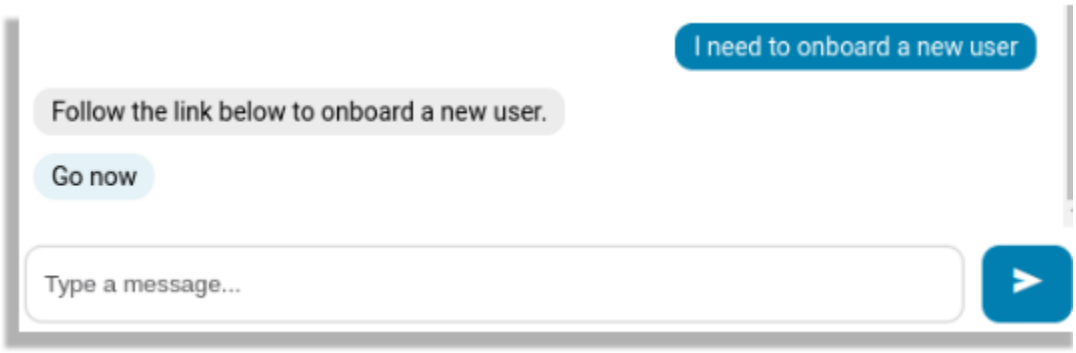


- "How many" and "Show me" questions use the Insights data source that is available from release 24.1 and is also used to create dashboard widgets. For details, see: *Introduction to Automate dashboards*. This means that while questions for data can be refined by also specifying a single provider, reseller or customer or site hierarchy name in the question, questions do not return data when a question specifies all hierarchies.

Copyright © 2025 VisionOSS Limited. All rights reserved.

I need/want to

Wingman Chat responds with action recommendations or instructions and with a **Go now** link - based on user's menu layout - to the appropriate form, dashboard or feature.



The **Go now** links use the following models for the matching tasks:

- Onboard a new multi-vendor user

  `view/AddSubscriberFromProfile`
- Onboard a new Microsoft user

  `view/MicrosoftSubscriberQas`
- Onboard a new Cisco user

  `view/QuickSubscriber`
- Create a new Cisco phone

  `view/AddPhone`
- Add a range of numbers to the number inventory

  `view/NumberInventoryRangeMgmtVIEW`

How do I/What is/Tell me about/Explain

Formulate questions that start with these words to ask documentation questions about the product.

Wingman responds with:

- a summarized answer
- a set of generated reference links to the full documentation on the documentation portal that may be relevant

Copyright © 2025 VisionOSS Limited. All rights reserved.

how do i manage microsoft defender in automate

To manage Microsoft Defender in Automate, you can follow these steps:

1. **Enable Microsoft Defender**: Go to the Global Settings and enable Microsoft Defender for Office and/or Endpoint. This will also create a new Microsoft Defender administrator menu item with links to related dashboards for easier management.
2. **Configure a Microsoft Tenant**: Set up a Microsoft tenant in Automate. This configuration will sync Microsoft Defender data to Automate.
3. **Data Collection and Sync**: Once the tenant configuration is saved, Automate will create a data collection instance that syncs data from the tenant. This includes various models such as SecureScore, Alerts, Incidents, and more.
4. **Access Dashboards**: Use the administrator interface to access dashboards for managing data related to Defender for Endpoint and Defender for Office. This includes security management and actions.
5. **Manage Policies and Quarantine Messages**: For Defender for Office, you can manage email quarantine messages, Safe Attachment Policies, and Safe Link Policies, as well as handle requests for policy updates.

For detailed steps, refer to the specific sections on Microsoft Defender setup, sync, and overbuild in the Automate documentation.

Source link 1 Source link 2 Source link 3

explain the user audit feature in automate

The user audit feature in Automate addresses issues related to user and service associations within the system. It helps identify problems such as:

- Users being absent from the system.
- Users not being properly associated with the services present in the system.
- Users existing without corresponding service associations.
- Users being located at a different site from their associated service users.

These issues can lead to performance degradation, inaccurate workflows, and incorrect license audit data.
Automate provides both a command and a scheduled action to carry out the user audit. The System User Audit link on the default System Configuration dashboard allows administrators to run a user audit on users and their associated services. When running the audit, administrators can select a hierarchy and choose specific audit actions, such as creating missing users, updating service statuses, or aligning user hierarchies.
Additionally, the system user audit runs automatically during system upgrades and is scheduled to run nightly. When executed as a service, a CSV report is generated to document the operations performed during the audit.

Source link 1 Source link 2

Copyright © 2025 VisionOSS Limited. All rights reserved.

Wingman data sources

The table describes the list of Automate data sources that are available to Wingman when **Show me**/**List all**/**How many** - type questions are asked.

Table 1: Wingman Data Sources

model_type	friendly_name
data/MonitoringCluster	Monitoring Platform Cluster
data/MonitoringQueue	Monitoring Transaction Queue
data/MonitoringSessions	Monitoring Sessions
data/MetricDatabaseCollectionStats	Monitoring Database Stats
data/LicenseAuditCounts	Automate License Counts
data/BaseSiteDAT	Site
data/CountLimit	Subscriber Count Limit
data/HcsDpDNE164AssociateDAT	E164 Number Association
data/HcsDpE164InventoryDAT	E164 Number Inventory
data/HcsEntitlementProfileDAT	Entitlement Profile
data/HierarchyNode	Hierarchy
data/InternalNumberInventory	Number Inventory
data/MicrosoftSubscriberQasStaging	Microsoft Subscriber Staging
data/User	User
device/cuc/User	Cisco CUC User
device/cuc/UserLicense	Cisco CUC User License
device/cuc/Callhandler	Cisco CUC Call Handler
device/cucm/CallPickupGroup	Cisco UCM Call Pickup Group
device/cucm/DeviceProfile	Cisco UCM Device Profile
device/cucm/Gateway	Cisco UCM Gateway
device/cucm/GatewaySccpEndpoints	Cisco UCM Gateway SCCP Endpoints
device/cucm/HcsLicense	Cisco UCM License
device/cucm/HuntList	Cisco UCM Hunt List
device/cucm/HuntPilot	Cisco UCM Hunt Pilot
device/cucm/LicensingResourceUsage	Cisco UCM Licensing Resource Usage
device/cucm/Line	Cisco UCM Line
device/cucm/LineGroup	Cisco UCM Line Group
device/cucm/Phone	Cisco UCM Phone
device/cucm/PhoneType	Cisco UCM Phone Type
device/cucm/RemoteDestination	Cisco UCM Remote Destination
device/cucm/RemoteDestinationProfile	Cisco UCM Remote Destination Profile
device/cucm/User	Cisco UCM User
device/pexip/Conference	Pexip Conference
device/pexip/ConferenceAlias	Pexip Conference Alias

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

model_type	friendly_name
device/msexchangeonline/UserMailbox	Microsoft Exchange Online User Mailbox
device/msgraph/MsolAccountSku	Microsoft O365 User SKU
device/msgraph/MsolUser	Microsoft O365 User
device/msteamsonline/CsAutoAttendant	Microsoft Teams Auto Attendant
device/msteamsonline/CsCallQueue	Microsoft Teams Call Queue
device/msteamsonline/CsOnlineUser	Microsoft Teams User
device/msteamsonline/CsTeamsClientConfiguration	Microsoft Teams Client Configuration
device/spark/Announcements	Webex Calling Announcements
device/spark/AutoAttendants	Webex Calling Auto Attendants
device/spark/CallParkExtensions	Webex Calling Call Park Extensions
device/spark/CallParkGroup	Webex Calling Call Park Group
device/spark/CallPickup	Webex Calling Call Pickup
device/spark/Device	Webex Calling Device
device/spark/HuntGroup	Webex Calling Hunt Group
device/spark/Group	Webex Calling Group
device/spark/License	Webex Calling License
device/spark/Place	Webex Calling Place
device/spark/Number	Webex Calling Number
device/spark/Schedules	Webex Calling Schedule
device/spark/Team	Webex Calling Team
device/spark/User	Webex Calling User
device/uccx/Agent	Cisco UCCX Agent
device/webex/User	Cisco Webex User

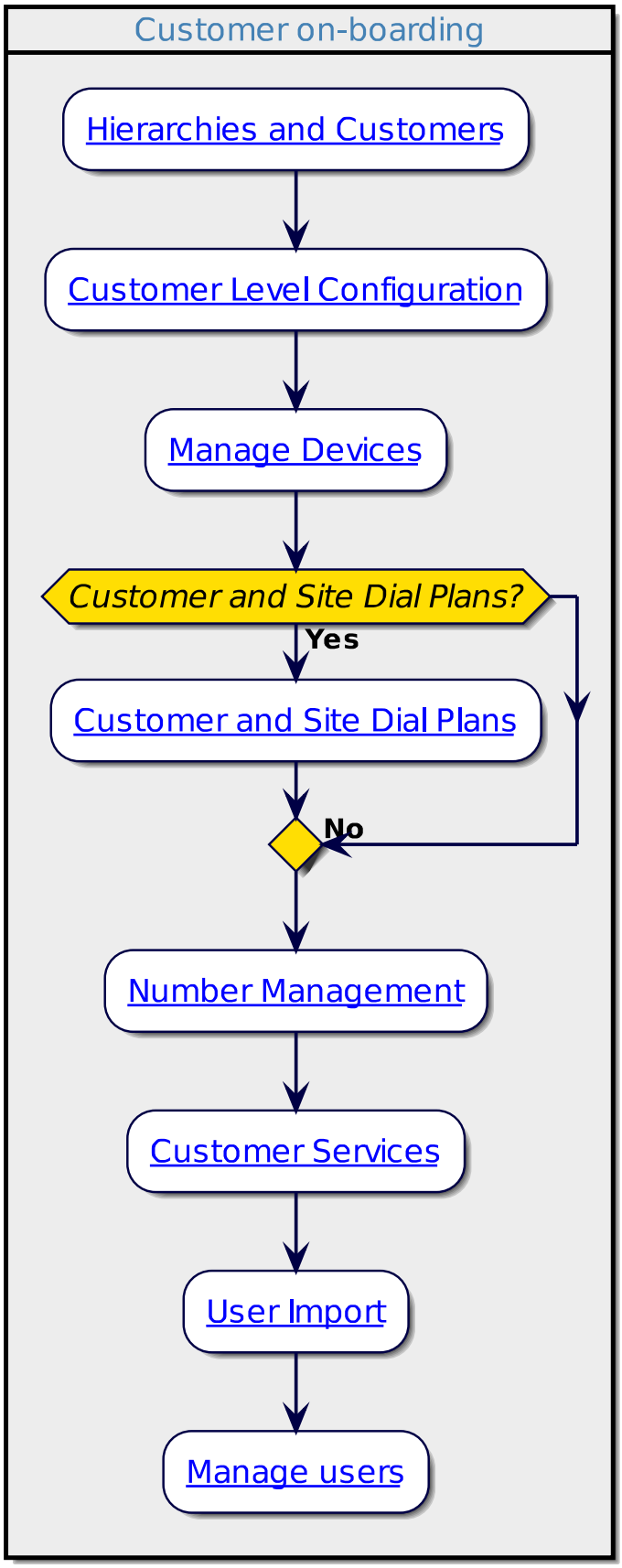
Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Quick Start Guides

3.1. Customer Onboarding Quick Start Guide (Multiple Vendors)

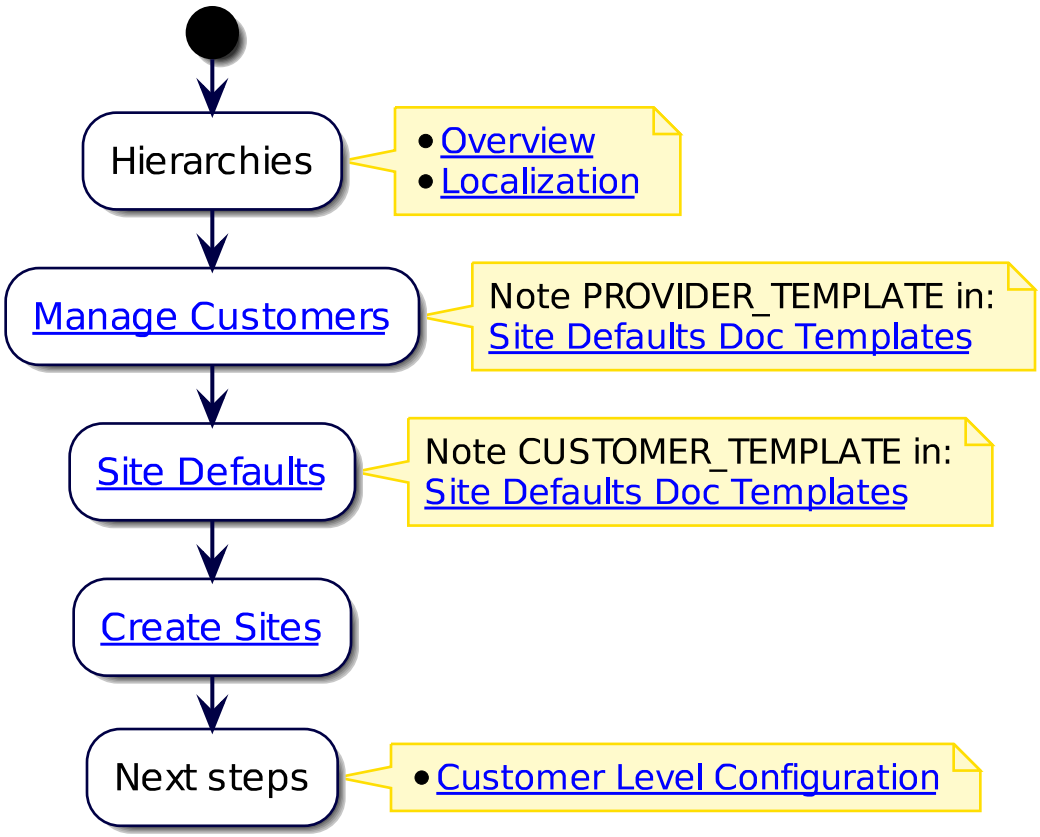
3.1.1. Overview

This quick start guide provides a walk through of the steps Provider admins can follow for a complete on-boarding of customers in a single of multi vendor deployment.



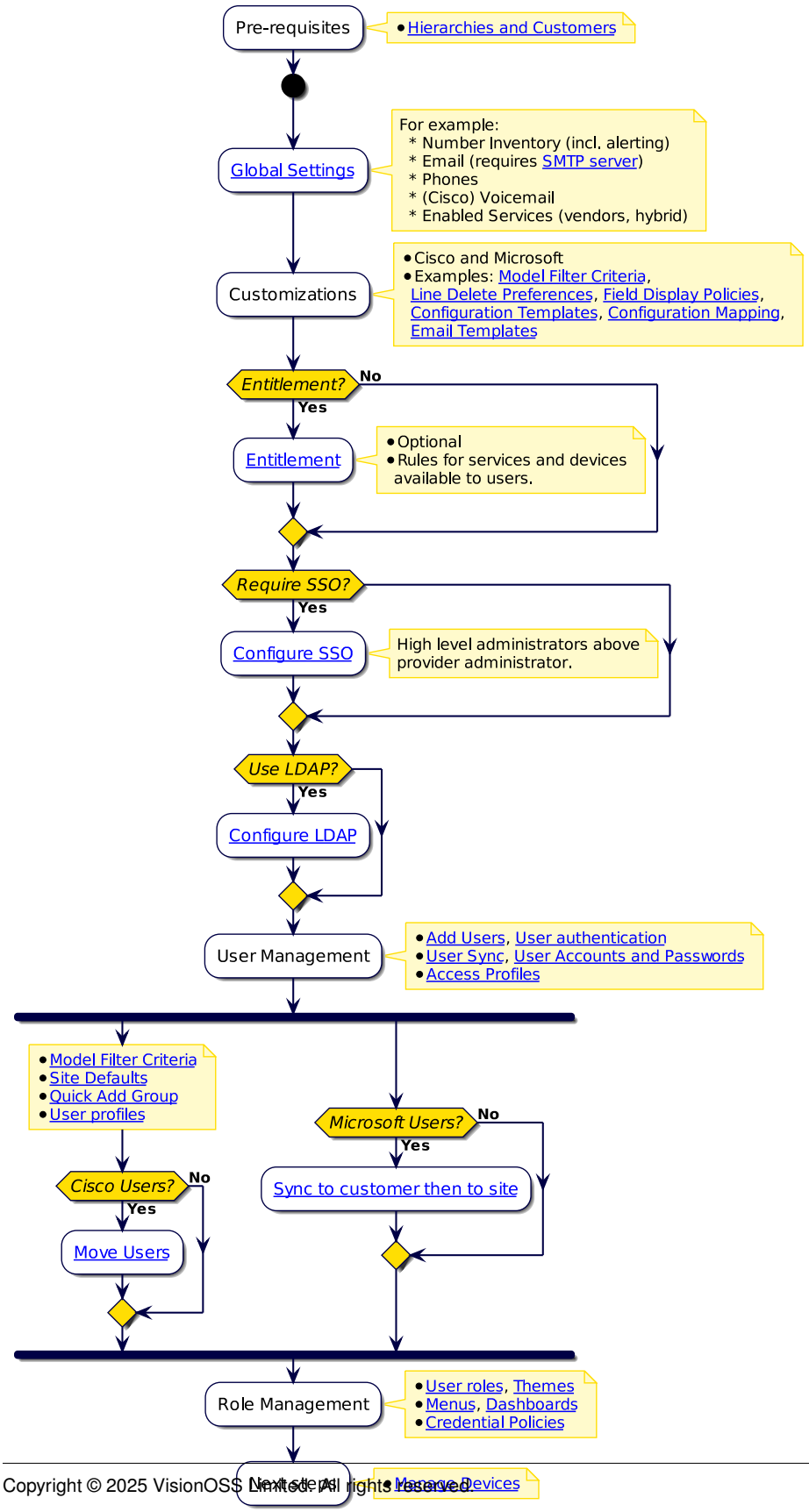
Copyright © 2025 VisionOSS Limited. All rights reserved.

3.1.2. Hierarchies and customers



Copyright © 2025 VisionOSS Limited. All rights reserved.

3.1.3. Customer-level configuration



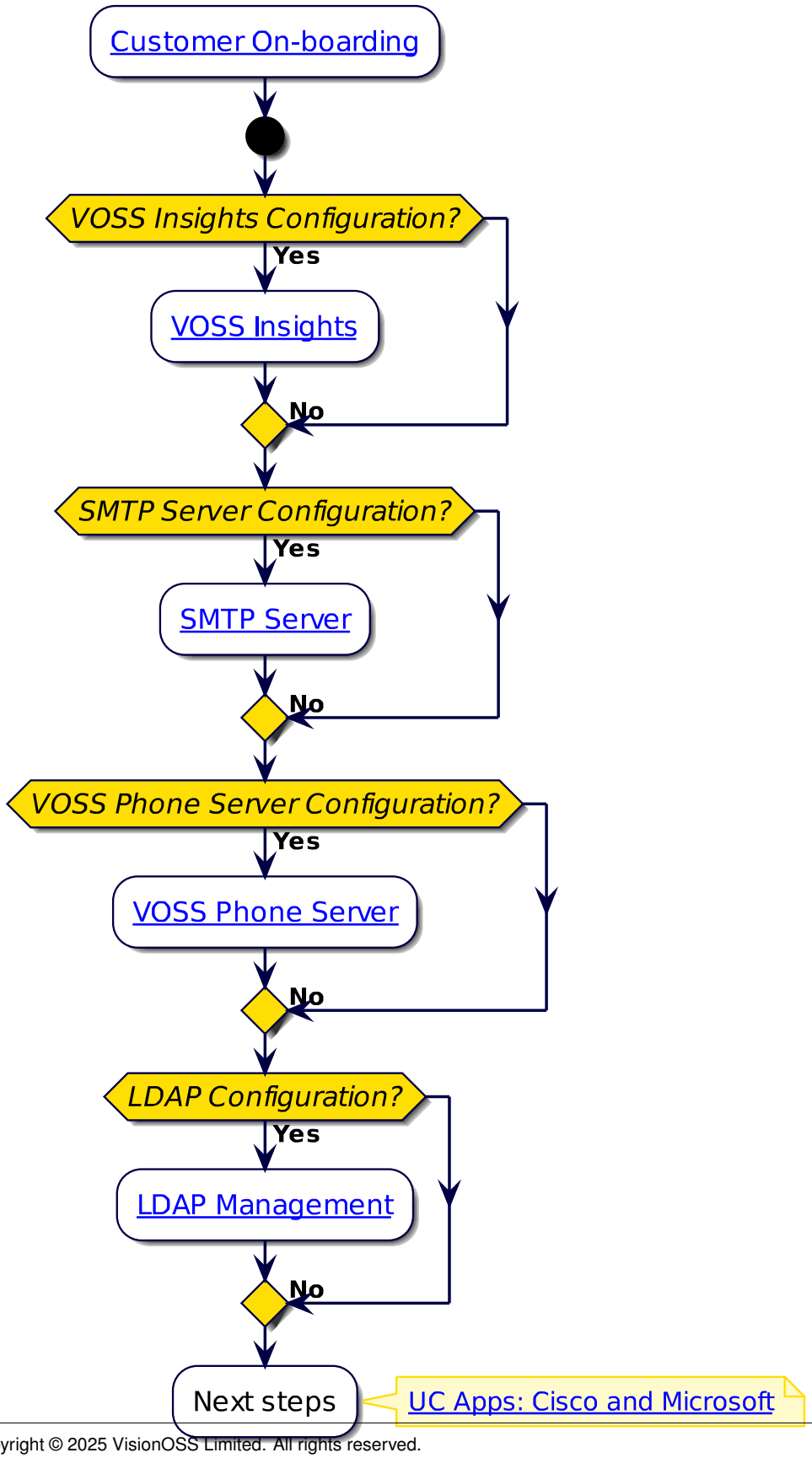
Copyright © 2025 VisionOSS Limited. All rights reserved.

3.1.4. Manage devices

- *General devices and Automate apps*
- *UC apps: Cisco, Microsoft, NDLs*

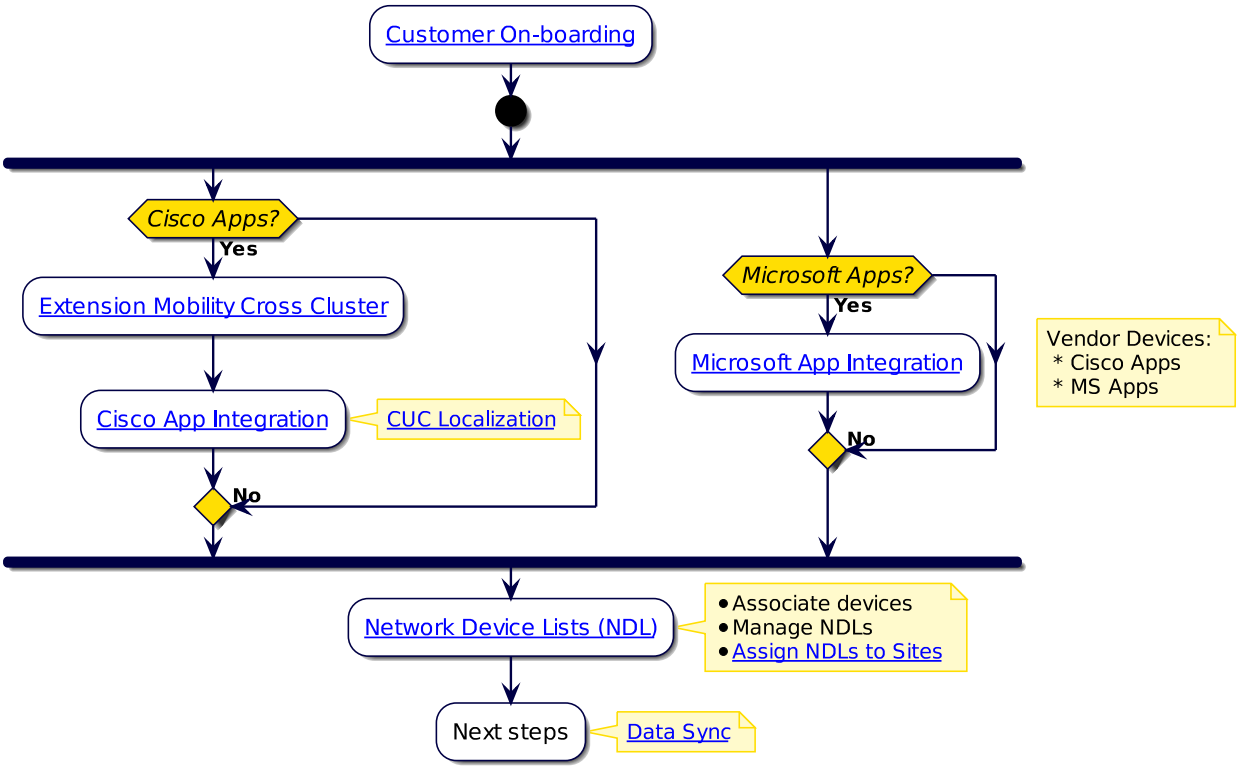
Copyright © 2025 VisionOSS Limited. All rights reserved.

General devices and Automate apps



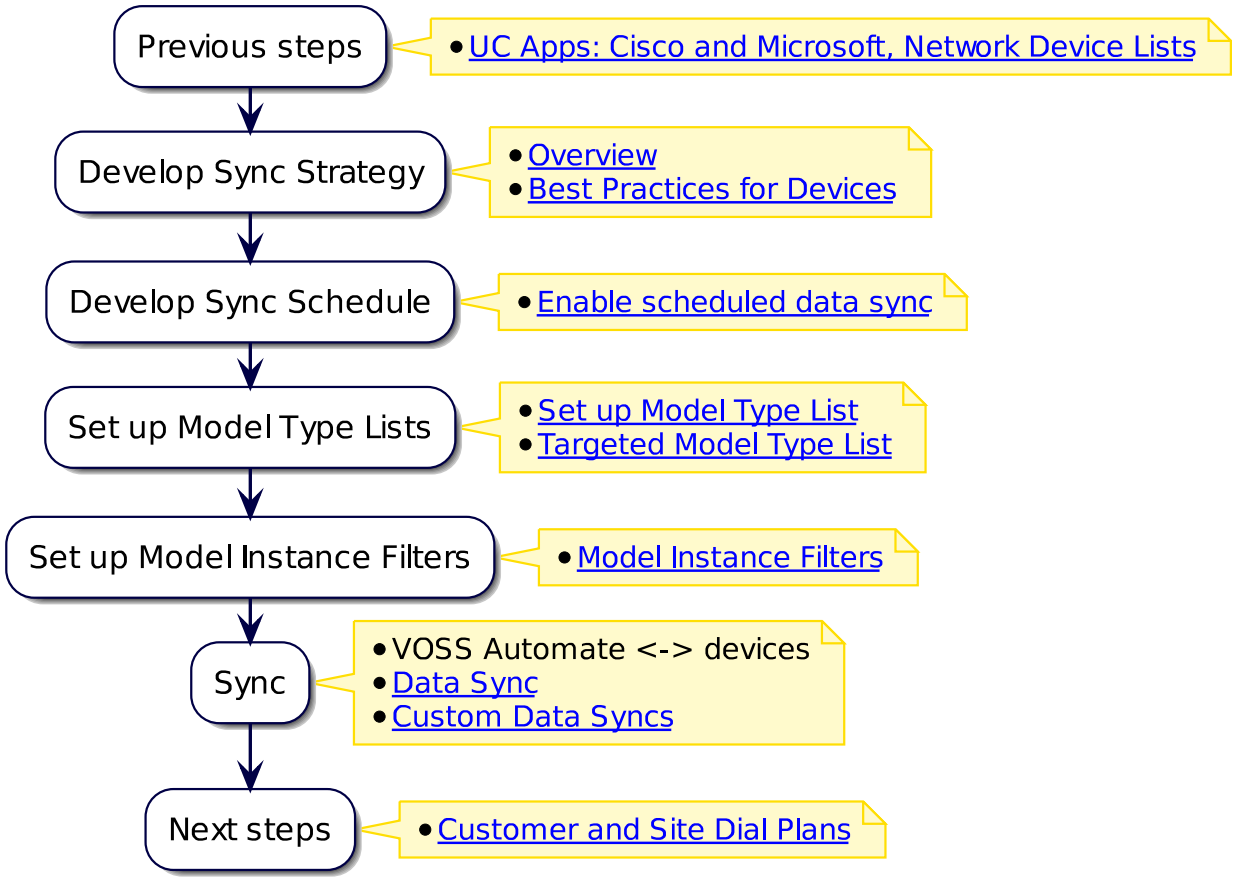
Copyright © 2025 VisionOSS Limited. All rights reserved.

UC apps: Cisco, Microsoft, NDLs

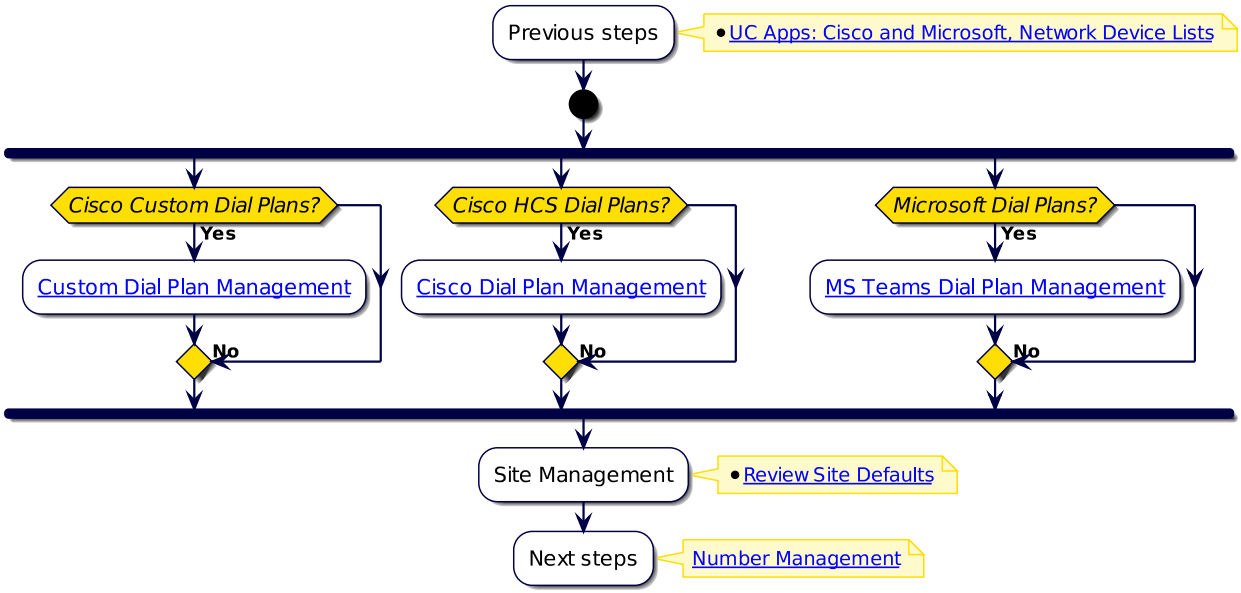


Copyright © 2025 VisionOSS Limited. All rights reserved.

Data sync

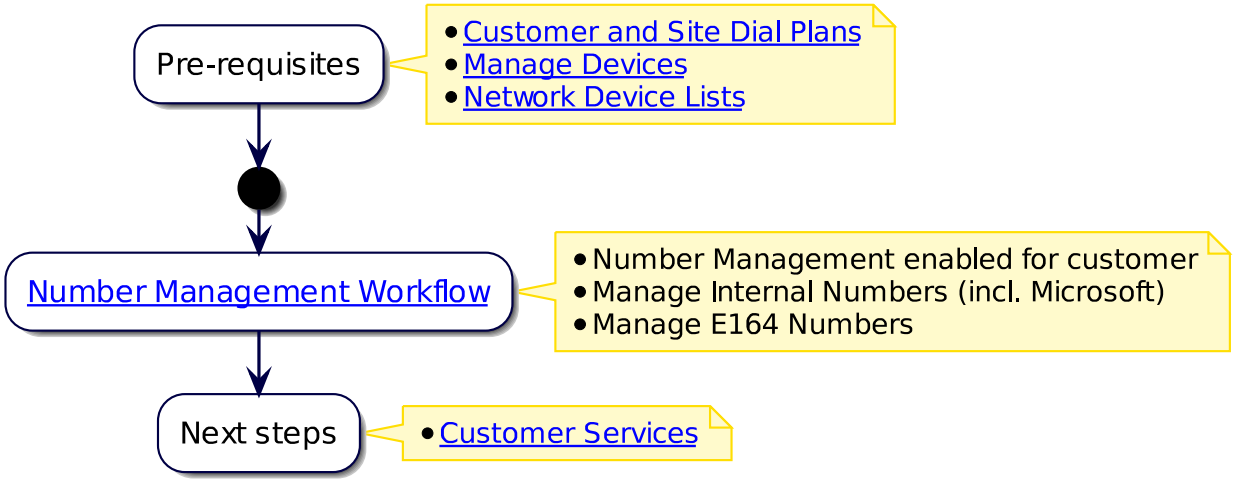


3.1.5. Customer and site dial plans

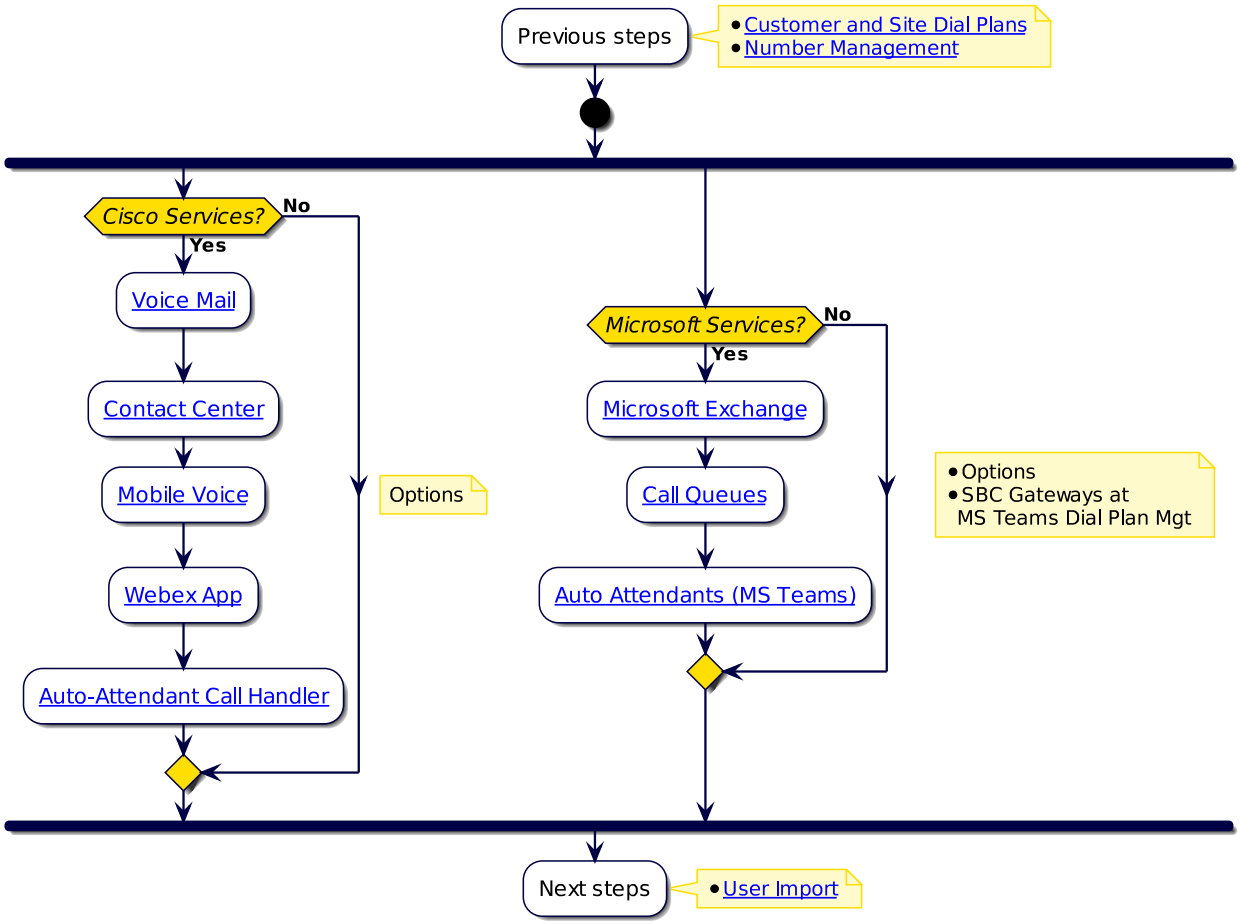


Copyright © 2025 VisionOSS Limited. All rights reserved.

3.1.6. Number management



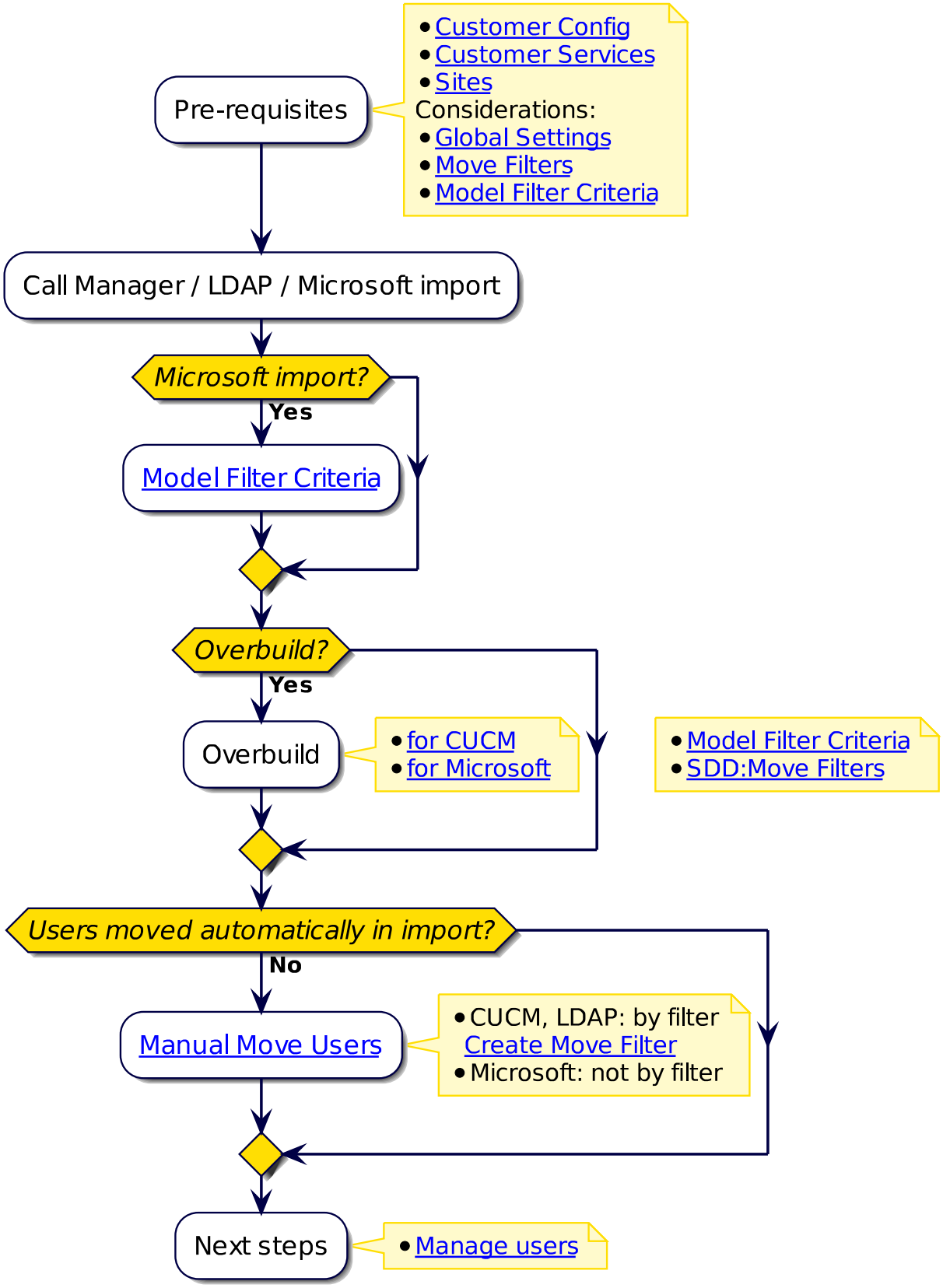
3.1.7. Customer services



Copyright © 2025 VisionOSS Limited. All rights reserved.

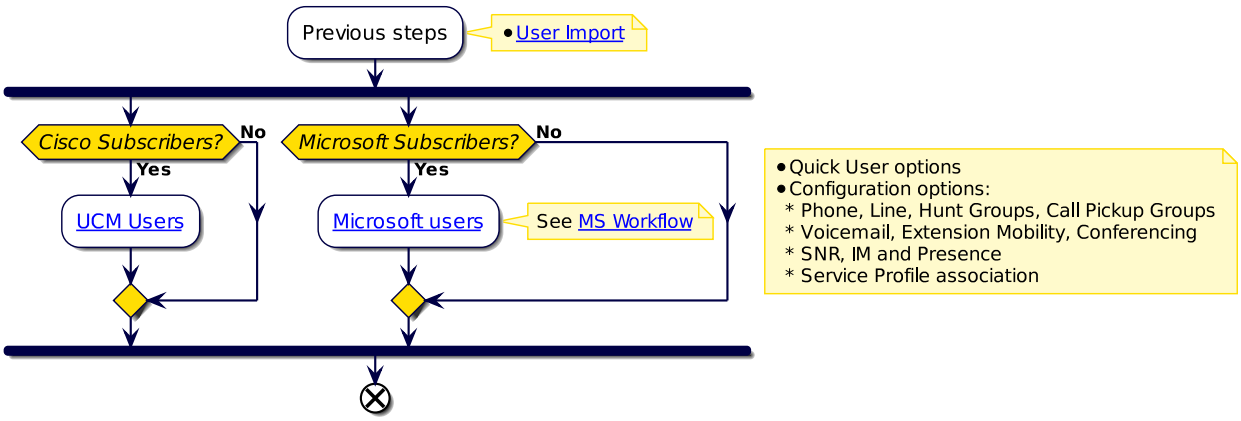
Copyright © 2025 VisionOSS Limited. All rights reserved.

3.1.8. User import



Copyright © 2025 VisionOSS Limited. All rights reserved.

3.1.9. Manage users



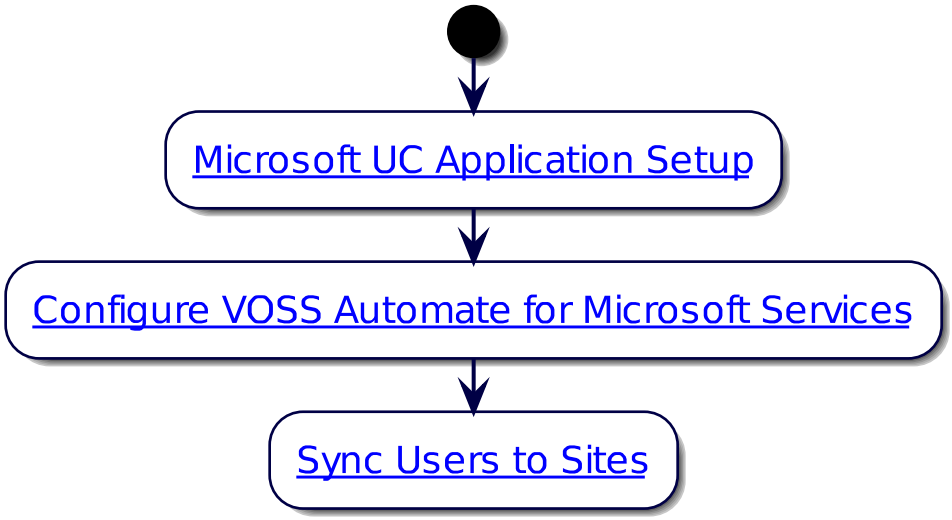
3.2. Microsoft Quick Start Guide for Automate

3.2.1. Overview

This quick start will guide you through the steps for setting up VOSS Automate for Microsoft.

The flowchart provides a high-level overview:

- *Step 1: Microsoft UC Application Setup*
- *Step 2: Configure Automate for Microsoft Services*
- *Step 3: Sync Microsoft Users to Sites*



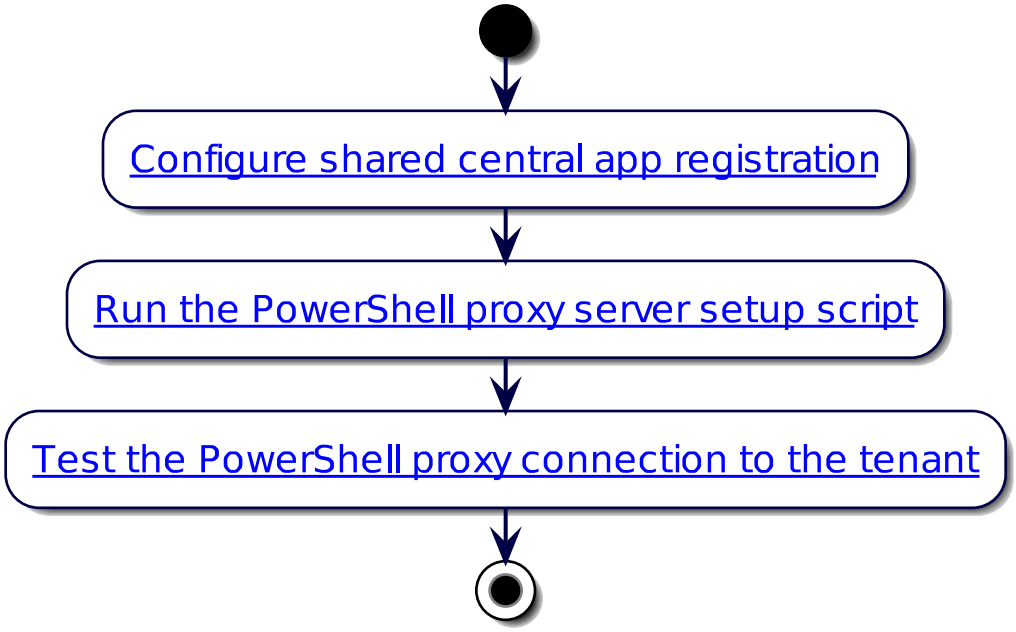
Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Introduction to Microsoft UC Integration* in the Core Feature Guide

3.2.2. Step 1: Microsoft UC Application Setup

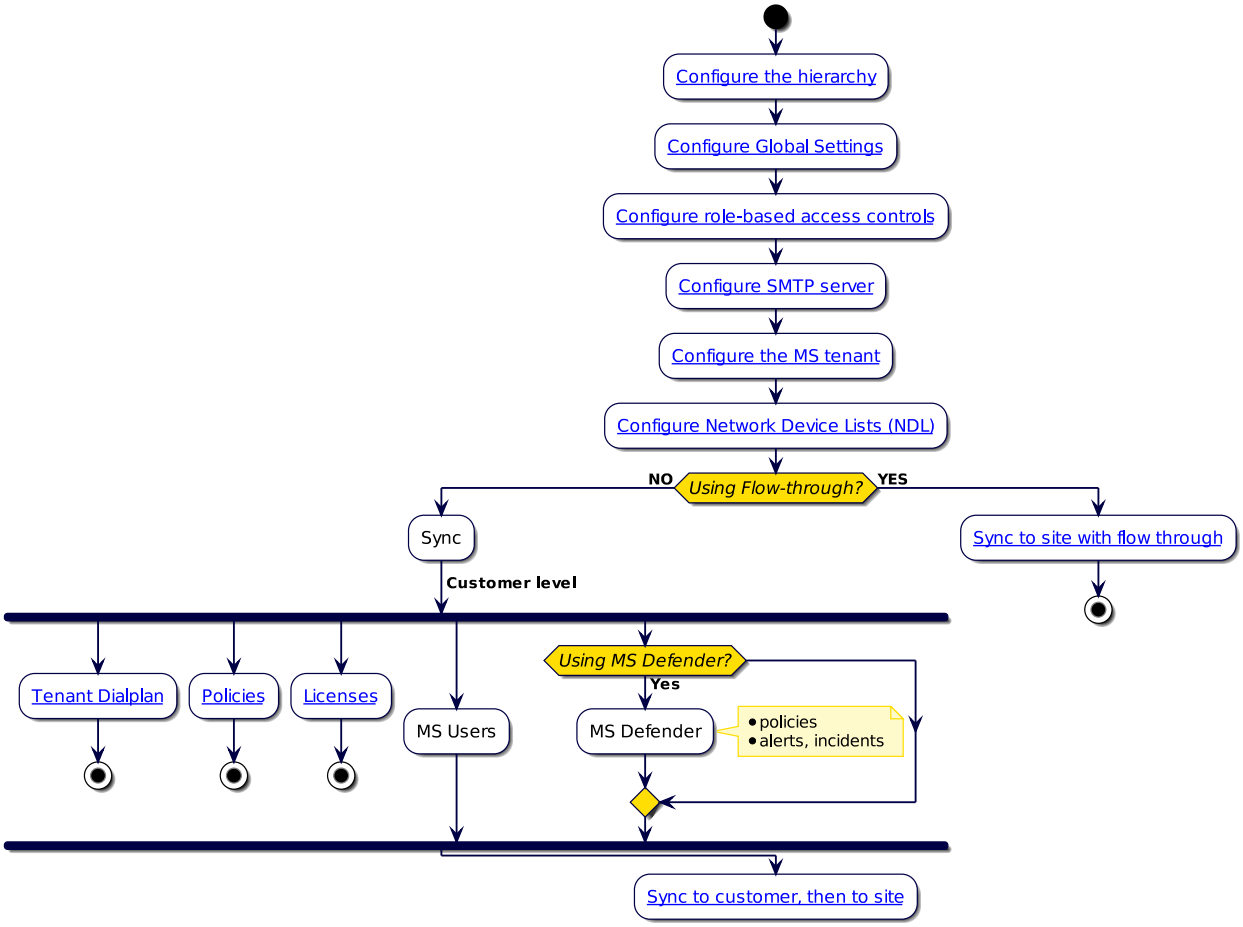
For details, see *Microsoft UC Application Setup*



3.2.3. Step 2: Configure Automate for Microsoft Services

For details, see *Configure Automate for Microsoft services*

Copyright © 2025 VisionOSS Limited. All rights reserved.



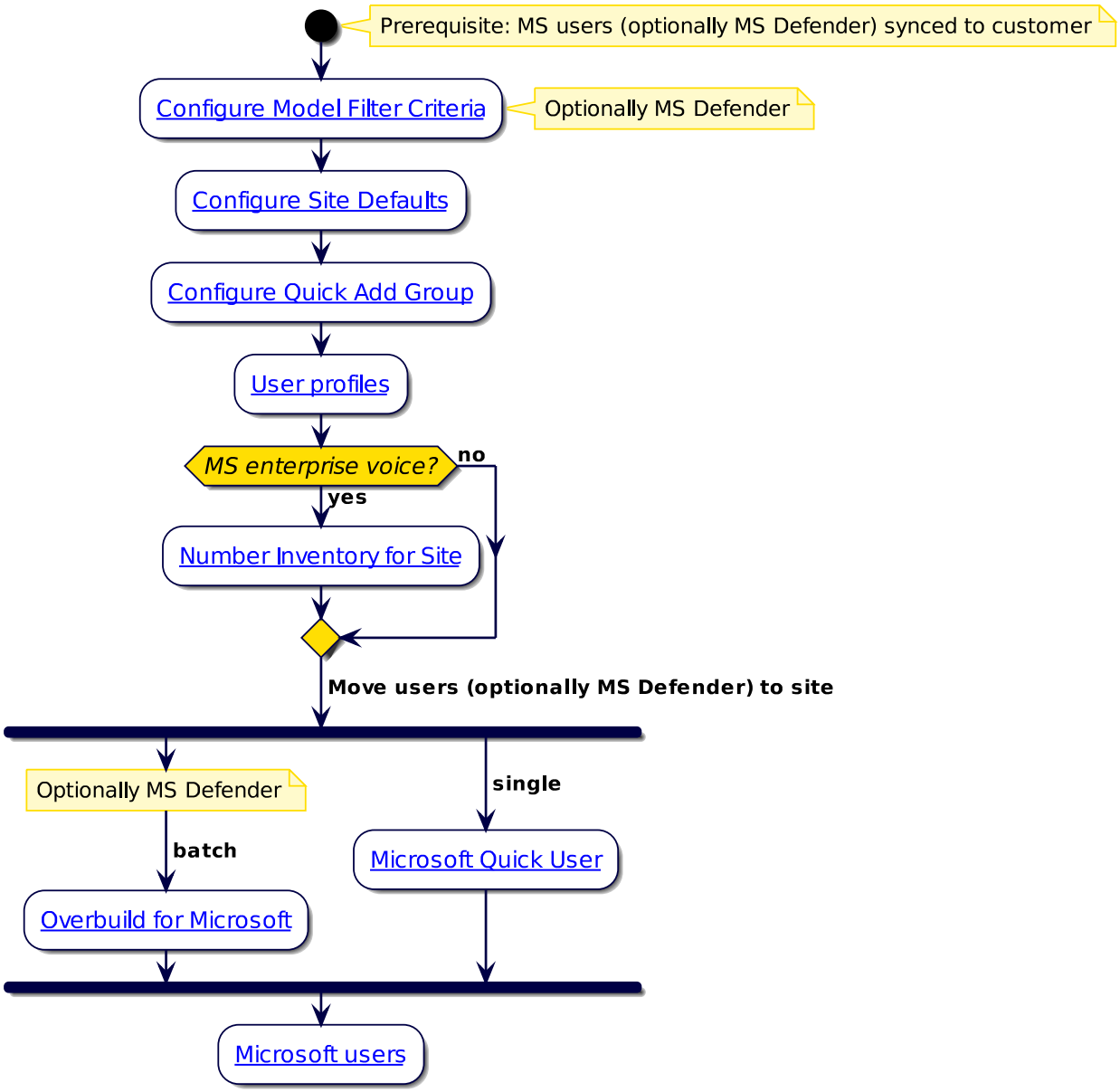
3.2.4. Step 3: Sync Microsoft Users to Sites

For details, see *Sync Microsoft users to sites*

You can choose to either directly sync in the tenant dialplan, policies, licenses and Microsoft users to the customer, or configure sync with flow through provisioning before syncing in Microsoft data and users:

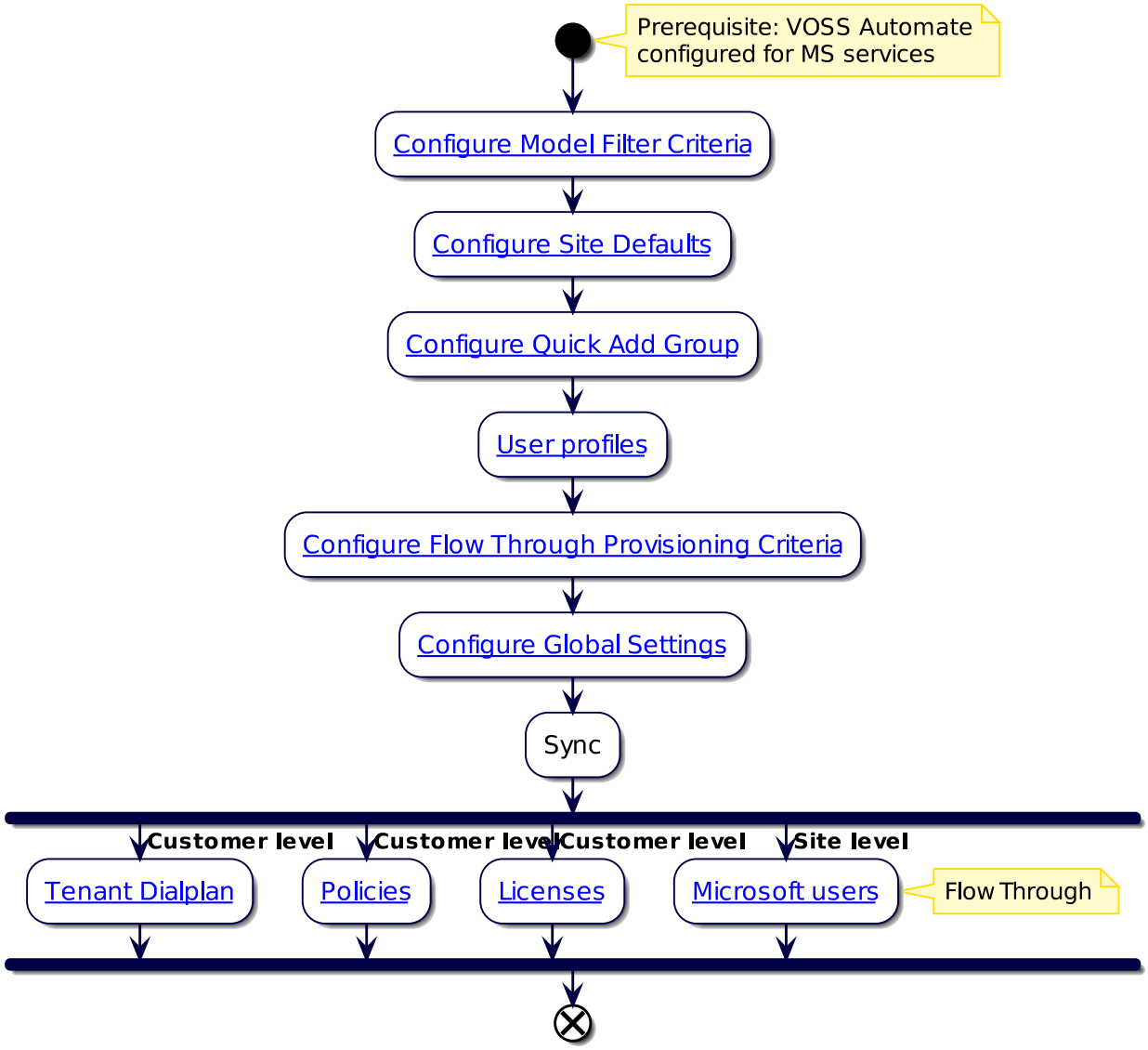
Copyright © 2025 VisionOSS Limited. All rights reserved.

Sync to customer, then to sites



Copyright © 2025 VisionOSS Limited. All rights reserved.

Sync to site with flow through provisioning



Copyright © 2025 VisionOSS Limited. All rights reserved.

4. Hierarchy Management

4.1. Introduction to hierarchies

4.1.1. Overview

Configurable hierarchy nodes in VOSS Automate allows you to partition data in a multi-tenant system. Together with user roles, data partitioning via hierarchies also provides data security.

Related Topics

- *Working with lists*

Important: An administrator can be set up to have access to a dedicated subset of hierarchies below a parent hierarchy. This is done by ensuring the administrator is assigned a user role that is associated with an **Authorized Admin Hierarchy** instance containing a a selection of allowed hierarchies. For details on this feature, see: *Authorized Admin Hierarchy Roles*.

The functionality described here in the current topic applies to the case where the **Authorized Admin Hierarchy** feature is *not* used.

4.1.2. Hierarchies mapped to business models

Hierarchies may be used to model the hierarchical nature of various types of businesses via hierarchy nodes, hierarchy node types, and hierarchy rules. Hierarchy rules can be applied to various models in the system. An example of a hierarchy rule is that sites can only be created under a customer.

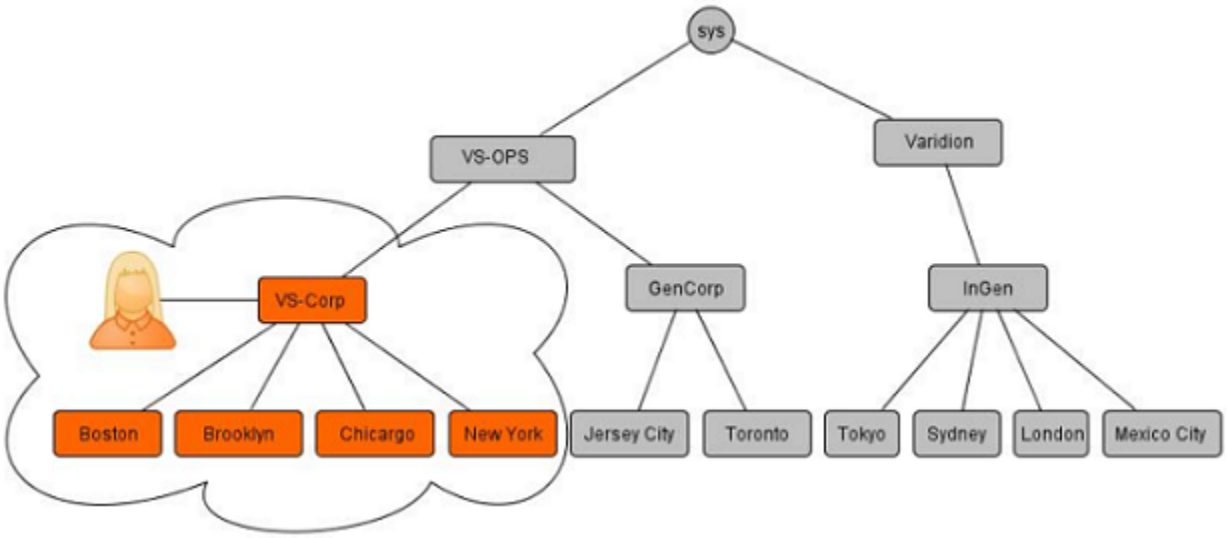
Hierarchy nodes and node types may include:

- Provider
- Reseller
- Customers
- Shared buildings
- Sites
- Divisions
- Branches

A hierarchical structure allows you to manage the allocation of infrastructure (such as network device lists), users, and other entities.

The diagram illustrates an example of a system that hosts two managed service providers: *Varidion* and *VS-OPS*.

- *VS-OPS* hosts two customers: *VS-Corp* and *GenCorp*
- *VS-CORP* operates from these locations: Boston, Brooklyn, Chicago and New York.



4.1.3. Data partitioning and hierarchies

Using hierarchies to partition data means that an administrator user is only allowed to view and perform operations on entity instances that are provisioned at the parent hierarchy of the hierarchy where they have access.

Access to resources is thus based on the user's parent hierarchy. This restriction is enforced in API middleware for every requested operation. Partitioning is enforced across the various system interfaces, for example loaders, API, and the Admin Portal. This means that an administrator user for customer "VS-Corp" cannot view or act on data at customer "GenCorp". The "VS-Corp" administrator can only view and act on entities assigned to "VS-Corp" or its child hierarchy levels (sites).

Note: When an administrator navigates to a particular hierarchy they may have read-only access to model instances created at a higher level of the hierarchy. For example, a provider administrator's view of the list of menu layouts may show instances created *above* the provider's hierarchy. In this case, the administrator requires read-only access in order to have the ability to clone a field display policy at a lower level of the hierarchy. This administrator will not be able to edit the model instance created at the higher level of the hierarchy. However, a provider administrator viewing the list of model instances below the provider level is able to edit model instances created at the provider hierarchy.

When the model is designed, the following setting is enabled: **Visible at Lower Hierarchy**

This setting is available for Data, Domain, and Relation definitions. For Relations, the setting overrides the setting in any related models. See the table below.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.1.4. Hierarchies and user roles

Automate secures access to data with the concepts of data partitioning via hierarchies, and user roles. You can create administrators with different roles for different types of hierarchy nodes for devolved administration. For example:

- An administrator is responsible for the setup of the overall system.
- Provider administrators own and manage infrastructure and define services available to resellers.
- Resellers offer the infrastructure and services to customers or enterprises.
- Customers and enterprises are grouped into various groupings.
- Groupings such as divisions or branches belong to customers.
- Physical locations hold users and phones.
- End users consume services and manage their own configurable settings.

A flexible hierarchy allows you to:

- Define as many levels as you need
- Create hierarchy node instances of different types
- Define the required business rules

4.1.5. Parent-child relationships

All entities in the system reside at a specific hierarchy and the data displayed is within the scope of the specified hierarchy. This means that every entity in the system (including users, device models and network components) has a parent hierarchy defined. A user is for example provisioned with a specific hierarchy node in a parent-child relationship. User names must be unique within a specific hierarchy.

4.1.6. User roles, access profiles, and data security

Access profiles define the read and write permissions assigned to user roles. The access profile defines how the user can interact with specific system entities. Permissions include details of each entity type in the system, as well as the relevant privileges related to that entity type. See *Introduction to role-based access control*.

- Hierarchy - defines the specific instances of the various entities that the user can interact with
- User's role and access profile - determines the permitted operations that can be performed on these instances.

The table below shows some of the models with **Visible at Lower Hierarchy** set to *true*, thereby allowing for clone operations by administrators at lower hierarchies:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Name	Model Type
AccessProfile	data/DataModel
Adaptation	data/DataModel
AdaptationLog	data/DataModel
BulkAdminDataRefreshPerHierarchy	data/DataModel
BulkAdminFullDataRefresh	data/DataModel
BulkAdminScheduleDataRefresh	data/DataModel
Bundle	data/DataModel
ConfigurationTemplate	data/DataModel
Countries	data/DataModel
CredentialPolicy	data/DataModel
FeatureConfigProfile	data/DataModel
FieldDisplayPolicy	data/DataModel
Dashboard	data/DataModel
Macro	data/DataModel
MenuLayout	data/DataModel
ModelInstanceFilter	data/DataModel
ModelTypeList	data/DataModel
Patch	data/DataModel
ProvisioningWorkflow	data/DataModel
QuickAddGroups	data/DataModel
Role	data/DataModel
SelfServiceFeatureDisplayPolicy	data/DataModel
SelfServiceLinks	data/DataModel
SelfServiceTranslation	data/DataModel
Theme	data/DataModel

Related topics

- Authorized Admin Hierarchy in the Core Feature Guide
- Network device lists in the Core Feature Guide
- Automate configuration and sync in the Core Feature Guide

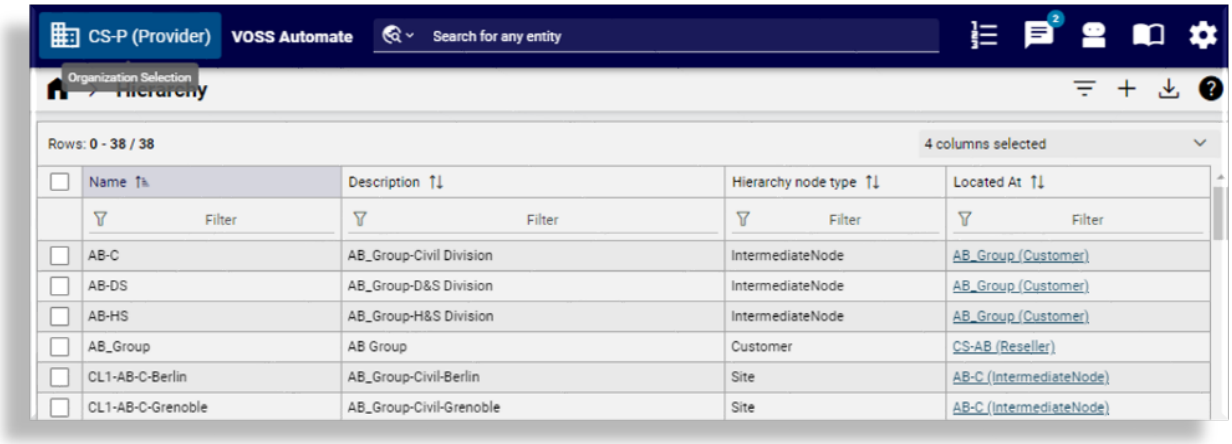
Copyright © 2025 VisionOSS Limited. All rights reserved.

4.2. Navigate the hierarchy

4.2.1. Overview

The Automate Admin Portal allows you to navigate to a particular hierarchy level and to set the context for various actions in the system at that level via the **Organization Selection** toolbar button, or to view a list of hierarchy nodes at your currently selected hierarchy in a list view.

Note: If you have the new dashboards and menus set up for your user profile, introduced in Automate 25.1, use the Action search to navigate the GUI. See *Use the Action search to navigate Automate* and *Role-based dashboards and menus*.



4.2.2. Hierarchy tree view

To open a tree view of the entire hierarchy, click the toolbar **Organization Selection** button.

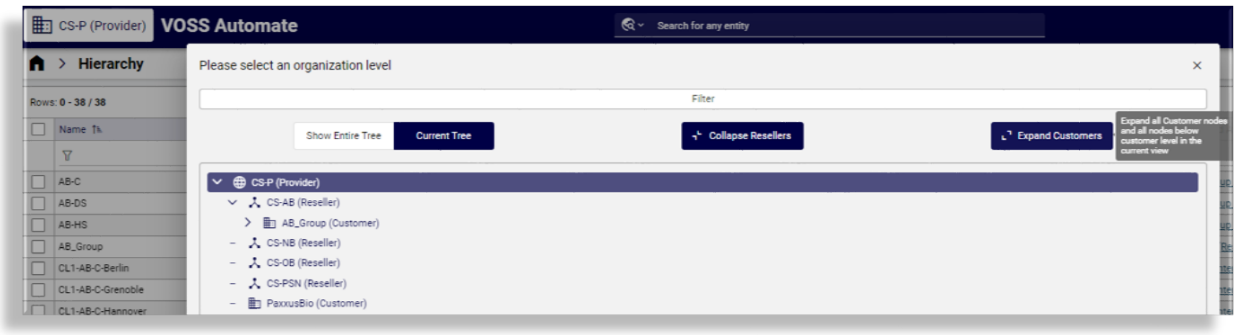
Nodes in the hierarchy tree are sorted alphabetically, and are displayed with their hierarchy type, either Provider, Reseller, Customer, or Site.

When opening the tree view, the initial state reflects the currently selected hierarchy, including its sibling and child nodes, with any intermediate and site nodes for that hierarchy expanded, allowing you to easily switch to a different site.

In the hierarchy tree view:

- Choose a hierarchy node to set the system hierarchy to that node
- Click **Entire Tree** to expand all hierarchy nodes in the tree
- Click **Current Tree** to expand the currently selected hierarchy node.
- Click **Expand Customers** to also expand intermediate nodes and site nodes within each customer in the tree
- The **Expand Resellers** button changes to **Expand Providers** if the hierarchy tree contains no *Reseller* nodes

Copyright © 2025 VisionOSS Limited. All rights reserved.



4.2.3. Switching to a different site

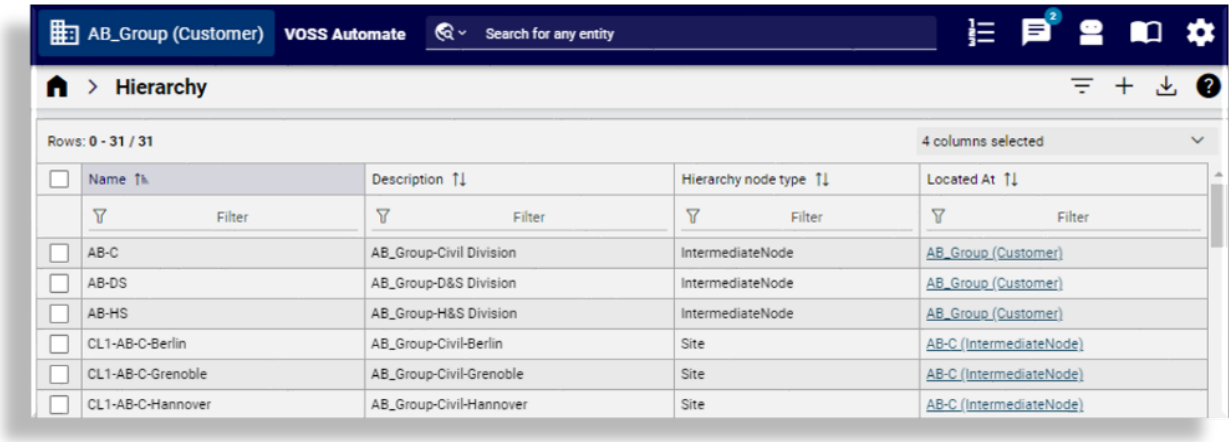
When you're working on a task at a specific site and want to switch to a different site, clicking the **Organization Selection** button opens the tree view with the list of sites expanded for the currently selected customer, allowing you to choose another site for the feature you're working with without having to go back to the previous level in the hierarchy.

4.2.4. Hierarchy list view links

For list views, the **Located At** column indicates the hierarchy level to which an object belongs.

The hierarchy level name and type shows as the column hierarchy link, for example `Overton (Customer)`.

All the entries in the list that the logged in user's hierarchy rules allows for, will show as hyperlinks. This also applies to list views of search results. Clicking on the hierarchy link sets the hierarchy to the selected hierarchy in the breadcrumb, and filters items in the list view for that hierarchy.



Note: In the event that another admin user, working on another browser, deletes a hierarchy, for example, a customer or site, the hierarchy bar refreshes once you refresh the browser.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.3. View the Hierarchy

4.3.1. Role-based Access to the Hierarchy

An administrator can view the portion of the hierarchy they have access to.

- A provider administrator can view the complete hierarchy.
- A customer administrator can view the customer, any intermediate nodes beneath the customer, and customer sites.

4.3.2. View, Sort, and Search the Hierarchy

- You can view the hierarchy on the relevant hierarchy list view. Hierarchy nodes visible to the administrator display in a table:

Field	Description
Name	Node name
Description	Node description
Hierarchy Node Type	Either Provider, Reseller, Customer, or Site. Blank for an intermediate node.
Located At	The node location in the hierarchy, in dot notation.

- To view a subset of the visible hierarchy, adjust the hierarchy path. For example, if a provider administrator sets the path to point to a particular customer, they can see only the hierarchy nodes for that customer.
- To sort hierarchy nodes, click on the field headers.
- To search hierarchy nodes, click the search icon on the field headers.

Related Topics

Navigating the Hierarchy in the Core Feature Guide

4.4. Add a provider

Tip: *Use the Action search to navigate Automate*

This procedure creates a provider hierarchy node in Automate.

Note: The system no longer automatically creates cloned roles when you add a hierarchy node. Automate roles are now all managed via the `data/Role` model and can be assigned directly without being cloned across hierarchies. See also *Role-based dashboards and menus*

Copyright © 2025 VisionOSS Limited. All rights reserved.

If you have custom bulk loaders and need to carry out this automatic cloning task, add a new boolean field to the bulk load sheets and set to TRUE:

```
"name": "clone_admin_role"
"title": "Clone Admin Role"
```

To add a provider:

1. Log in to the Automate Admin Portal:
   - Enterprise deployment: Log in as `entadmin` at `sys.hcs`.
   - Provider deployment: Log in as `hcsadmin` at `sys.hcs`.

   Note: Once Automate is installed, the *entadmin`* administrator (Enterprise deployment) or *hcs* administrator (Provider deployment) creates the provider.

2. Go to **Providers**.
3. Click the Plus icon (+) to add a new record.
4. On the **Service Provider Details** tab/panel, complete the following fields:

Field	Description
Name	The service provider name. The provider name is read-only once you save it.
Description	A description of the provider.
Domain Name	Mandatory. The service provider's directory domain, for example, "provider.com".

5. On the **Contact Information** tab/panel, fill out address, email, and phone information, as appropriate.
6. Click **Save**.

4.5. Resellers

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.5.1. Overview

You can create resellers (optional), once Automate is installed and the *entadmin*` administrator (Enterprise deployment) or *hcs* administrator (Provider deployment) has created the provider.

Note: The system no longer automatically creates cloned roles when you add a hierarchy node. Automate roles are now all managed via the `data/Role` model and can be assigned directly without being cloned across hierarchies. See also *Role-based dashboards and menus*

If you have custom bulk loaders and need to carry out this automatic cloning task, add a new boolean field to the bulk load sheets and set to TRUE:

```
"name": "clone_admin_role"
"title": "Clone Admin Role"
```

4.5.2. Add a reseller

This procedure creates a reseller.

1. Log in to the Admin portal as *Provider* admin, using the Provider admin's email address (case-sensitive).

   Note: The *hcsadmin*` administrator can find the Provider administrator's email address via the **Admins** page (click on the Provider's name to see these details).

2. Go to **Reseller**.
3. Click the Plus icon (+) to add a new record.
4. On the **Reseller Details** tab/panel, fill out the following fields:

Option	Description
Name	Mandatory. The name of the reseller. • This name can't be changed once you've saved it. • Any spaces in the reseller name are converted to underscores in the reseller local administrator name and email.
Description	Reseller description
Directory Domain	Reseller's directory domain. This field is used to create an email address for the reseller default local administrator, for example Reseller1Admin@reseller1.com. If omitted, the domain of the Provider is used.

5. On the **Contact Information** tab/panel, fill out the reseller's address details, email, and phone number.
6. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.6. Customers

Tip: *Use the Action search to navigate Automate*

4.6.1. Overview

Customers exist as a node in Automate's hierarchical structure. Typically, the structure has the following order (from highest level to lowest level).

- Provider
- Reseller
- Customer
- Sites (locations)

Optional intermediary nodes can also be created.

Automate employs hierarchies (organization levels), user roles, and access profiles to secure access to resources in the system. For details, see *Introduction to Hierarchies* in the Core Feature Guide.

Sites can only be created under a customer. You have to add and configure the customer before you can add sites. Onboarding of customers is done at the Provider hierarchy. For details around onboarding customers, see the *Customer On-boarding Quick Start Guide* in the Core Feature Guide.

Related topics

- Sites in the Core Feature Guide
- Role-based dashboards and menus in the Core Feature Guide
- Introduction to Hierarchies in the Core Feature Guide
- Customer On-boarding Quick Start Guide in the Core Feature Guide
- Network Device Lists in the Core Feature Guide

4.6.2. Add or update a customer

This procedure adds or updates a customer.

Note: You can enable or disable number management for a customer via the **Customer** page, if required.

The system no longer automatically creates cloned roles when you add a hierarchy node. Automate roles are now all managed via the `data/Role` model and can be assigned directly without being cloned across hierarchies.

If you have custom bulk loaders and need to carry out this automatic cloning task, add a new boolean field to the bulk load sheets and set to TRUE:

```
"name": "clone_admin_role"
"title": "Clone Admin Role"
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

To add or update a customer:

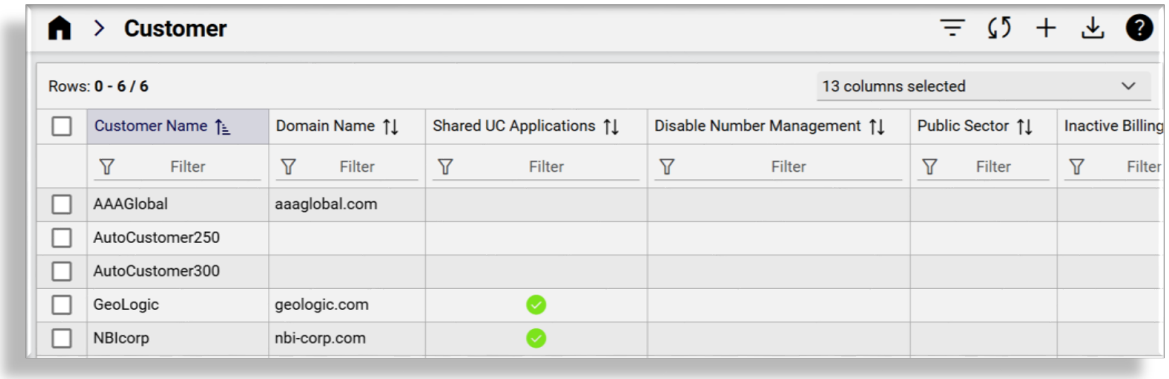
1. Log in as Provider or Reseller administrator (depending on which organization manages the customer).

   Note: Log in using the Provider or Reseller admin's email address (case-sensitive). You can find this email address via the **Admins** page, then click on the admin's name to view the email address.

2. Choose the hierarchy.

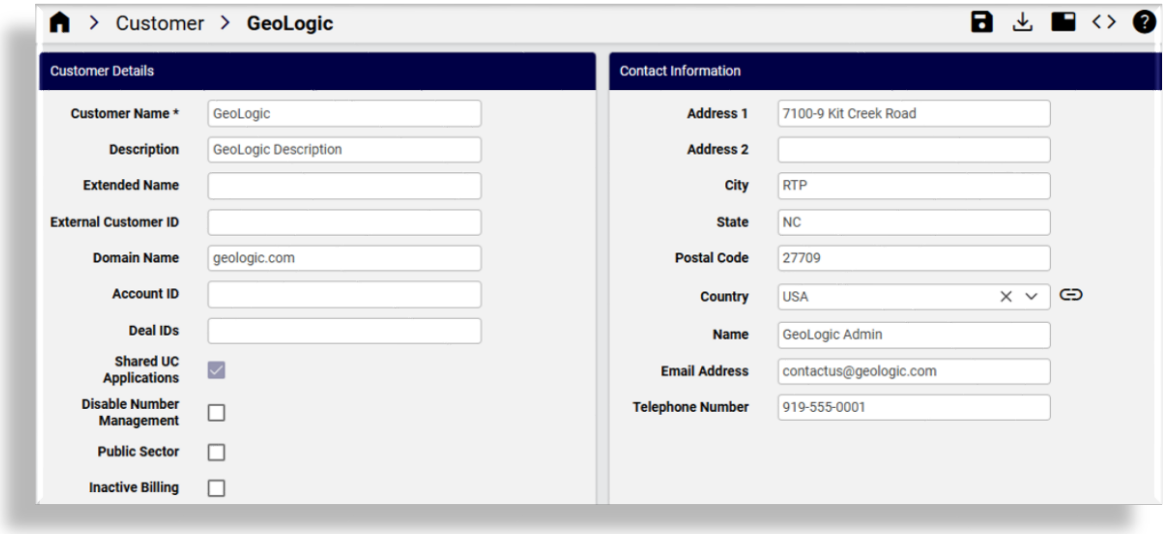
   Note: If logged in as Provider and the Customer is to be added under a Reseller, set the hierarchy path to the Reseller.

3. Go to the **Customer** page.



4. **Choose an option**:
   - **Add a new customer**? Click the Plus icon (+) to add a new record, then, fill out details for the new customer, including contact information and, optionally, enable or disable number management.
   - **Update an existing customer**? Click on the customer name in the list view to view its details. Modify customer details, including contact information and, optionally, to enable or disable number management.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Important: Additional custom string and boolean fields may be exposed via field display policies for the **Customers** configuration form. For details, see *Add custom fields to customer configuration screens*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Customer Details	Description
Customer Name	Mandatory. The name of the customer.
Description	Customer description
Extended Name (Provider)	Descriptive name for the customer, used by external clients to correlate their own customer records with customer records stored in HCS.
External Customer ID (Provider)	External customer ID used by the Service Inventory service, and included as a column in the customer record of the service inventory report. Specify an External Customer ID in this field that matches the customer ID used by the external inventory tool that receives the Service Inventory reports. If the Service Inventory service is not being used, this field is not required. However, it can be used to correlate customer records in external systems with customer records in HCS.
Domain Name	Customer domain. This field is used to create email addresses for: • The customer default local administrator, for example: Customer1Admin@customer1.com • Site default local administrators under the customer, for example: Site1Admin@customer1.com If the customer domain is omitted, the provider domain (or reseller domain, if the customer is under a reseller in the hierarchy and the reseller domain was provided) is used instead.
Account ID	The Account ID is used by external clients to correlate their own customer records with the customer records stored in HCS. This Account ID value is synced to the Customer record in the Shared Data Repository.
Deal IDs	Deal IDs are used by the Hosted License Manager (HLM) service. HLM supports Point of Sales (POS) report generation. The report includes all customers on the system with aggregate license consumption at customer level. The optional **Deal ID** field associated with the customer is included in the report. Each customer can have zero or more Deal IDs. The **Deal ID** field is free text format and each deal ID is separated by a comma.

Customer Details	Description
Shared UC Applications	Indicates whether the customer can use Shared UC Apps. If selected, the customer sites can use Network Device Lists that contain Shared UC Apps. Shared UC Apps are UC Apps that are defined above the Customer hierarchy level.
Disable Number Management	Enable or disable Number Management for this customer. • When disabled (checkbox selected), you cannot add directory numbers and E164 numbers to inventories for this customer. • When enabled (checkbox clear), you can add directory numbers and E164 numbers to inventories for this customer.
Public Sector	Defines whether the customer is a Public Sector customer. Used for License Reporting.
Inactive Billing	Defines whether to exclude the customer from billing (for testing). Used for License Reporting.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: If you enable number management for a customer after it was disabled, run the DN Audit Tool. See *Number inventory audit*.

5. Save your changes.

Related topics

- *Number inventory audit*
- Delete issues and purges in the Core Feature Guide
- Role-based dashboards and menus in the Core Feature Guide

4.6.3. Add custom fields to customer configuration screens

You can add up to ten custom string fields and up to 10 custom boolean fields to the field display policy you apply to the Customer data model (*relation/HcsCustomerREL*). This provides flexibility to add additional details for a customer, if required.

The summary attributes in the **Customers** list view always display three Boolean fields and three String fields, regardless whether they've been included in the FDP. If you wish to change the title of these fields in the summary attributes you can add a field override entry in the FDP.

When configuring a customer (add or update), you may specify field values or use named macros to populate values for these fields.

Macros for custom string fields for relation/HcsCustomerREL:

- macro.HcsVossCustomerDAT_custom_string_1
- macro.HcsVossCustomerDAT_custom_string_2
- macro.HcsVossCustomerDAT_custom_string_3
- macro.HcsVossCustomerDAT_custom_string_4
- macro.HcsVossCustomerDAT_custom_string_5
- macro.HcsVossCustomerDAT_custom_string_6
- macro.HcsVossCustomerDAT_custom_string_7
- macro.HcsVossCustomerDAT_custom_string_8
- macro.HcsVossCustomerDAT_custom_string_9
- macro.HcsVossCustomerDAT_custom_string_10

Macros for custom boolean fields for relation/HcsCustomerREL:

- macro.HcsVossCustomerDAT_custom_boolean_1
- macro.HcsVossCustomerDAT_custom_boolean_2
- macro.HcsVossCustomerDAT_custom_boolean_3
- macro.HcsVossCustomerDAT_custom_boolean_4
- macro.HcsVossCustomerDAT_custom_boolean_5
- macro.HcsVossCustomerDAT_custom_boolean_6

Copyright © 2025 VisionOSS Limited. All rights reserved.

- macro.HcsVossCustomerDAT_custom_boolean_7
- macro.HcsVossCustomerDAT_custom_boolean_8
- macro.HcsVossCustomerDAT_custom_boolean_9
- macro.HcsVossCustomerDAT_custom_boolean_10

The macros can be applied in workflows and configuration templates to reference the custom field values. For example, executing *macro.HcsVossCustomerDAT_custom_string_1* will return the value in the field where the macro is used.

Expose custom fields for *relation/HcsCustomerREL*

1. Log in to Automate as Provider admin or higher.
2. Create or update the Customers data model field display policy:
   - Go to the **Field Display Policies** page, then locate the entry for target model type, *relation/HcsCustomerREL*.
   - Click on the default field display policy (FDP) for the model (the FDP named *default*).
   - Clone (copy) the default FDP for the model, and give the clone a new name.

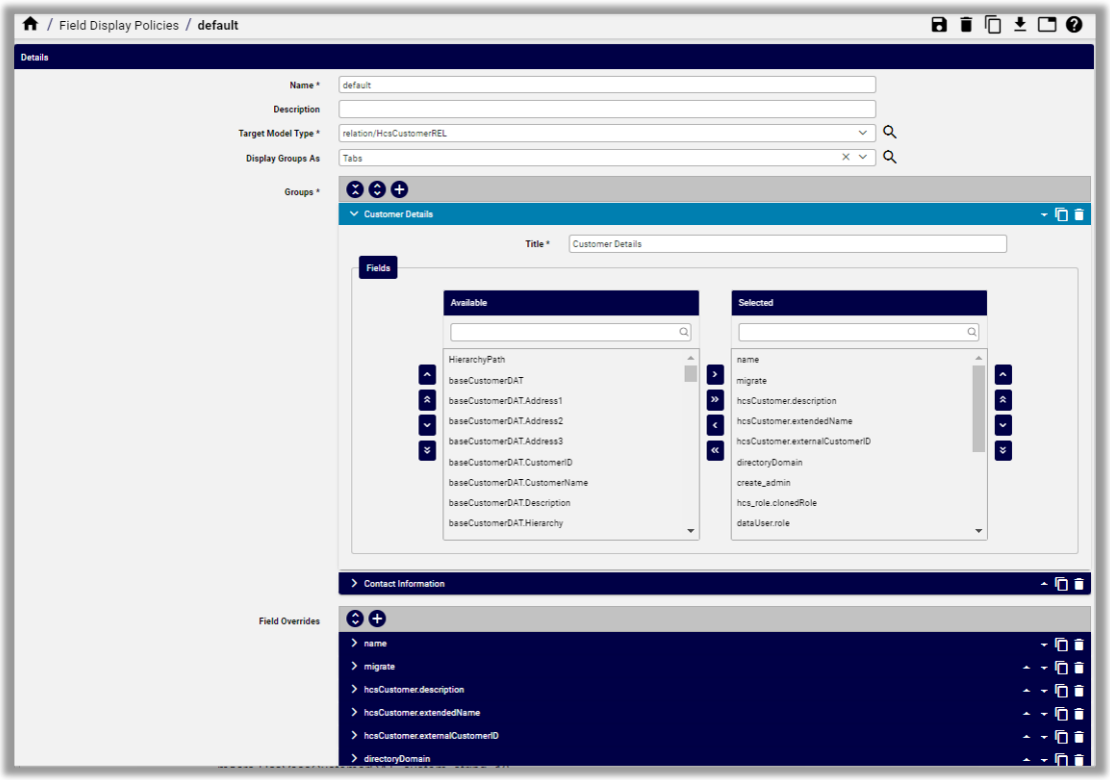
     Note: You can't modify default FDPs that ship with the system. This allows you to refer to or revert to a system default at any time, if required.

   - Modify the new FDP (the clone).

     Note: You can add a new group of fields containing only the new custom fields, or add fields to existing field groups.

     You can also create field overrides, which allow you to define that a custom field value will be referenced in place of an existing field.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- Save your changes.

3. Update the menu layout to apply the field display policy:
   - Go to **Menu Layouts**, and locate the Provider admin menu layout (HcsProviderMenu).
   - Click on **HcsProviderMenu**, and create a clone with a new name.

     Note: You can't modify default menu layouts that ship with the system. This allows you to refer to or revert to a system default menu layout at any time, if required.

   - Modify the clone (copy) of **HcsProviderMenu**:
     - Expand the **Customer Management** menu.
     - At **Customers**, click in the **Field Display Policy** cell, and choose the FDP you configured to add the custom fields.
   - Save your changes.
4. Log out, then log in again as Provider admin.

   This allows the role-based access profile changes to refresh so that you can view the updated menu layouts and field display policies you applied, including new custom fields.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.7. Intermediate node

Tip: *Use the Action search to navigate Automate*

4.7.1. Overview

An intermediate node is an optional node in the Automate hierarchy. It is located between the standard hierarchy nodes (provider, reseller, customer, and site).

Intermediate nodes can be used to logically group other nodes, and to restrict access by administrators to a defined subset of nodes. For example, intermediate nodes could be used to group customers by industry, or sites by geography.

When an intermediate node is created, an administrator is created for the intermediate node in a separate step. A default admin is not created for it.

4.7.2. Add an intermediate node

This procedure adds an intermediate node.

1. Log in as an administrator at the hierarchy where you want to create the intermediate node. For example, if adding an intermediate node to group sites, log in as the customer administrator.
2. Go to the **Intermediate Node** page, then click the Plus icon (+) to add a new record.
3. Fill out details for the new intermediate node:

Field	Description
Name	The name of the node. This field is mandatory. The name is read-only once it's changed.
Description	A description of the node (optional).
Hierarchy node type	The type of hierarchy node you're adding, either Hcs, IntermediateNode, LinkedSite, Provider, Reseller, or Site.
Shadow	.

4. Save your changes to create the intermediate node in the hierarchy.

Next steps

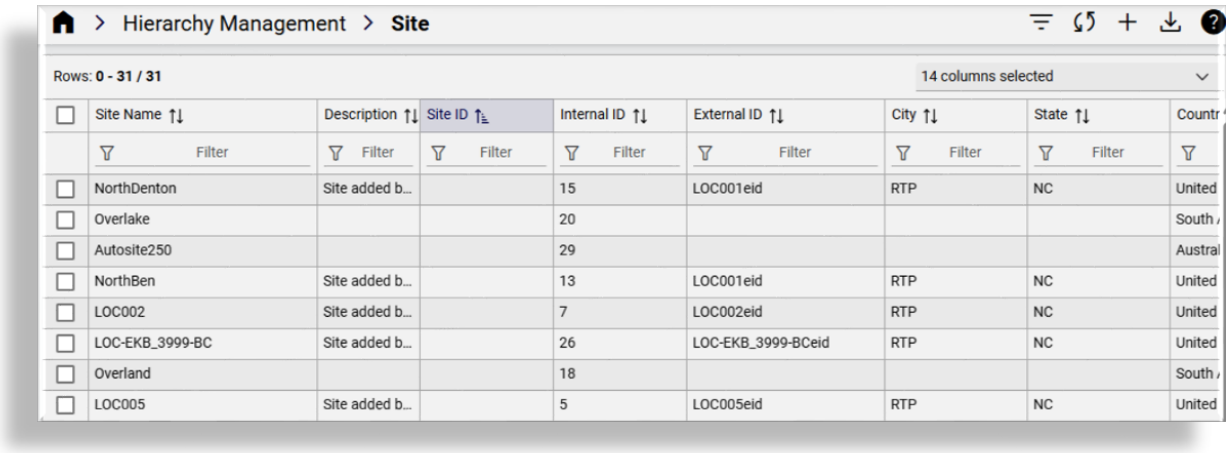
- Create a local administrator for the intermediate node.
- Then create nodes underneath the intermediate node for the intermediate node local administrator to manage.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.8. Sites

4.8.1. Overview

Sites (locations) are a node on the hierarchy (organization) structure of Automate and are created under customers.



Related topics

- *Customers*
- *Delete a hierarchy*
- *Site Defaults Doc templates*
- *Site defaults*
- *Introduction to hierarchies*

4.8.2. Add a site

This procedure adds a site.

Note: The system no longer automatically creates cloned roles when you add a hierarchy node. Automate roles are now all managed via the `data/Role` model and can be assigned directly without being cloned across hierarchies. See also *Role-based dashboards and menus*

If you have custom bulk loaders and need to carry out this automatic cloning task, add a new boolean field to the bulk load sheets and set to TRUE:

```
"name": "clone_admin_role"
"title": "Clone Admin Role"
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

To add a site:

1. Log in as either provider, reseller, or customer admin.
2. Set the hierarchy to the customer where you're creating the site.
3. Go to the **Site** page.
4. Click the Plus icon (+) to add a new record, then fill out site details and contact information:

Field	Description
Site Name	Mandatory. The name of the site. Note: Any spaces in the site name are converted to underscores in the site local administrator name and email, if the **Create Local Admin** check box is selected. You can't migrate a customer location to a site if the customer for the site is different than the customer associated with the customer location. When migrating a customer location to a site, an NDL is not selected for the site. You can set the NDL for the site later.
Description	The site description.
Extended Name	Provider deployments. External clients can use the extended name of the site if needed. This field is not used by other components within Cisco HCS.

Field	Description
Internal ID	Read only. Internal ID of the site.
External ID	Provider deployments. External clients can use the External ID of the site if needed. This field is not used by other components within Cisco HCS.
Site ID	Unique identifier for the site.
Country	Mandatory. The selected country determines the dial plan to download to the site when the dial plan is configured on the site.
Network Device List	Choose the network device list (NDL) containing the UC applications and Webex to be used by the site. Once an NDL is set for the site, it can't be removed from the site, nor can the NDL be changed to another NDL.
Auto Push Users to CUCM	Disabled by default. When enabled, users are automatically pushed to the CUCM associated with the NDL at the site. You can also edit the site after it's been created: • To automatically push users at the site to the CUCM • To execute auto push to CUCM when an NDL (with a CUCM) is added to the site • To execute auto push to CUCM when a CUCM is associated with the NDL at the site

5. Click **Save** to create the site hierarchy node and location.

   If **Auto Push Users to CUCM** is selected:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- All users associated with the NDL, provided they are user type *End User*, are pushed to the CUCM associated with the NDL
- A user's surname is required by the CUCM and must be set for that user to be successfully pushed to the CUCM
- A Cisco user is created when onboarding Cisco users but not when onboarding Microsoft or Webex users (for sites with this setting enabled)

4.8.3. Add custom fields to site configuration forms

Automate allows you to add up to ten custom string fields and up to 10 custom boolean fields to the field display policy you apply to the site model (*relation/HcsSiteREL*). This provides flexibility to add additional details for a site, if required.

The summary attributes in the **Sites** list view always display three boolean fields and three string fields, regardless whether they've been included in the FDP. If you wish to change the title of these fields in the summary attributes you can add a field override entry in the FDP.

When configuring a site (add or update), you may specify field values or use named macros to populate values for these fields.

Macros for custom string fields for `relation/HcsSiteREL`:

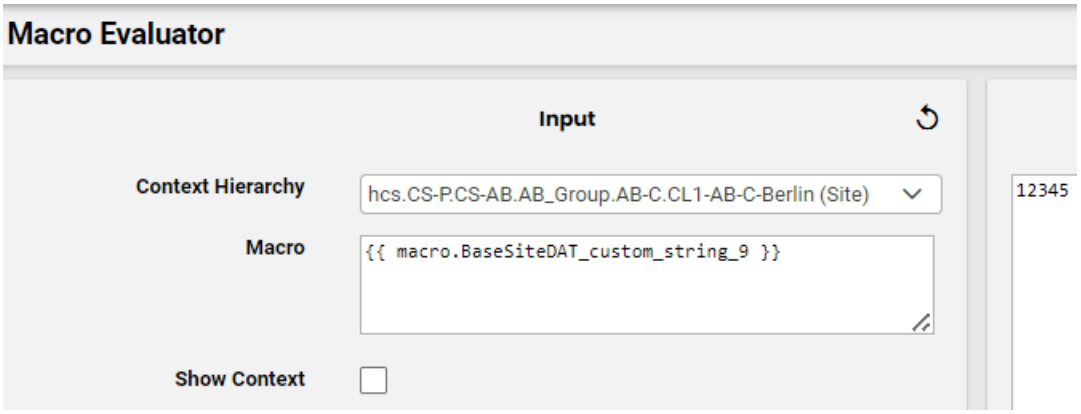
- macro.BaseSiteDAT_custom_string_1
- macro.BaseSiteDAT_custom_string_2
- macro.BaseSiteDAT_custom_string_3
- macro.BaseSiteDAT_custom_string_4
- macro.BaseSiteDAT_custom_string_5
- macro.BaseSiteDAT_custom_string_6
- macro.BaseSiteDAT_custom_string_7
- macro.BaseSiteDAT_custom_string_8
- macro.BaseSiteDAT_custom_string_9
- macro.BaseSiteDAT_custom_string_10

Macros for custom boolean fields for `relation/HcsSiteREL`:

- macro.BaseSiteDAT_custom_boolean_1
- macro.BaseSiteDAT_custom_boolean_2
- macro.BaseSiteDAT_custom_boolean_3
- macro.BaseSiteDAT_custom_boolean_4
- macro.BaseSiteDAT_custom_boolean_5
- macro.BaseSiteDAT_custom_boolean_6
- macro.BaseSiteDAT_custom_boolean_7
- macro.BaseSiteDAT_custom_boolean_8
- macro.BaseSiteDAT_custom_boolean_9
- macro.BaseSiteDAT_custom_boolean_10

Copyright © 2025 VisionOSS Limited. All rights reserved.

The macros can be applied in workflows and configuration templates to reference the custom field values. For example, executing *macro.BaseSiteDAT_custom_string_9* will return the value in the field where the macro is used.



4.8.4. Expose custom fields for "relation/HcsSiteREL"

1. Log in to Automate as provider admin or higher.
2. Create or update the customers data model field display policy:
   - Go to the **Field Display Policies** page.
   - Locate the entry for target model type `relation/HcsSiteREL`.
   - Click on the default field display policy (FDP) for the model (the FDP named *default*).
   - Clone (copy) the default FDP for the model, and give the clone a new name.

     Note: You can't modify default FDPs that ship with the system. This allows you to refer to or revert to a system default at any time, if required.

   - Modify the new FDP (the clone).

     Note: You can add a new group of fields containing only the new custom fields, or add fields to existing field groups.

     You can also create field overrides, which allow you to define that a custom field value will be referenced in place of an existing field.

   - Save your changes.
3. Update the menu layout to apply the field display policy:
   - Go to **Menu Layouts**.
   - Locate the Provider admin menu layout (HcsProviderMenu).
   - Click on **HcsProviderMenu**, and create a clone with a new name.

     Note: You can't modify default menu layouts that ship with the system. This allows you to refer to or revert to a system default menu layout at any time, if required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Modify the clone (copy) of **HcsProviderMenu**:
  - Open the **Sites** .
  - Click in the **Field Display Policy** cell, then select the FDP you configured to add the custom fields.
- Save your changes.

4. Log out, then log in again as Provider admin.

   This allows the access profile changes to refresh so that you can view the updated menu layouts and field display policies you applied, including new custom fields.

4.9. Site Defaults Doc templates

When a provider hierarchy is created in VOSS Automate, a system workflow creates a default Site Defaults Doc (SDD) template called `PROVIDER_TEMPLATE`, at the Provider level.

Note: For Cisco CUCM environments, the `PROVIDER_TEMPLATE` SDD template can be pre-populated with relevant values for Cisco CUCM, provided you have enabled the **Enable Cisco CUCM** Global Setting. Automate's Provider SDD template creation workflow checks whether this setting is enabled before populating values for Cisco CUCM in the template.

For each customer added to the system at a particular provider, data in the provider's `PROVIDER_TEMPLATE` is used to generate a customer-level, default SDD template called `CUSTOMER_TEMPLATE`.

When adding a site at a customer, that customer's `CUSTOMER_TEMPLATE` SDD template is used to create a SDD instance on the site.

The site-level SDD is useful for managing multi-site, multi-country customers, and allows a Provider admin (or higher) to define geo-specific information at a site level. This allows multinational sites to stay in sync.

Site-level SDDs:

- Have the same name as the site
- Are pre-populated with several default values
- Provide the default values for several of the tasks performed during onboarding

For Provider deployments, when creating a Cisco HCS site dial plan, the site defaults on the site are updated with dial plan-related attributes that are affected by the deployed site dial plan. Any related existing values are overwritten. When the site dial plan is removed, these values are reset (set to empty) in the site's defaults.

Administrators with appropriate permissions can modify the `PROVIDER_TEMPLATE` and `CUSTOMER_TEMPLATE` SDD templates as required in order to customize SDD settings in the template when creating lower-level SDDs and SDD templates.

Default SDD templates display in the **Site Defaults** menu. Use the Action search to open the page. See *Use the Action search to navigate Automate*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Site defaults*
- Global Settings in the Core Feature Guide.

4.10. Site defaults

Tip: *Use the Action search to navigate Automate*

4.10.1. Overview

Site defaults provide the default values for several of the tasks performed during onboarding. When creating a site, a site defaults instance is created on the site, having the same name as the new site, and pre-populated with several default values.

For Provider deployments, when creating a Cisco HCS site dial plan, the site defaults on the site are updated with dial-plan-related attributes that are affected by the deployed site dial plan. Any related existing values are overwritten. When the site dial plan is removed, these values are reset (set to empty) in the site defaults.

The Site Defaults Doc (SDD) is useful for managing multi-site, multi-country customers. A SDD allows a Provider administrator (or higher) to define geo-specific information at a site level, allowing multinational sites to stay in sync.

Geo-specific information includes CUCM user-locale and network-locale defaults, as well as the CUC time zone and language defaults.

Site defaults may also be used to include a site for the overbuild, an Automate process that syncs in users, and which may include moving users to sites (based on model filter criteria chosen for the site defaults), and assigning services to s at the sites (when flow through provisioning is enabled).

4.10.2. Configure site defaults

This procedure displays and updates site defaults.

1. Log in to the Automate Admin Portal as Provider, Reseller, or Customer admin.
2. Go to **Site Defaults**, then select the relevant site to open its site default settings.
3. Click through the tabs of the **Site Defaults** to modify site default values. See *Site defaults settings*.
4. Save your changes.

Note:

- Field descriptions for the tabs on this screen are documented below.
- Note that the SDD also contains ten custom string fields and ten custom boolean fields, which are, by default, untitled and hidden:
  - `custom_string_1` to `custom_string_10`
  - `custom_boolean_1` to `custom_boolean_10`

Copyright © 2025 VisionOSS Limited. All rights reserved.

To enable and use these fields, higher-level administrators can modify the field display policy (FDP) for the SDD (at a specific hierarchy). Once the fields are available, designers can reference the fields in custom configuration templates and workflows.

Related topics

- Site Defaults Doc Templates in the Core Feature Guide.

4.10.3. Site defaults settings

On the site **Defaults** page, you can view and edit a site's default settings (the site defaults document, or SDD).

You can configure settings on the following tabs/panels on this page:

- *General Defaults tab*
- *Device Defaults tab*
- *Line Defaults tab*
- *User Defaults tab*
- *CUC Defaults tab*
- *HotDial Defaults tab*
- *Overbuild Defaults tab*
- *Move Filter Criteria tab*
- *MS Teams tab*
- *Webex tab*

Copyright © 2025 VisionOSS Limited. All rights reserved.

General Defaults tab

Option	Default Value
Name	Mandatory. The same name as the site. Only one instance of site defaults exists for a site.
Default CUCM Device Pool	Cu{CustomerId}Si{SiteId}-DevicePool
Default CUCM Location	Cu{CustomerId}Si{SiteId}-Location
Default CUCM Region	Cu{CustomerId}Si{SiteId}-Region
Default CUCM Date/Time Group	CMLocal For Provider deployments, choose from the drop-down list.
Default User Locale	The user locale identifies a set of detailed information to support users at the specific location, including language and font. Choose the required user locale from the drop-down list, which contains all user locales available on the CUCM at the selected location.
Default Network Locale	The network locale contains a definition of the tones and cadences that the phones and gateways use at the specific location. Choose the required network locale from the drop-down list, which contains all network locales available on the CUCM at the selected location.
Default User Profile (for User Self Provisioning)	Choose from the drop-down list.
Default CUCM Hunt Pilot Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM Call Pickup Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM Call Park Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM MeetMe Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM Group	Defined via a macro in the CUSTOMER_TEMPLATE and the algorithm chosen for CUCM Group selection, either *Least Utilized* or *Default*. See CUCM Group Selection in the Core Feature Guide for details.

Related topics

- CUCM Group Selection in the Core Feature Guide.
- Configure CUCM Groups in the Provider HCS Dial Plan Management Support Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Device Defaults tab

Values on the **Device Defaults** tab are applied to the configuration template associated with adding a (SubcriberPhonePrePopulate).

Option	Default Value
Default CUCM Phone Product	Cisco 9971
Default CUCM Phone Protocol	SIP
Default CUCM Phone Button Template	Standard 9971 SIP
Default CUCM Phone Security Profile	Cisco 9971 - Standard SIP Non-Secure Profile
Default CUCM Phone Softkey Template	Standard User
Default CUCM Phone SIP Profile	Standard SIP Profile
Default CUCM Phone Presence Group	Standard Presence Group
Default CUCM Phone Common Profile	Standard Common Phone Profile
Default CUCM Phone Line E164 Mask	Enter a E164 mask value that will be applied as a default when devices have not been configured with static values.
Default CUCM Device CSS	Cu{CustomerId}Si{SiteId}-{countryIsoCode}- DP-Emer-CSS
Default CUCM User Subscribe CSS	Internal-CSS
Default CUCM Phone Subscribe CSS	Cu{CustomerId}Si{SiteId}-InternalOnly-CSS
Default CUCM Device Profile Product	Cisco 9971
Default CUCM Device Profile Protocol	SIP When adding a phone (or when choosing a phone for a user), the phone type you choose must support the protocol you wish to use (SIP or SCCP). If the phone type does not support the protocol, the protocol defaults to the protocol value set up in the site defaults (if the phone type supports the default protocol).
Default CUCM Device Profile Button Template	Standard 9971 SIP

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Default Value
Default CUCM Device Profile Line E164 Mask	None. Enter a E164 mask value that will be applied as a default when devices have not been configured with static values.
Default CUCM Device Profile EMCC CSS	None
Default CUCM Remote Destination Profile CSS	None
Default CUCM Remote Destination Profile ReRouting CSS	None
Default CUCM Remote Destination Profile Line E164 Mask	None. Enter a E164 mask value that will be applied as a default when devices have not been configured with static values.
Use National Mask Format	When this check box is selected, the E164 Mask will use the National format of the associated E164 Number. For example, if the E164 Number has been added in the format +44 1234 5000, and this check box is selected, the E164 Mask on the device will have the International Dialing Code prefix removed e.g. +44, and a '0' will be prefixed to the number e.g. 012345000. Note: For Quick Add User, set the following value in the **E164 Mask** field of the relevant phone, device profile and remote destination profile configuration template {{ macro.SDD_QAS_E164Number_MCR }}. See the "Reference CUCM Phone Template" CFT for an example configuration.

Line Defaults tab

Values on the **Line Defaults** tab are applied to the configuration template associated with adding a line (line-cft).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Default Value
Default CUCM Line BLF Presence Group	Standard Presence Group
Default CUCM Line Voicemail Profile	None
Default CUCM Line Partition	
Default CUCM Line Alternate E164 Partition	None
Default CUCM Line CSS	Cu{CustomerId}Si{SiteId}-InternalOnly-CSS
Default CUCM Line Call Forward CSS	Internal-CSS
Default CUCM Line Call Forward No Answer CSS	Internal-CSS
Default CUCM Line Call Forward All CSS	Internal-CSS
Default CUCM Line Call Forward No Answer Internal CSS	Internal-CSS
Default CUCM Line Call Forward Busy CSS	Internal-CSS

Option	Default Value
Default CUCM Line Call Forward Busy Internal CSS	Internal-CSS
Default CUCM Line Call Forward No Coverage CSS	Internal-CSS
Default CUCM Line Call Forward No Coverage Internal CSS	Internal-CSS
Default CUCM Line Call Forward On Failure CSS	Internal-CSS
Default CUCM Line Call Forward On Failure Internal CSS	Internal-CSS
Default CUCM Line Call Forward Not Registered CSS	Internal-CSS
Default CUCM Line Call Forward Alternate Party CSS	CU1-DummyBlk-CSS
Default CUCM Line Call Forward Secondary CSS	Internal-CSS

Copyright © 2025 VisionOSS Limited. All rights reserved.

User Defaults tab

Option	Default Value
Default System User Role	{SiteName}SelfService
Default CUCM User BLF Presence Group	Standard Presence group
Default CUCM Service Profile	None
Default Self-service Language	Choose from the drop-down list of installed Self-service languages. Default is English (en-us).

Note: When selecting the **Default System User Role**, the selection options include roles where the **Hierarchies Allowed** list includes sites.

See *Add and edit roles* in the Core Feature Guide.

CUC Defaults tab

For more information about the settings on this tab, see:

Cisco Unity Connection Localization in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Default Value
Default CUC Phone System	This field is populated by the Voice Mail workflow when a Voice Mail pilot number is associated with a site. Likewise, the field is reset (Empty) when the Voice Mail pilot number is disassociated from a site.
Default CUC Subscriber Template	This field is populated by the Voice Mail workflow when a Voice Mail pilot number is associated with a site. Likewise, the field is reset (Empty) when the Voice Mail pilot number is disassociated from a site.
Default CUC HTML Notification Template	Default_Dynamic_Icons
Default CUC SMPP Provider	None
Default CUC TimeZone	None. Choose from the drop-down list, for example: GMT-05:00-America-New_York. The timezones available in this drop-down are those added in **Services > CUC Localization > CUC TimeZone Filters** (see cross reference below). You can also manually enter a valid timezone index value in this field, for example 035 for (GMT-05:00) Eastern Time (US and Canada). Note that the code entered must already be installed on the CUC server associated to this site.
Default CUC Language	None. Choose from the drop-down list, for example: English-US. The languages available in this drop-down are those in **Services > CUC Localization > CUC Language Filters** (see cross reference below). You can also manually enter a valid Locale ID (LCID) value for the language in this field, for example 1036 for French - France. Note that the code entered must already be installed on the CUC server associated to this site.
Default Language That Callers Hear	None. Choose from the drop-down list: • Inherit Language From Caller • Use System Default Language • [Use the User Language] e.g. English (United States). See “Default CUC Language” above. • [Choice of Languages] e.g. Spanish (Spain Traditional). See “Default CUC Language” above).

HotDial Defaults tab

Option	Default Value
Default PLAR CSS	None
Default HotDial TimeZone	None

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overbuild Defaults tab

This tab defines how imported objects are moved to the site hierarchy during an overbuild.

Note: The Overbuild Defaults tab in the Site Defaults is accessible only to Provider and Reseller administrators.

Important: It is recommended that you request support from a system integrator for all managed services, Day 2 overbuild projects).

The table describes the settings on this tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Include Site for Overbuild	Defines whether the site is included in the overbuild.
Create Internal Number Inventory at Customer	Defines whether to create the internal number inventory only at the site level, or only at the customer level. When set to True (checkbox selected), the internal number inventory is created only at the customer level, and will be used by all sites belonging to that customer. The default is False. CAUTION: If overbuild has already been run for a site and the internal number inventory has been created for the site, if *Create Internal Number Inventory* is enabled and you run overbuild for the same site, a duplicate set of internal number inventory is created at the customer. The same applies if Create Internal Number Inventory at Customer is enabled when the overbuild is run for the site, if it is then disabled and overbuild is run again, a duplicate set of internal number inventory is created at the site.
Additional Device Pools	By default, if a site is included for overbuild, the Default CUCM Device Pool on the General Defaults tab must match the device pool of phones that have been imported in order for these and their related objects to be moved to the site at which the Site Defaults Doc exists. The Run Overbuild tool uses the device pool to determine the devices and models to move to the site where the site defaults are defined. You can however add additional device pools, so that more than one device pool from those of the imported phones can be moved to the same site. Additional device pools are selected from the Device Pool Name drop-down, as instances of the Additional Device Pools group control. The names of the additional device pools can be renamed to the Default Device Pool name (as defined on the General Defaults tab) if Replace with Default Device Pool is selected.
Overbuild Device Control	Options are: • Move all devices - when True, all matching and related imported devices are moved to the site. • Limit moved devices - when True, options display to choose devices to import to the site (as on Run Overbuild page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Overbuild for Microsoft in the Core Feature Guide

Move Filter Criteria tab

This tab defines the rules the system uses to match users to sites when syncing in users, and to determine whether users should be moved directly to the site as subscribers.

- The **MS 365 Model Filter Criteria** model filter criteria you can choose (depending on the user type you're syncing in, for example, Microsoft, LDAP, CUCM, Cisco Webex), is configured in the Admin Portal, via the **Model Filter Criteria** page. Use the Action search to go to the page. See *Use the Action search to navigate Automate*.
- The **Move by Number** check box (unchecked by default) is used for MS Teams users. When checked:
  - it requires that all numbers are pre-loaded
  - *only if* the synced-in MS Teams user's LineUri matches a pre-loaded internal number at a site, will user data be moved to that site
  - current users at customer level will be moved to the site during Overbuild (if the **Include Site for Overbuild** check box is enabled on the *Overbuild Defaults tab*).
  - MS Teams users will be moved directly to the site during MS Teams user sync.

Note: The order of processing of these two options are:

1. **MS 365 Model Filter Criteria** is processed first if it is selected and the filter exists.
2. **Move by Number** is processed second.

In other words, when a user's details match the model filter criteria, the system will move the user according to the filter criteria. Otherwise, the system will attempt to move the user by number. If neither option is applicable, the user is not moved and remains at the current hierarchy.

Related topics

- Flow Through Provisioning in the Core Feature Guide
- Model Filter Criteria in the Core Feature Guide
- Overbuild for Microsoft in the Core Feature Guide

MS Teams tab

Important: From release 21.4-PB2 onwards, License Management has been removed and is no longer used to control the logic with managing licenses. Automate will honor any license-related configuration in the Configuration Templates and related Workflows. This includes Quick User, Quick Offboard User, associated Quick Add Groups and general user management functionality.

It is advised that administrators evaluate their current Configuration Templates and ensure that if any licensing logic exists in the templates, that this is correct as it will be applied when invoked.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Also see the *Licensing Users for MS Teams and Teams Phone by Group Membership* topic in the Core Feature Guide.

The table describes settings on this tab:

Option	Description
Enterprise Voice	Defines whether to provision MS Teams users with the Enterprise Voice service.
MS Teams Direct Routing	Defines whether MS Teams Direct Routing is disabled on the PBX or in the SBC.
Default Tenant Dial Plan	Defines the default tenant dial plan for the site. For details, see *Configure Microsoft Tenant Dialplan* in the Core Feature Guide.
Default MS Teams Policies	These drop-downs allow you to choose the MS Teams policies to use as defaults in the SDD. Policies are synced in to Automate from MS Teams. Choosing a default policy for a site in the SDD automatically assigns the policy to user at the site. When creating a user via Quick Add User, the SDD is used, but you can also edit the configuration template for the Quick Add Group (QAG) to use a policy different to the SDD, or you can edit a user directly to choose a different policy for that user. Note that Teams Upgrade Policy is read-only in the Admin Portal as (at the time of writing) it is deprecated in the Teams online portal. See *Introduction to Microsoft Teams Policies* in the Core Feature Guide
Default Calling Line Identity	
Default Usage Location	The country for default usage.

Webex tab

The table describes settings on this tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Webex Location ID	The Webex location to which the site is mapped. Webex locations, numbers and users with location ID matching this site, will be synced to it. This dropdown allows selection of Webex locations at higher hierarchies.
Webex App - Use Organization's Domain	Displays only when: • The entitlement profile allows the Webex App service • A Webex App server is configured • The user and Webex App user have the same email address • User does not already have Jabber clients • CUCM calling behavior is not yet configured for the Webex App user Enabling this option hides the following field: **Webex App - UC Manager Profile** Default (when displayed) is unchecked (clear). When enabled, Webex App provisioning via QAS refers to values generated via the following named macros in the **device/spark/User** configuration template (CFT): • SDD_WtCallBehaviourUcManagerProfile • SDD_WtUseOrgDomain When the CFT with these macros is chosen for the QAS, the QAS uses site default values to provision Webex App (the macros allow QAS to determine whether the user has a Jabber client and whether CUCM calling behavior is configured).
Webex App - UC Manager Profile	Displays only when the following checkbox is clear (not selected): **Webex App - Use Organization's Domain** Choose the UC Manager profile from the drop-down. Options in the drop-down are the UC manager profiles added via **UC Manager Profile** (`device/spark/CallingProfile`).
Webex User Model Filter Criteria	Allows you to select predefined model filter criteria for use with the Webex user. Requires that you set up the model filter criteria so that it appears in this drop-down. You can use this option to move the user to the site when running a data sync.

Related topics

- For Webex Location ID, also see Webex Locations in the Core Feature Guide.
- Configure Microsoft Tenant Dialplan in the Core Feature Guide.
- Introduction to Microsoft Teams Policies in the Core Feature Guide.
- Microsoft Quick User in the Core Feature Guide.
- Microsoft Licenses in the Core Feature Guide
- Model filter criteria in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

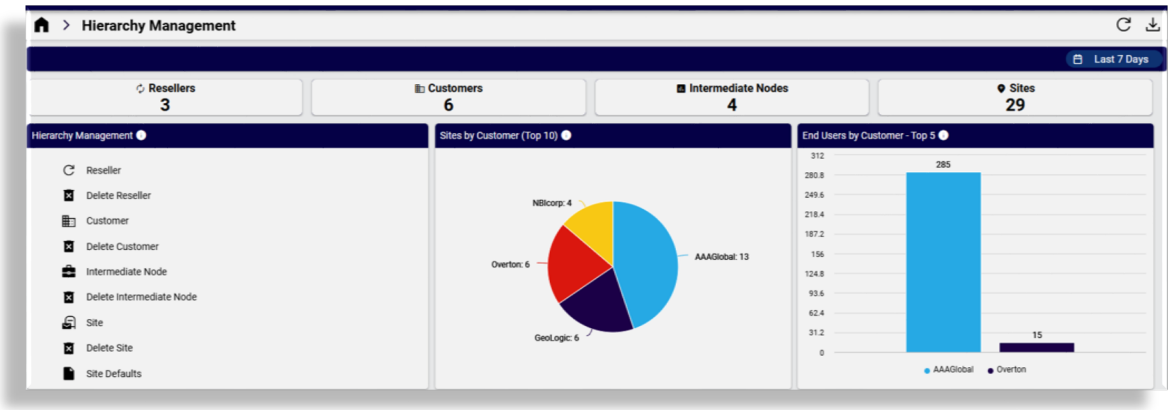
4.11. Delete a hierarchy

Tip: *Use the Action search to navigate Automate*

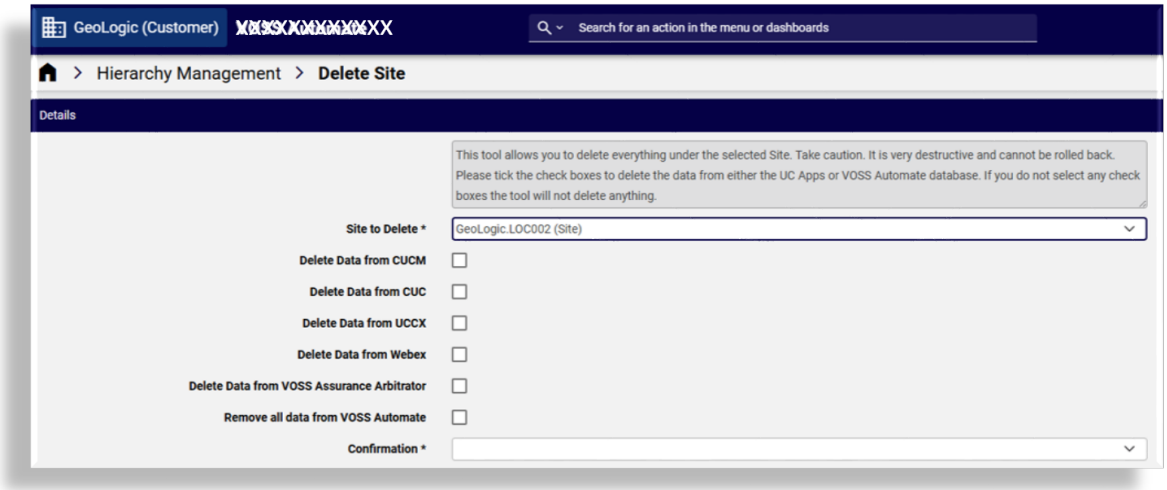
This procedure deletes a hierarchy (for example, a reseller, customer, intermediate node, or site).

Caution: Unintentionally deleting a hierarchy can have serious effects on the system. Proceed with caution.

1. Go to **Hierarchy Management**.
2. Choose an option for the hierarchy you wish to delete, for example, **Delete Reseller**, **Delete Customer**, **Delete Intermediate Node**, or **Delete Site**.



3. If you're deleting a site, choose the customer where the site exists.



4. Choose options for relevant data to delete for the selected hierarchy. Options are the same for all hierarchy types. You can remove data on selected UC apps configured on the hierarchy and completely remove all hierarchy data from the Automate system database:
   - Delete data from CUCM

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Delete data from CUC
- Delete data from UCCX
- Delete data from Webex
- Delete data from VOSS Assurance Arbitrator
- Remove all data from VOSS Automate

Note:

- If you don't select any data delete options, the hierarchy is deleted but its data is retained.
- The option to delete data from Webex does not delete Webex locations since these can only be deleted via Webex Control Hub and not via the API.
- If deleting a customer, remove any entities associated with the customer, such as LDAP, SSO providers, Devices, and NDLs.

5. At **Confirmation**, since a risk exists when using the hierarchy delete tool, you will need to select the acknowledgement for the delete/purge from the drop-down.
6. Click the toolbar **Save** icon to execute the transaction.

Note: If deleting a site, an additional cleanup workflow step also removes site-related data above the site level.

The table indicates the DN and E164 Inventory state after a site is deleted:

DN	E164	E164 Association	DN Inventory	E164 Inventory	E164 Association Flag	E164 Association
Site	Site	Site	Removed	Removed	N/A	Removed
Site	Customer	Site	Removed	Remain	set to false	Removed
Site	Customer & Site	Site	Removed	Remain at customer Removed at site	set to false	Removed

4.12. Delete issues and purges

Cisco

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.12.1. Overview

Whenever CUCM and CUCX data is synced into VOSS Automate, it assumes management of the data and, as a result, that data would be deleted by any hierarchy delete performed in VOSS Automate. These deletes can fail if your CUCM model dependencies don't reflect the additional data contained in existing, provisioned dial plans brought into VOSS Automate.

4.12.2. Preventing delete failures

There are two ways to prevent delete failures:

- (Provider deployments) Work with a Cisco System Integrator to update your HcsCucmWrapperCascadeDelPWF workflow to handle the dependencies in your existing dial plan.
- Perform a purge instead of a delete.

  Purging deletes all users, subscribers, phone, profiles, and devices from a brownfield customer's VOSS Automate while leaving these objects on the Unified CM and the Cisco Unity Connection.

4.12.3. Execute a purge

To execute a purge:

1. Log in as a Reseller administrator or higher.
2. Go to the **Data Sync** page.
3. From the hierarchy drop-downs, select the customer whose data you need to purge. If the data was created at the Site hierarchy, the purge only takes place at site level.
4. Click **HcsPurge-<IP address + fully qualified domain name + hostname>**.
5. From the **Sync Type** drop-down, choose **Purge Local Resources**. All other default values remain unchanged.
6. Click **Execute**.
7. Repeat steps 4-6 for the CUCM.
8. Verify that the instances and device models are deleted by checking Phones, Users, and Voicemail.

Note: Now you can attempt to migrate the customer into Automate by executing HcsPull from the same menu for CUCM and Unity Connection, and then running the overbuild.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4.13. Localization language

hcs-admin

Tip: *Use the Action search to navigate Automate*

4.13.1. Overview

The HCS Admin can set a default language at any hierarchy. Users and local administrators inherit the default language from the nearest hierarchy with the default language set.

Example

A Provider admin has not set a default language at the Provider level.

The provider has a reseller in Germany, so the default language at the reseller is German. This reseller has a customer in France, so the default language at that customer level is set to French. In addition, the customer in France has a site in Italy, so the default language for that site is set to Italian.

In this scenario, users that are not under the reseller have English as their language by default.

4.13.2. User default language

If a user's language is not explicitly set, the language is inherited from the nearest hierarchy node (at or above the user node) that has a default language configured. If no default language is set anywhere in the hierarchy at or above the user node, the language is set to English.

The default language can be overridden for an individual user or local administrator via the **Users** page (**User Details** tab).

4.13.3. Configure localization language

1. Log in as HCS Admin.
2. Set the hierarchy path to point to the node where you want to set a default language.
3. Go to the **Localization Language** page.
4. Click the Plus icon (+) to add a new record.
5. From the **Language** drop-down, choose the default language.
6. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

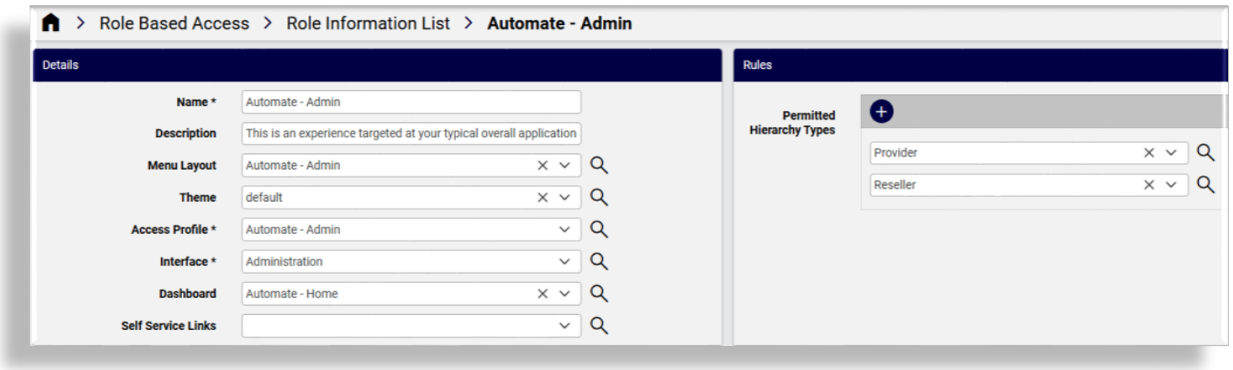
5. Role Based Access

5.1. Introduction to role-based access control

Tip: *Use the Action search to navigate Automate*

5.1.1. Overview

Automate ships with a streamlined, role-based access control (RBAC) system to manage what users can see and do across different hierarchy levels. Roles directly determine a user's interface experience, permissions, and access scope, ensuring secure and tailored access to system resources.



A user's role defines their experience and access by combining the following components:

Component	Description
Dashboard	The landing page shown after login, including widgets and links.
Menu Layout	Defines the navigation menu and associated configuration templates and field display policies (FDPs).
Theme	Controls the visual appearance of the interface.
Access Profile	Specifies permissions for accessing and managing system resources.
Interface	Indicates whether the role applies to the Administration or Self-service interface.

These components are managed via the `data/Role` model and are visible in the **Role Management** list view.

Related topics

- *Role-based dashboards and menus*
- *Introduction to hierarchies*
- *Authorized Admin Hierarchy Roles*
- *Add admin user*
- *Introduction to role-based access control*
- *Introduction to access profiles*
- *Menu layouts*
- *Introduction to Automate dashboards*
- *Menu diff tool*

5.1.2. Default experience-based roles

Automate ships with ready-to-use roles that reflect common user experiences:

- **Automate - Admin**
- **Automate - Admin - Microsoft Only**
- **Automate - License Manager**
- **Automate - Self Service**
- **Automate - Service Desk**
- **Automate - Service Desk - Microsoft Only**
- **Automate - Analyst**
- **HcsAdmin**

Each shipped role includes a predefined dashboard, menu layout, theme, and access profile. These roles reside at `hcs` level and don't require cloning as they can be assigned directly. However, the `hcsadmin` user can clone and customize them if needed.

Note: Users cannot modify their own role or its associated dashboard, menu layout, access profile, configuration templates, or field display policies.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Role-based dashboards and menus*
- *Introduction to access profiles*
- *Menu layouts*
- *Introduction to Automate dashboards*

5.1.3. Role assignment

When creating or updating a user, you can assign them a role from the available list. The assigned role determines:

- What the user sees upon login
- Which menus and actions are available
- What permissions they have
- The interface styling and layout

Roles can be reused across multiple users and assigned at any hierarchy level, provided the role supports that level.

5.1.4. Custom roles

You can create custom roles by defining your own combinations of dashboard, menu layout, theme, and access profile, or the `hcsadmin` user can clone and customize one of the predefined roles that ship with the system. All roles are managed entirely through the `data/Role` model.

Note: You cannot edit your own role.

Related topics

- *Role-based dashboards and menus*
- *Clone a role*

5.1.5. Hierarchy awareness

Role-based access control is implemented through:

- Hierarchies and user roles
- Authorized Admin Hierarchies, Authorized Admin Hierarchy roles, and roles

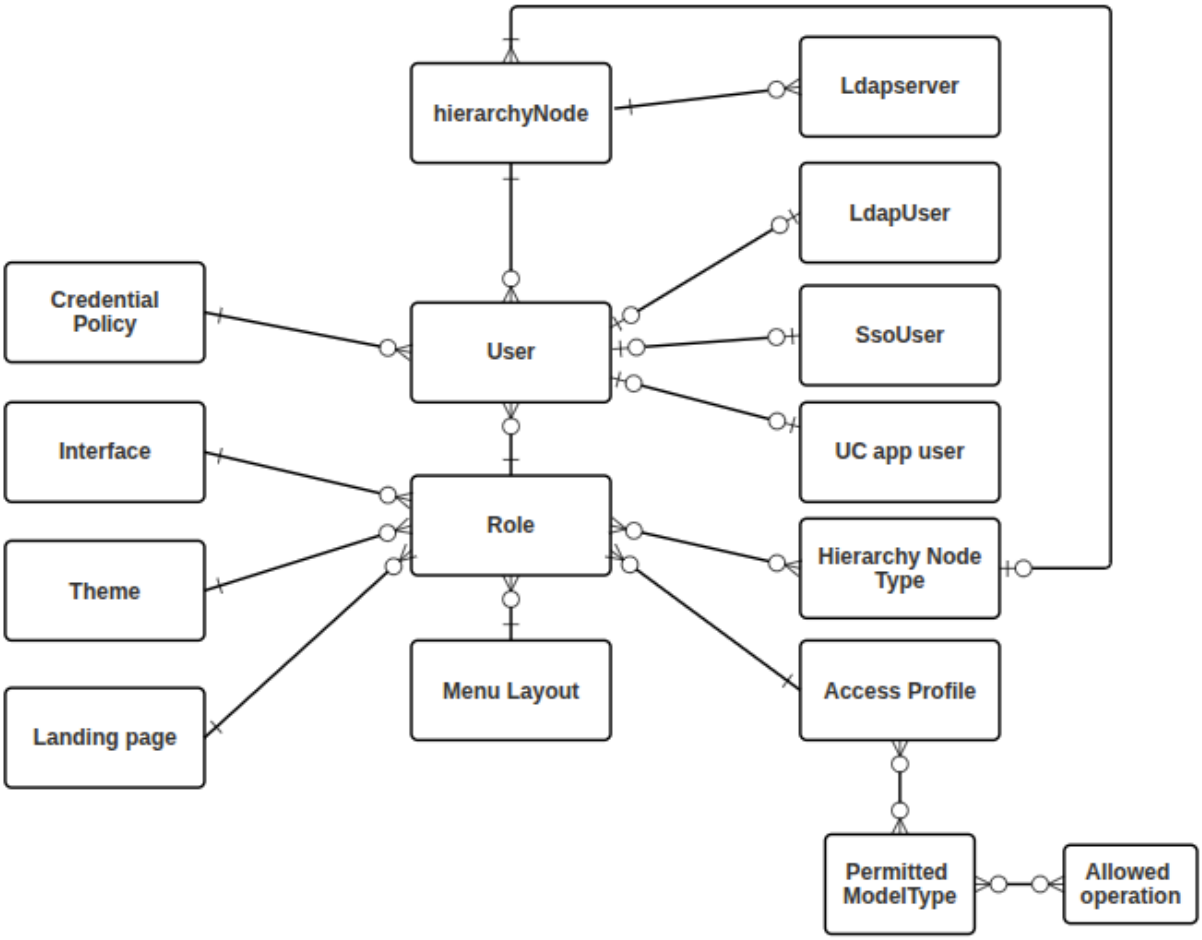
Users are created at a specific hierarchy level. They can view and manage resources only within their assigned level and below. Some roles are restricted to certain levels based on predefined hierarchy rules. For example, a site admin role may only be assigned to users at the site level.

Authorized Admin Hierarchy roles allow more flexible access configurations, where roles can be selected and added to an Authorized Admin Hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Each role includes:

- **Hierarchy rules**: Roles are only available at permitted hierarchy types defined for the role.
- **Allowed hierarchies**: Hierarchies selected from a list and applied to the role.
- **System permissions**: Access to resources and operations within the hierarchy.
- **Access profiles**: Define operations and permissions.
- **Interface customization**: Includes visibility of resource attributes, default values, and UI appearance.

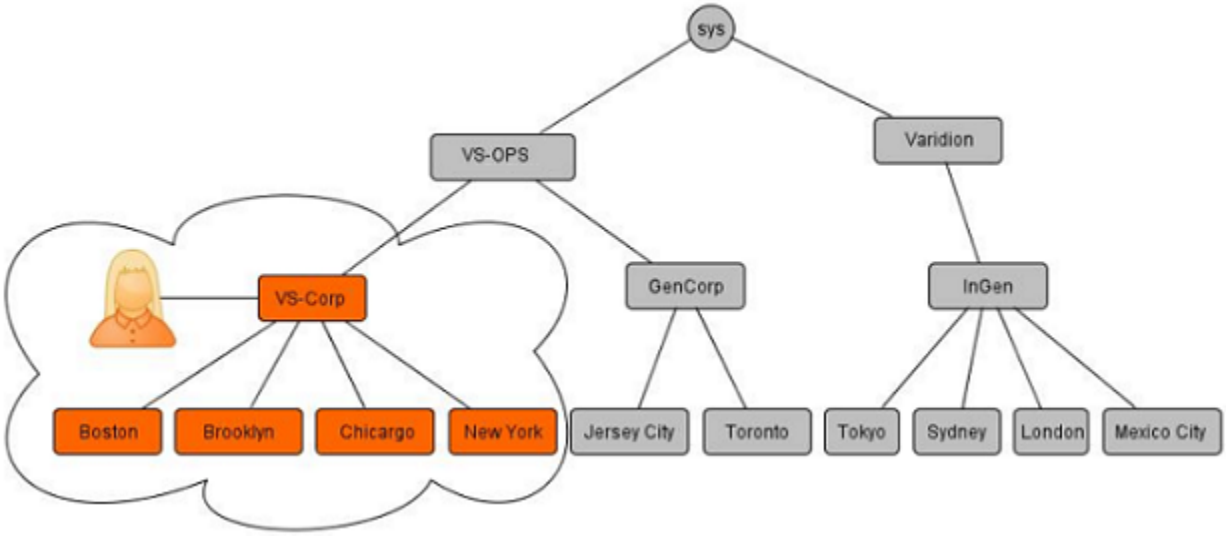


The image provides an example of the following scenario:

- A user at **VS-Corp** cannot view resources in **GenCorp** or **InGen**
- Users can navigate down the hierarchy tree but not across or above their assigned level.

This ensures that users only access data relevant to their organizational scope.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- *Authorized Admin Hierarchy Roles*

5.1.6. Authorized admin hierarchy roles

For advanced access scenarios, you can assign an Authorized Admin Hierarchy to a user via a role. This allows:

- Multi-role access: A user can operate in both Self-service and admin contexts.
- Scoped admin access: Admins can be restricted to specific hierarchy branches.

These roles are especially useful for site-level administrators who need elevated access without full system visibility.

An admin user at the Site level with a Self-service role can be assigned an **Authorized Admin Hierarchy** role that in turn contains an admin role. Such a user is then a multi-role user, so that when logged in as a self-service user, the authorized admin hierarchy role also applies. An **Authorized Admin Hierarchy** can also be assigned to an administrator, thereby only providing access to hierarchies.

Related topics

- *Authorized Admin Hierarchy Roles*

Copyright © 2025 VisionOSS Limited. All rights reserved.

5.2. Clone a role

Tip: *Use the Action search to navigate Automate*

This procedure clones an existing role so that you can customize it.

1. Log in to the Automate Admin portal.

   Note: Administrators can create or clone roles at or below their hierarchy.

2. Go to the **Role Management** list view.
3. Click on a role to view its details.
4. Click the toolbar **Clone** icon.
5. Modify the cloned role. You can update any fields.

   Ensure you provide a value or select an option for all mandatory fields (Name, Access Profile, Menu Layout, Dashboard).

   Optionally, you can also change the role description, interface (if relevant), theme, Self-service links (if relevant), or permitted hierarchy types.

   Note: The role name must be unique. Provide a descriptive name, using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscores (_).

6. Save your changes. The new role is created.

5.3. Delete unused roles

hcs-admin

Tip: *Use the Action search to navigate Automate*

This procedure deletes unused roles from all hierarchies or a selection of hierarchies.

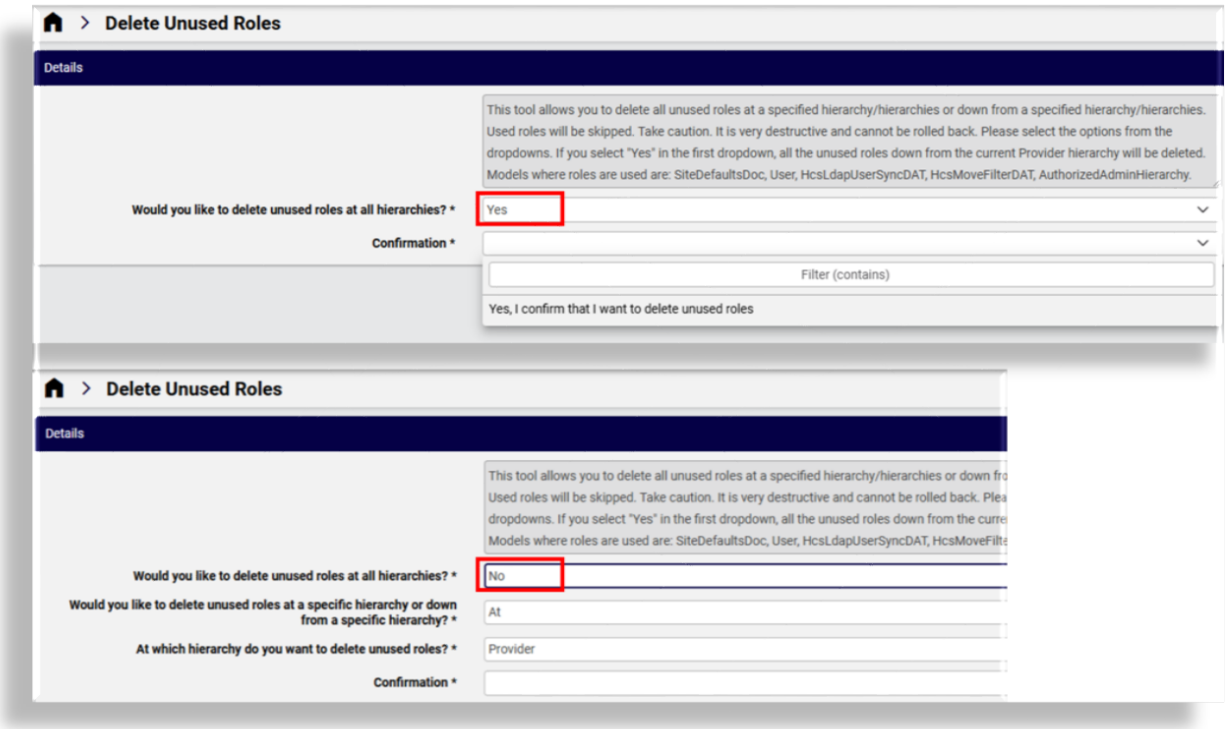
The **Delete Unused Roles** tool allows you to delete:

- *All* unused roles
- Unused roles *at* specified hierarchies
- Unused roles *down from* specified hierarchies - with the option to *select hierarchies*

Note:

- Only unused roles are deleted.
- Use this tool with caution since the transaction to delete unused roles can't be rolled back.

Copyright © 2025 VisionOSS Limited. All rights reserved.



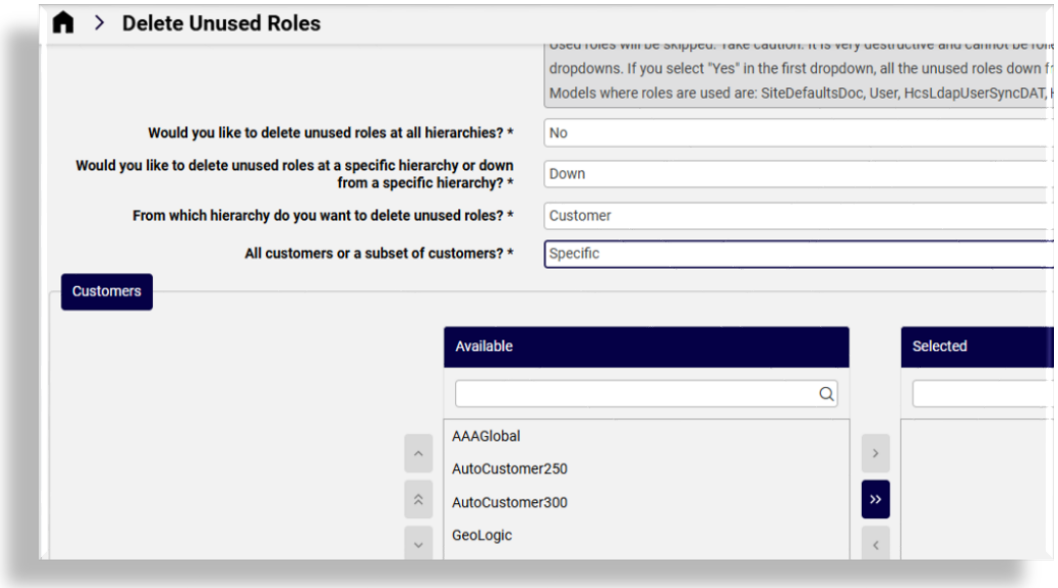
Roles are used in for example the following functional areas:

- *Site defaults*
- *Add admin user*
- *LDAP user sync*
- *Create a filter to move users*
- *Authorized Admin Hierarchy Roles*

To delete unused roles:

1. Log in to the Admin portal as `Hcsadmin`.
2. Go to **Delete Unused Roles**.
3. At **Would you like to delete unused roles at all hierarchies**, choose delete options:
   - **Delete unused roles at all hierarchies**? Select **Yes**. Confirm your choice, then save. All unused roles at the current hierarchy and down are deleted.
   - **Delete unused roles from selected hierarchies and define delete scope**? Select **No**, then:
     - Choose hierarchy scope, either **At** or **Down** from a specific hierarchy, then choose options for the selected hierarchy, for example, all or a subset of your customers, resellers, or sites.
     - If deleting from a subset of a hierarchy, choose the subset (one or more customers, sites, resellers, and so on), depending on the selected hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- Confirm your choices, then save. Unused roles are deleted for the options selected.

4. Check the transaction log to monitor progress of the role delete. See *Transaction logging and audit*.

5.4. Roles and Admins

5.4.1. Admins

Introduction to user management

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate supports various types of users:

Administrators	• Administrator users access the system to perform admin tasks • Can be assigned to any hierarchy (provider, customer, or site)
End users	• End users are provisioned with services • Can be created at any level of the hierarchy, but can only be assigned services at a site.
End User + Admin	A single user account can be configured as *both* an End User (with services) and as an Administrator by assigning an Authorized Admin Hierarchy containing a self-service role to the user - see: *Authorized Admin Hierarchy Roles*.

An Automate user exists only on Automate and represents local data associated with that user, including their user details. This user can exist on different hierarchies, and can be created independently, either on Automate directly, or imported from an external source, such as LDAP.

Non-automate users exist on the UC applications, such as Cisco UCM, CUC, Microsoft, Avaya, or Webex. These users represent UC application data and are always associated with an Automate user since they are created once the corresponding Automate user is sent downstream to the UC application. Users brought in from the UC applications are provisioned with phones and/or services only at a site on Automate.

Related topics

- User provisioning use cases in the Core Feature Guide
- Multi-vendor users in the Core Feature Guide
- *User authentication methods*
- *View users*
- *Add admin user*
- *Update a user*
- *User management scenarios*
- *User sync source*
- *User field mapping*
- *Localization language*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Users and the provisioning workflow

Users are impacted during user provisioning operations, such as LDAP sync, CUCM sync, or user bulk loading.

A typical “top-down” approach to user provisioning progresses from LDAP to Automate user, to provisioned user.

1. Sync user from LDAP into Automate. An Automate user is created.
2. Move the Automate user to a site via **Move Users**.
3. Push the user to the UC applications. The corresponding provisioned user is created either via Quick Add User or the Users page in the Automate GUI

Note: You don’t need to send all Automate users to a UC application, such as Cisco UCM, and have a corresponding provisioned user created; this is the administrator’s decision, based on criteria associated with each user. It is recommended that you filter out any users from LDAP that are not eligible for UC services. It is possible that some ineligible users can’t be filtered due to missing attributes and thus get synced into Automate. These users remain un-provisioned.

Additional functionality of Automate user

Automate users also allow:

LDAP sync	The workflows to manage syncing users from LDAP.
LDAP authentication	Enabling and disabling LDAP authentication.
SSO	Enabling and disabling SSO authentication.
Provisioning status	Tracking where the user comes from (LDAP, CUCM, manual configuration), and the hierarchy the user was originally added to.
Moving users	Between hierarchy nodes.

Automate user and corresponding provisioned user

All provisioned users have a corresponding Automate user. This allows the user to sign in to Automate (using either local authentication, LDAP authentication, or SSO authentication), and to track the provisioning status.

You can create a provisioned user via the Admin Portal, bulk load, or sync from the UC application, such as a Cisco UCM sync.

An Automate user instance is created automatically. If staging is not required (such as when configuring a user directly on a site, using bulk loading), the admin doesn’t need to add an Automate user explicitly (as a separate step).

Provisioned users at a site provide all of the UC application provisioning logic by distributing the user configuration to each of the UC applications, and combine most of the data associated with a user into one logical entity:

- Cisco UCM users
- Phones

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Lines
- Extension Mobility profiles
- Remote destinations
- Voicemail
- Webex users

A provisioned user is simply a representation of data in the UC applications. Each provisioned user is created when the UC application end user is created, and disappears when the UC application end user is deleted (either on the UC application, such as Cisco UCM directly or from Automate). This user is removed even if there are phones, lines, or profiles remaining that were previously associated with the corresponding user.

When the UC application data is created (such as the Cisco UCM end user), you can view the user in the summary list view. When the UC application data is deleted (such as the Cisco UCM end user), the provisioned user disappears.

A provisioned user is based on data in the UC applications. An Automate user is associated with local data. Any user with a UC applications end user instance displays in the **Users** list view, regardless of whether they are associated with any other data (such as phone or line).

Note: Any changes on the UC application, such as adding or deleting end users, appear in Automate only after syncing. Refer to the "Data Sync" section of the Guide for more information on data syncing.

Provisioned users are a representation of the data in the UC applications and may be updated either in Automate or in the UC applications directly.

How users are added to Automate

Users may be added to Automate from these sources:

- Synced in from LDAP, and promoted to a user (including flow through provisioning)
- Synced from Cisco UCM
- Synced from Azure (Microsoft users)
- Bulk loaded, via a Bulk loader template
- Manually created

Note: Conflicts between users synced from different sources are handled according to the strategy described in *Manage duplicate usernames*. For information about user password management, depending on the source of the user, see Password Management.

Users are typically associated with a site. You can create move filters to automatically assign users to sites once they are synced from LDAP or from CUCM. Bulk loaded and manually created users can be moved using filters or by individually selecting users.

Cisco users associated with a site can be added to the UCM that appears in the network device list (NDL) assigned to that site.

For details around how Microsoft users are synced in from Azure and then moved to the sites, refer to *Microsoft users*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Authentication on log in

Authentication (auth) methods define how a user is authenticated when logging in to Automate, either Automatic, LDAP, SSO, or Local.

If an identity provider (IdP) server is deployed at a hierarchy node above the site, you can configure Automate to provide single sign-on (SSO) support for users created or synced at that hierarchy node.

Note: Typically, Microsoft users will not need to log in to Automate. Their default auth method is Automatic. When the default auth method is set to LDAP, Automate checks with the LDAP server to verify the user's credentials. Once verified, the user is logged in to Automate.

View users

Tip: *Use the Action search to navigate Automate*

The **Admins** list view displays users at or below the current hierarchy node. Users can be created in the system in various ways, depending on your setup:

- Synced in from LDAP and promoted to a user
- Synced in from applications (for example, Voicemail or Conferencing)
- Added to Automate when creating an end user
- Added to Automate when creating an admin user

User creation can also vary across different hierarchies in the system.

Note the following user details:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Sync Source	The source application of user data, for example: **LOCAL** indicates that the user has been manually created in Automate and has not been synced from LDAP or from Cisco Unified Communications Manager (Cisco UCM). **UCM** indicates that the user exists on both Automate and Cisco UCM, and is not synced from LDAP. The user may have been created first on Automate (top-down) or created on UCM and synced into Automate (bottom-up).
Sync Type	Identifies the user that was synced from a device as indicated by **Sync Source** according to a type. The setting is read-only and assists in for example distinguishing LDAP sync users (bottom-up UCM-LDAP or or top-down LDAP). Example values: • **UCM-Local**: if the sync source is **UCM** and user is synced from Cisco UCM • **UCM-LDAP**: if the sync source is **UCM** and user is LDAP synced • **LDAP**: if the sync source is **LDAP** and user is LDAP synced • **LOCAL**: sync source is LOCAL
User Type	Administrators (**Admin**) who are users accessing the system in order to perform administrative activities End users (**End User**) that will be set up with services in the system. Users with multiple roles (**End User + Admin**)[1]
Auth Method	See: User Authentication Methods[2]
License Audit Status[3]	From release_21.4-PB5 onwards, the results of the last license counting process can be viewed as a **License Audit Status** field or when viewing a specific user. When viewing a specific user, the linked services details will indicate the services the user is consuming for further details. The license status field will indicate if the user is: • Licensed - consuming a license • Unlicensed - not consuming a license • Unknown - status has not been determined yet - typically means the user was added since the last calculation was run

- Click on a user to view its details. See also: *View a user's provisioning status*.
- Click **Add** to add a user manually.
- You can filter the **Users** list view via the toolbar **Filter** icon, then select the field (attribute), condition,

[1] **User Type**: see: *Add admin user*.
[2] **Auth Method**: see: *User authentication methods*.
[3] This column will only show after the first run of the license-audit-service. See the Licensing and Subscriber Data Export Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

and a filter value. The list view returns only those users matching the attributes you specified. For example, you may want to filter the list to display only users with authorized admin hierarchy set up.

Add admin user

Tip: *Use the Action search to navigate Automate*

Overview

- If you're adding a single role admin user and select an **Authorized Admin Hierarchy** instance that has been associated with the role, then the hierarchies set in the **Authorized Admin Hierarchy** override the default hierarchies associated with the role. See: *Authorized Admin Hierarchy Roles*.
- If you're adding a multi-role admin user, the user must first reside at site level and then be assigned a self-service **Role** by a system administrator, and a selected **Authorized Admin Hierarchy** instance that has an administrator role.

  If needed, this step should also be carried out manually in the case of synced in users or users moved to a site.

Note that enabling the system setting **Additional Role Access Profile Validation** will restrict **Authorized Admin Hierarchy** roles to those with linked access profiles that are in the *subset* of the administrator's own access profile.

If the role is set to an administrator role and an **Authorized Admin Hierarchy** instance is also specified for the user, the role on **Authorized Admin Hierarchy** takes precedence. This is NOT a recommended configuration.

Related Topics

- *Authorized Admin Hierarchy Roles*
- Additional Role Access Profile Validation in Settings topic in the Advanced Configuration Guide.

Manually add an admin user

Tip: *Use the Action search to navigate Automate*

This procedure manually adds an admin user in Automate.

1. Log in at the hierarchy node where you want to create the admin user.
2. Go to the **Users** page.
3. Click **Add**.
4. Fill out details for the admin user on tabs or panels of the *User settings*.

   Note: You'll need to fill out at least the mandatory field values. Note that the read-only **User Type** field can have the following values:

   - "Admin" - this value is defined by the admin role

Copyright © 2025 VisionOSS Limited. All rights reserved.

- "End User + Admin" - this value is defined by a `data/AuthorizedAdminHierarchy` instance associated to the user as well as a self-service role

5. Click **Save** to add the new admin user.

   You can view transaction progress and details in the Transaction Logs (when adding, updating, or deleting a user).

Important: Users are typically added or updated on Automate from the sync source, such as LDAP, Cisco UCM, or CUC. See *User sync source* for more details.

Sync source precedence may override user input. When updating a user on Automate and the following conditions exist, field values are updated from the sync source and not from data input to Automate (in this case, the fields are read-only in the Admin Portal):

- Exists on a sync source
- Has mapped fields
- Has a higher precedence than LOCAL (Automate) data

Related Topics

- *User settings*
- *User field mapping*
- *Authorized Admin Hierarchy Roles*
- *User login options by auth method and server auth scope*
- *Update a user*
- *Hybrid Cisco-Microsoft management*
- *Introduction to role-based access control*
- *User authentication*
- Transaction Logging and Audit in the Core Feature Guide

User settings

On the **Users** page you can view, add, or update a user.

You can select the following tabs/panels on this page:

Note: Click the toolbar **Switch to Tab/Panel** layout option to toggle between a panel or tab layout.

- User Details
- Account Information
- Contact Information
- Hybrid Status
- Provisioning Status

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Services
- Custom
- LDAP

Copyright © 2025 VisionOSS Limited. All rights reserved.

User Details

Fields	Description
User Name*	Sign-in username. This field is mandatory.
Local Password	The local, Automate password. The password specified when the user is manually added or provisioned in Automate.
Role*	Choose the user's role. This field is mandatory. The list of created roles to choose from include those with the current hierarchy in the **Permitted Hierarchy Types** list.[1]
Entitlement Profile	Choose the entitlement profile that specifies which devices and services the user is entitled to.
Language	Choose the user's language. Note: If no language is selected, the language is inherited from the nearest hierarchy node (at or above the user) that has a default language configured. If no default language is configured anywhere in the hierarchy at or above the user, the user's language is English. Note: If a language is manually set for a user, that language remains unchanged even if the user is moved to a new place in the hierarchy. However, if the language is inherited, then the user's language changes when the user is moved to a hierarchy node that has a different default language.
Exclude from Directory	If this check box is selected, the user will **not** appear in the corporate directory accessed via Automate Phone Services -[2]
Sync Source	Identifies the application from which the user (and user data) was synced, i.e. LOCAL (Automate), UCM or MS-LDAP. This field is read only.
User Type	Read-only. Determined by the role interface. ("Admin", "End User" or "End User + Admin") -[3]
Auth Method	Identifies the authentication method for the user -[4] This section is *applicable to End Users only*. • Local - Automate User • Automatic - If LDAP or SSO set at hierarchy or above, use this • LDAP -[5] • SSO -[6]
LDAP Server and Username	Only editable when **Auth Method** is LDAP
LDAP Username	Only editable when **Auth Method** is LDAP
SSO Identity Provider	Only editable when **Auth Method** is SSO
SSO Username	Only editable when **Auth Method** is SSO. Defaults to Automate username.
Authorized Admin Hierarchy	Selected for users with multiple user roles to enable administrative capabilities for end users or for administrators who have permissions to a restricted set of hierarchies.[7]

Copyright © 2025 VisionOSS Limited. All rights reserved.

Account Information

This tab/panel allows the administrator to manage user account information, including:

- Change Password on next Login
- Credential Policy
- Disabled (Y/N)
- Reason for Disable
- Time Locked Due to Failed Login Attempts
- Time of Last Successful Login
- Locked (Y/N)
- Number of failed login attempts since last successful login
- Time of last password change
- Time of last password change by user

Contact Information

This tab/panel is relevant only to end users.

Defines contact information for the user, such as employee number, employee type, country, state, state, street, department, manager, Fax number, directory URL, Jabber ID, telephone number, mobile, and IP phone.

Hybrid Status

This tab/panel is relevant only to end users and is available if the Global Setting **Enable Cisco** / **Microsoft Hybrid** is enabled on the **Enabled Services** - see *Global settings*.

For details on the **Hybrid Status** tab and managing hybrid users, see: *Hybrid Cisco-Microsoft management*.

Provisioning Status

Provides a read-only view of the user's provisioning status, including multi-vendor provisioning if applicable.

[1] See *Role Management*
[2] See *Configure phone services*
[3] See Authorized Admin Hierarchies and Roles under *Introduction to role-based access control*
[4] See *User authentication methods*
[5] See *View and update LDAP authentication users*
[6] See *Single Sign On (SSO) Overview*
[7] See *Authorized Admin Hierarchy Roles*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Assigned Lines

This tab/panel is relevant only for hybrid multi vendor scenarios. The fields are blank by default.

The fields on this tab are used to capture line details for users set up with an integrated service between two vendors (for example, Cisco and Microsoft).

Provisioning Status

This tab/panel is relevant only to end users.

Provides a view showing the composition of the user, this typically includes:

- Cisco UCM
- CUC
- Automate user hierarchy
- Cisco UCM user hierarchy
- CUC user hierarchy
- Cisco UCM 1 to N

Select the **Provisioned** checkbox to view additional UCM's if applicable.

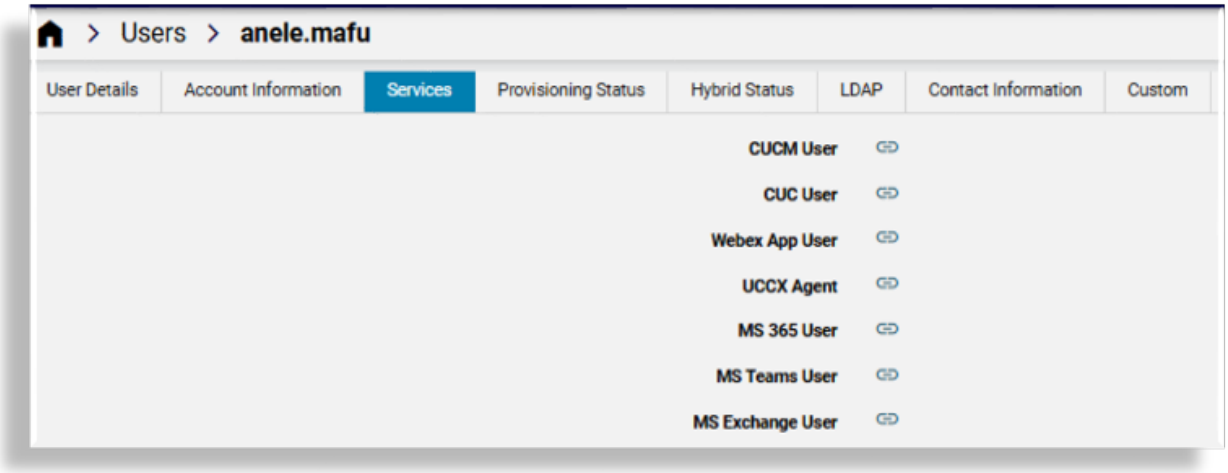
If the user is added to an LDAP server (see the **LDAP** section below), then the provisioning status will also show the server here next to the **LDAP** label.

Services

This tab/panel is relevant only to end users, and provides direct links to the user's services, typically only their available and enabled services, which may include Cisco UCM user, CUC user voicemail, Webex App user, Pexip, UCCX Agent, MS 365, MS Teams, or MS Exchange. Clicking on the link for the service opens the settings for that service. For example, clicking the link for MS Exchange user opens the user's User Mailboxes settings page.

Note: You can choose to show or hide disabled services via the **Enabled Services** tab in the Global Settings.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Custom

This tab/panel is relevant only to end users. User defined customized strings and booleans.

LDAP

If a secure Microsoft Active Directory LDAP server (port 636) is configured higher in the user hierarchy and the server has **Enable Write Operations** checked, user details can be managed on the server if it is selected from the **LDAP Server** drop down list. Only secure LDAP servers are listed. If no suitable servers have been set up, then the tab will not display any fields.

If no such Microsoft Active Directory LDAP server is configured and enabled, the tab will show a message to indicate this.

For setup server details, see: *LDAP server*. If the Microsoft Active Directory LDAP server is configured and the user already exists on this server, the tab will show a message to indicate this.

The **Description** field will display in the Microsoft **Active Directory Users and Computers** interface.

The **User Account Control** dropdown supports the following UserAccountControl values (associated with codes):

- **Normal Account** (512)
- **Disabled Account** (514)
- **Enabled, Password Not Required** (544)
- **Disabled, Password Not Required** (546)
- **Enabled, Password Doesn't Expire** (6648)
- **Disabled, Password Doesn't Expire** (66050)
- **Enabled, Password Doesn't Expire & Not Required"** (66080)
- **Disabled, Password Doesn't Expire & Not Required"** (66082)

Important:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- User management on the LDAP server from this tab/panel is *not* supported if the **LDAP server** is not secure, in other words if indicated with port `389`.
- When adding a user to the LDAP server for the *first* time:
  - A **Password** is required.
  - The **Push To Ldap** menu must be used to add the user. The **Save** menu can then be used upon subsequent user updates on the LDAP server. (If the **Save** button is used the first time, other user details will be saved, but no LDAP user is added.)

When the LDAP user is added, the **User Details** tab/panel will show the **Sync Source** and **Sync Type** of the user as `LDAP`.

For details on updating and deleting the user on the LDAP server, see: *Update a user*.

Note:

- If SSO is enabled for the hierarchy node where the user is added, the corresponding SSO user is created.
- IdPs are not configured at the site hierarchy node. Therefore, you can enable SSO for a user created at the site level only by performing these steps. Go to the **SSO User** page, click **Add**, and choose the IdP that can authenticate the user.

Update a user

Tip: *Use the Action search to navigate Automate*

Overview

Users are typically added or updated on Automate from the sync source, for example, LDAP, Cisco UCM, or CUC. See *User sync source*.

Important: Sync source precedence may override user input. If you update a user on Automate that . . .

- Exists on a sync source
- Has mapped fields
- Has a higher precedence than LOCAL (Automate) data

Only the mapped fields are updated from the sync source. Data in these fields is updated from the sync source and not the user input added in Automate. These fields are typically read-only in Automate Admin Portal.

For user authentication method (Auth Method) changes when updating, see *Authentication method setting rules*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Sync source scenarios

Updating an admin user creates a sync with the application highest on the User Sync Source precedence, and according to the field mapping for that source. The sync occurs once you click **Save**.

- *Add user sync scenarios*
- *Update user sync scenarios*
- *LDAP add sync scenarios*
- *LDAP update and delete sync scenarios*

Related topics

- *User field mapping*

Admin user password updates

If the admin user password is updated, user passwords on Cisco UCM, CUC, and Webex are also updated if these have been provisioned for the user.

Note: Since different UC apps can have different password strictness rules, the update transaction will only succeed if the strictness rules of *all* the UC apps have been met. Otherwise, the update transaction will roll back.

Administrators should therefore choose a password that meets the requirements of all the UC apps.

User added as Microsoft Active Directory LDAP user

If a user was added as a Microsoft Active Directory LDAP user (see: *Add admin user*), then:

- Additional fields on the User tabs are exposed that can be saved to the Microsoft Active Directory LDAP server.
- Updates to user details on the **LDAP** form tab will update the Microsoft Active Directory LDAP server when clicking **Save**.
- If user updates made directly on the Microsoft Active Directory LDAP server will reflect on Automate once the user is again synced in Automate from the **Sync & Purge** menu.

The table describes additional actions for managing a user. These may be found in the toolbar overflow menu of the *User settings*:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Align Hierarchy to Sync Source	For example, if the user's sync source is *UCM*, the `data/User` is at Customer level, and the *UCM* user is at Site level, then the `data/User` instance will be moved from the Customer level to the Cisco UCM's hierarchy, that is, to the Site level.
Align Hierarchy to User	All other related instances of the user (e.g. UCM, `device/cucm/User`, `device/cuc/user`, etc.) will be moved to the hierarchy of the `data/User` instance.
Delete From Ldap	Relevant only for Microsoft Active Directory LDAP server. The *delete* transaction succeeds only for users on Microsoft Active Directory LDAP servers on port `636`, where the **Enable Write Operations** setting is checked. Thus, if *Write* operations are enabled on the associated LDAP server and the LDAP server is a secured Active Directory LDAP server, the LDAP user (`device/ldap/user`) is removed, and the Automate user (`data/User`) is updated, that is, the sync type (source) is set to *LOCAL* to reflect LDAP removal. See also, *Add admin user* If there is an associated Cisco UCM user, the UCM user and the Automate user are updated. In this case: • The UCM user is converted to a non-LDAP user and the LDAP directory name is removed (set to clear) • The Automate user's (`data/User`) sync type is updated to *UCM-Local*.
Push To Ldap	Creates an LDAP user (if the LDAP user does not exist). Requires availability of an LDAP server that allows write back and is configured as a secure Microsoft Active Directory server. This server must be on port *636*, with **Enable Write Operations** checked. Used when adding user details on the **LDAP** form tab for the *first time* and first adding the LDAP user. See *Add admin user*. Clicking the **Save** button when you're done also updates the LDAP user details on the LDAP server. However, if any user details have been updated for the LDAP server, this **Push To Ldap** menu option will also save these. On the **Users** list view: 1. Click on a non-LDAP user you wish to push to LDAP. 2. On the **LDAP** tab/panel, choose the LDAP server, fill out a description and password. 3. Click **Action > Push to LDAP**. The LDAP user is created on the selected LDAP server. This menu option can't be used for Automate LDAP-synced users (in which case a system message on the LDAP tab displays the following error message: *Push to LDAP is not allowed*).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Add admin user*
- *User settings*

Manage local administrators and operators

Tip: *Use the Action search to navigate Automate*

This procedure adds administrators for intermediate nodes, and adds or edits local administrators or operators.

Note: Default local Automate administrators are created when provider, reseller, customer, and site hierarchy nodes are established.

An administrator for a particular hierarchy level can create or modify the administrators and operators at that hierarchy level and any level below. For example, a Customer XYZ administrator can create other Customer XYZ administrators and site administrators for Customer XYZ.

1. Log in as an administrator.
2. Set the hierarchy path:
   - To add or edit an administrator or operator at a level below your current level, set the hierarchy path at the top of the window.
   - If you have signed in as provider administrator and want to create a customer administrator, set the hierarchy path to the customer for which you want to create the administrator.
3. Go to the **Admins** list view.

   Note: This menu list makes use of an `[OR]` condition to filter admins: `Admin[OR]End User + Admin`. For details on the filter, see: *Working with lists*.)

4. To edit an existing administrator or operator:
   - Click on the relevant user to open the Users[username) form.
   - Make the changes you require.
   - Save your changes.
3. To add a new administrator or operator:
   - Click the plus icon (+) to open the Users/New Record form.
   - Fill out the field values. Mandatory fields are indicated with an asterisk (*):

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Username	Sign-in username. This field is mandatory.
Email Address	User email address.
Role	Choose the administrator's role. This field is mandatory. • For a provider, reseller, customer, or site administrator or operator, the available roles are limited to those applicable to the hierarchy level. • For an intermediate node administrator or operator, the available roles are limited to those associated with the nearest non-intermediate node above the intermediate node in the hierarchy.
Local Password	Set the Automate local password. This field is mandatory.
Language	Choose the administrator's language. Note: If no language is chosen, the language is inherited from the nearest hierarchy node (at or above the administrator) that has a default language configured. If no default language is configured anywhere in the hierarchy at or above the administrator, the administrator's language is English.
Sync Source	This is set LOCAL when the administrator is created on Automate.
User Type	Cannot be edited - determined by the Role interface (administration / selfservice).

5. Click **Save**.

View and update LDAP authentication users

Tip: *Use the Action search to navigate Automate*

LDAP-authenticated users display on the **Admins** page in Automate. The list view includes users that use LDAP for authentication only, and users that have been synced from LDAP.

Note: To view LDAP-authentication users only, filter the list to display **LDAP** users.

1. Log in as provider, reseller, or customer administrator.
2. Go to the **Admins** page.
3. Filter on the **Sync Source** column to display **LDAP** users.
4. Click **Add** to add a new LDAP user or select an existing LDAP user to update. For each user that uses LDAP for authentication the following information is displayed on the **Account Information** tab:

Field	Description
LDAP Server	The LDAP server being used for authentication.
LDAP Username	Matches the value of the LDAP authentication attribute which is specified in the User Model Type field of the LDAP User Sync configuration.

5. To disable LDAP authentication for a user, select the user and click **Delete**. LDAP Authentication for the user is removed from the Users list. Local authentication is used for the user to log in.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. To update LDAP authentication for a user, select the user, make the updates and click **Save**.

Note: You can update only the **LDAP Username** field. However, LDAP authentication fails if the corresponding change is not also done on LDAP.

Cisco Webex App users

Tip: *Use the Action search to navigate Automate*

Overview

You can view, update, and add Webex users into Automate via:

- Webex User Services > System User Details (add record) (`relation/User`)
- Webex User Services > Onboard User (at site) (`view/AddSubscriberFromProfile`)
- Webex User Services > Webex User Details (at site) (`relation/SparkUser`)
- Webex User Services > Webex Quick User (at site) (`view/WebexTeamsSubscriberQas`)

Note: Automate also allows for the periodic logging and inspection of changes made to data directly in the Webex Control Hub. Contact VOSS if this functionality is to be exposed. The `view/WebexAuditEvent` and `data/WebexAuditEvents` models are used for this purpose.

Related topics

- *Provisioning users with Cisco Webex*
- *Webex Quick User*

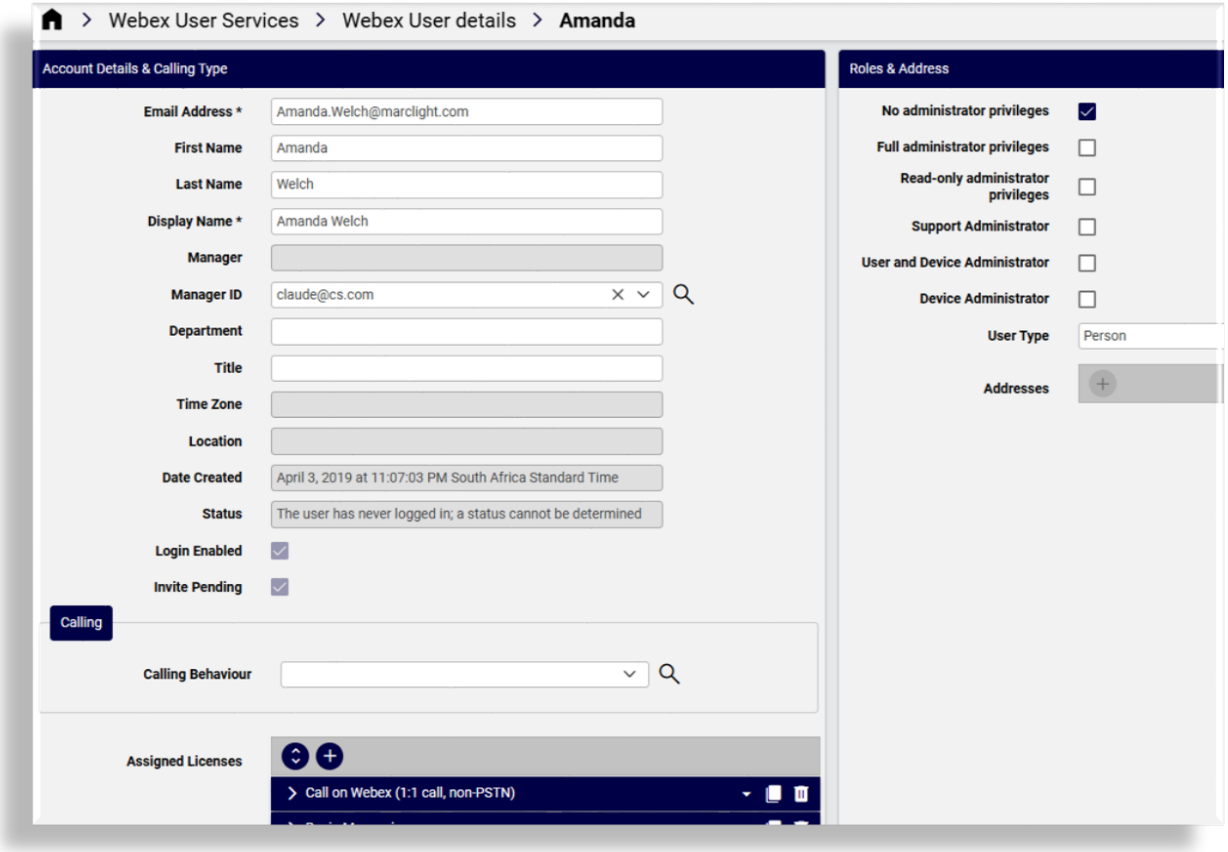
Webex User Details

This procedure displays, updates, or adds a Webex user via the **Webex User details** page (`relation/SparkUser`).

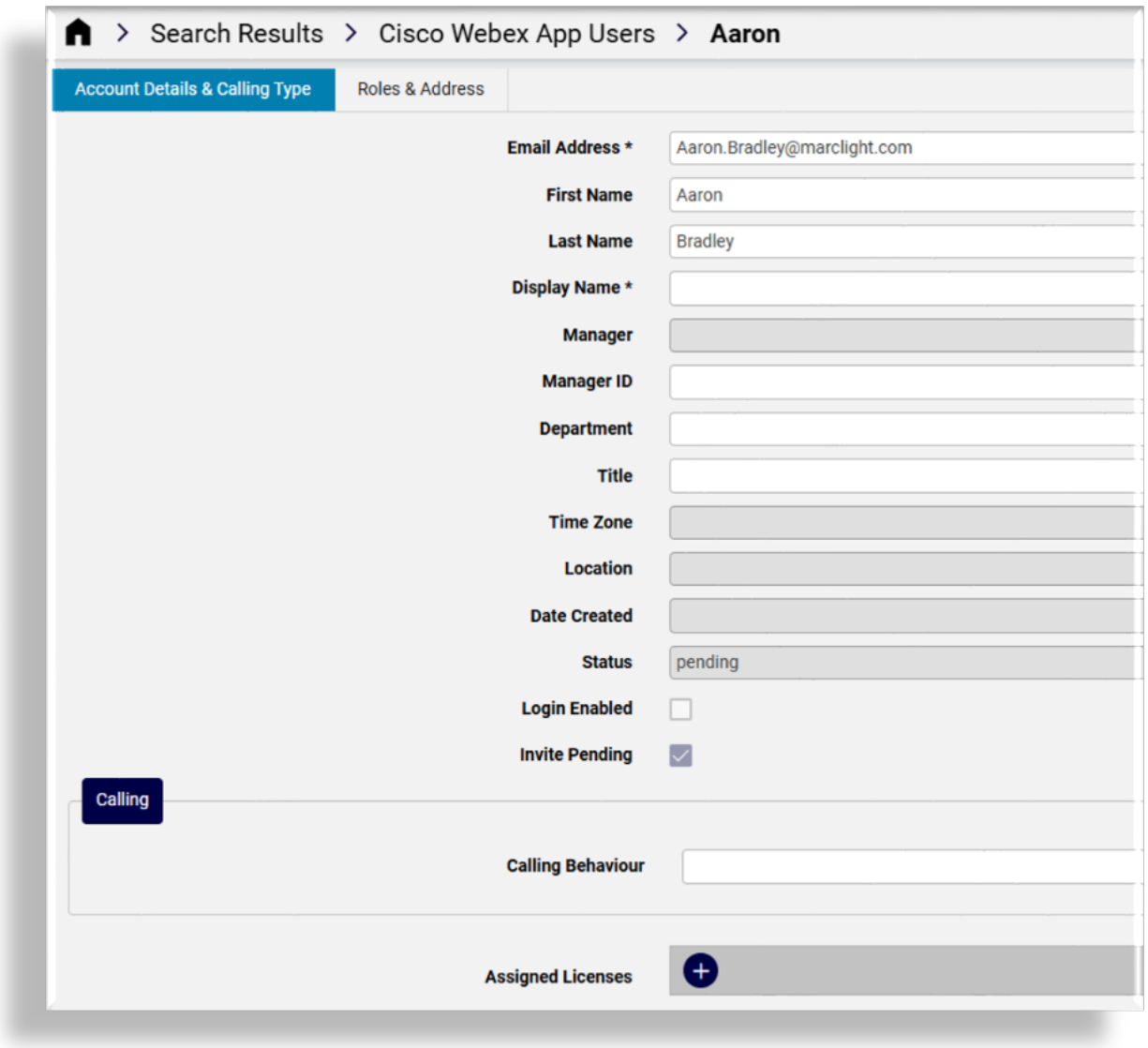
Note:

- Webex Contact Center agents can be added if a user is assigned a Contact Center Premium Agent or Contact Center Standard Agent license. Refer to the **Assigned Licenses** entry below, particularly the **Contact Center** panel form that allows for Contact Center agent management.
- You can choose phone numbers and assigned licenses. For phone number type, a Webex Calling license is required, and the Webex API (used for syncing with the Webex Control Hub) only supports add or update for phone number type *Work*.
- By default, **No administrator privileges** is enabled.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.



On the **Webex User Details** page (`relation/SparkUser`) you can view a list of Webex users in Automate, and click on a user to view or configure the following settings:

- Account Details & Calling Type
- Roles & Address
- Wholesale Package
- Calling Settings
- Contact Center

Copyright © 2025 VisionOSS Limited. All rights reserved.

View, add, or update the Webex user

1. Log in to the Admin Portal as a Provider, Reseller, Customer, or Site administrator.
2. Go to the **Webex User Details** list view.
3. Select a user to view or manage their account, or click the Plus icon (+) to add a new record, then choose the relevant site.
4. Configure account details and calling type on the **Account Details & Calling Settings** tab/panel:

   Note: Location is read-only, synced from Control Hub.

   - (Mandatory). Select an email address. This value is used to match users when they're moved during an overbuild.
   - Fill out a first name and last name.
   - (Mandatory) At **Display Name**, fill out a display name for this user, typically, name and surname.
   - At **Manager ID**, select the manager's email address.
   - At **Calling Behavior**, choose an option to auto-populate settings:

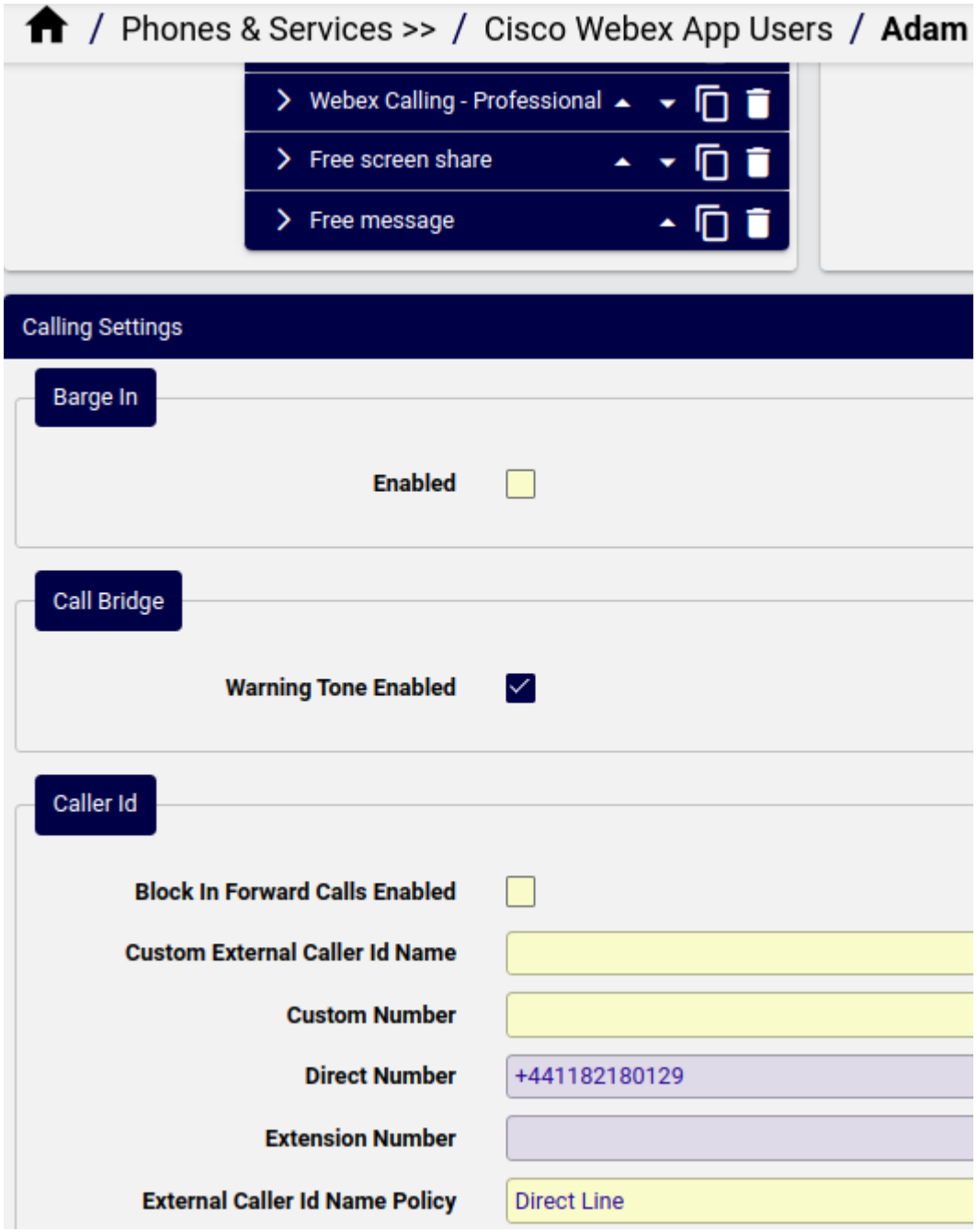
     Note: The default calling behavior is *Calling in Webex App*.

     - Calling in Webex App
     - Calling in Webex App (Unified CM)
     - Cisco Jabber app
     - Third Party app

       Note: For *Calling in Webex App (Unified CM)*, fields for device creation (Iphone, Android, CSF, Tablet) are displayed and checked by default.

   - **Phone Numbers**: The fields: **Type** (e.g. "Work") and **Number** are available for each entry.
   - **Extension**: Webex Calling extension is available if a user has a Webex Calling license.
   - **Assigned Licenses**: selected from licenses available on the Cisco Webex service as synced in from the Webex Control Hub.
     - Depending on a user's license, services such as Collaboration, Conferencing and Contact Center are available.
     - If Webex calling is enabled and a user is assigned a **Webex Calling - Professional** license, a **Calling Settings** panel on the form allows for the user management of **Calling Settings** (such as Barge In, Caller ID, Call Forward, Call Recording, Call Waiting, Intercept).

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: If a user has **Calling Settings** available, these need to be removed and to be re-provisioned if it is necessary to move the user to another site. For details, see *Move users*.

– Configure **Contact Center** settings - displays only if the user is assigned a *Contact Center Premium Agent* license. Settings include:

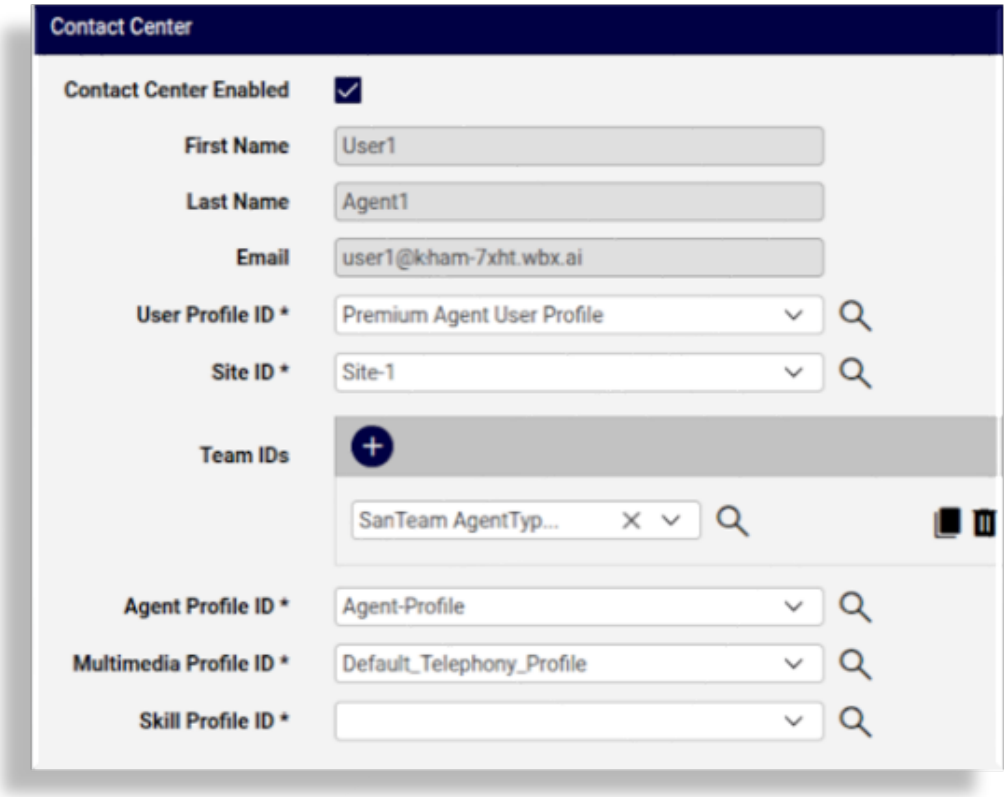
  * User profile ID, Site ID, Team IDs, Skill Profile ID. See *Introduction to Webex Contact Center* in the Core Feature Guide.

  * Agent Profile ID, Multimedia Profile ID.

Copyright © 2025 VisionOSS Limited. All rights reserved.

See *Webex Contact Center Desktop Experience* in the Core Feature Guide.

Note: At **Agent Profile ID**, all global and only desktop profiles assigned to the same contact center site as the user are available.



6. On the **Roles & Addresses** tab/panel, select relevant roles:

No administrator privileges	Default
Full administrator privileges	Assigns access to all portal features, including: • Assign roles • Company policy and templates • Device management • Licenses and upgrades
Read-only administrator privileges	Assigns read-only access to content available to a full privilege admin
Support administrator privileges	Assigns access to user information and support logs
User and Device Administrator	.
Device Administrator	.

7. If available, on the **Wholesale Package** tab/panel, manage settings for packages in the *Webex for Wholesale* service, and their status, for example, *provisioned*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

This tab/panel displays *only* when the *Webex for Wholesale* service is available. See *Webex Application Access (Webex Organization)* in the Core Feature Guide.

Depending on the package selected, the user's assigned licenses, as available on the *Webex for Wholesale* service, are then also updated when the user is provisioned.

Note: When modifying a Webex user and UCM Calling Licensing is deleted and the work phone number is also set to empty, the number is removed from the user. Work phone number remains assigned to the user if it's not set to empty.

---

8. Save your changes.

   The Webex user is added. The summary list view provides details:

   - On-Prem UCM Calling Service (True/False) - Defines whether calling services are on-premise or cloud. The On-Prem UCM Calling license is removed if the Cisco Webex Calling (with UCM) is removed from the user.
   - Calling Behavior (determines license use) - options are:
     - Calling in Webex App - Allows calling via the Webex app using native Webex calling
     - Calling in Webex App (Unified CM) - Allows calling via the Webex app using a registration to UCM
     - Cisco Jabber App - Allows calling using a Cisco Jabber client registered to UCM
     - Third Party App - Allows calling using a third party app registered to UCM
       - Use Organization's Domain (True/False) - When enabled, the Cisco Webex organization domain is used for calling in Cisco Webex (Unified CM)
       - UC Manager Profile - May be used to identify the required UCM cluster when a calling behavior using UCM is selected. If the default UCM domain is selected, this is not required.
       - User Type - "Person", "Bot" or "App User (Guest User)".
       - Status - the current Cisco Webex App user status: for example: active/inactive, in a call/meeting/presenting, and so on. If unknown, then displayed as: "The user status could not be determined".

Webex Quick User

To add a Webex user via Webex Quick User (`view/WebexTeamsSubscriberQas`), go to *Webex Quick User*.

In this case, it is recommended you add Webex App users on a Webex Control Hub with the *wholesale customer* service. See *Webex Application Access (Webex Organization)* and *Quick Add Groups* in the Core Feature Guide.

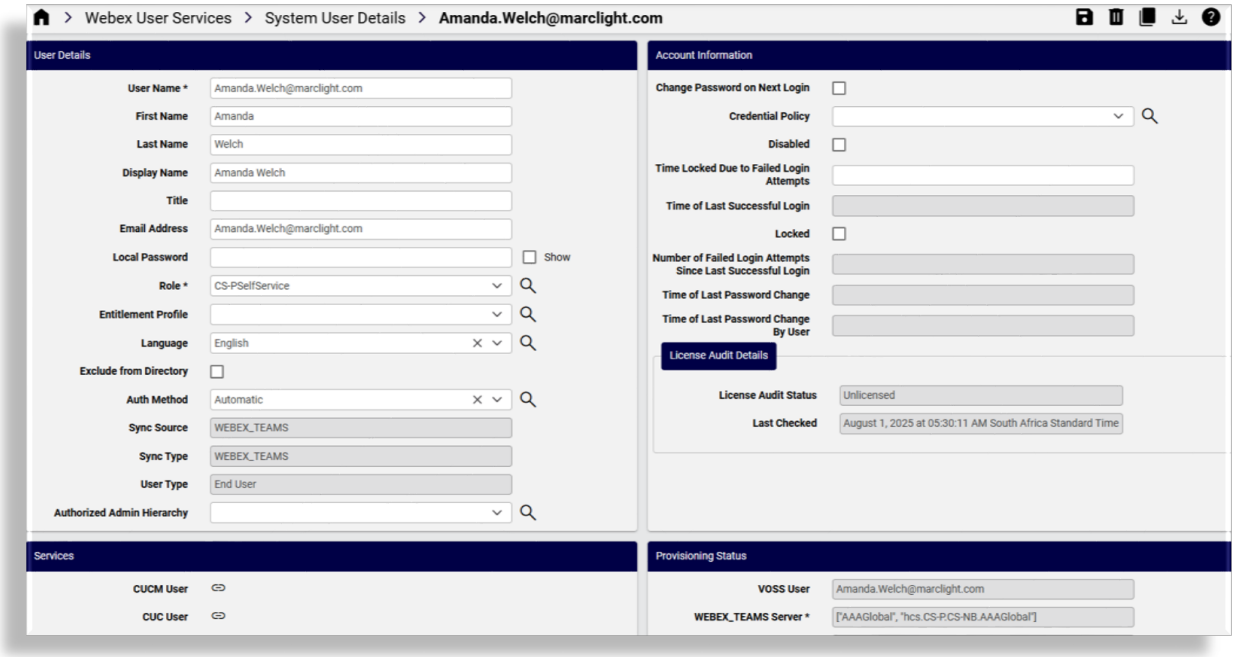
In Webex Quick User, choose a *Webex Teams User Template* from the drop-down, or use the default user template (which is referenced in the **Quick Add Groups** associated with the user).

If you want customized values, clone the *Webex Teams User Template* via the **Configuration Templates** page, and edit as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

System User Details

On the **System User Details** page (`relation/User`) you can select a Webex user to view and manage their user details (including their authorized admin hierarchy and sync source), their account information, license audit details, their provisioning and hybrid status, their contact details, and their services.



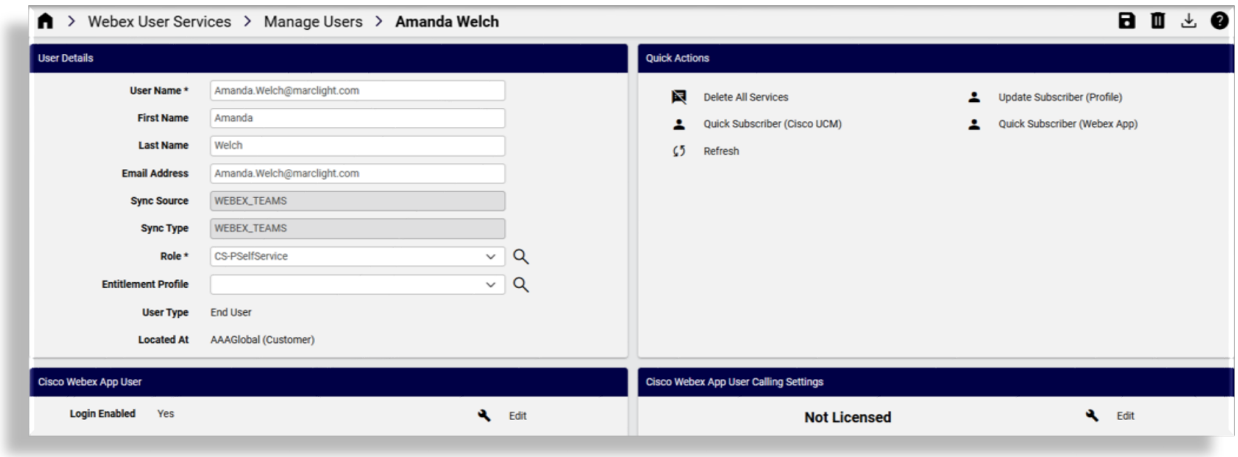
Related topics

- *View users*
- *Add admin user*
- *Update a user*
- *Manage local administrators and operators*
- *View and update LDAP authentication users*

Manage Users

On the **Webex User Services** > **Manage Users** page (`relation/MultiVendorSubscriber`) you can select a user to view and manage their user details, licenses, calling settings, phones, or services. You can also access quick actions available for the user, and enable or disable their login.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: If the user is associated with a phone (device) you can click the link adjacent to the device to go to `relation/WebexDevice` to view and manage the device settings.

Multiple Jabber devices can be added to a Webex user as long as the user does not have an existing device of the same device type.

Related topics

- *Add a user*

Sync Webex user with flow through provisioning

Sync with flow through for Webex users requires pre-configuring several settings in Automate (including flow through provisioning criteria) *before* the initial sync from the Webex Control Hub. See: *Flow through provisioning (FTP)*.

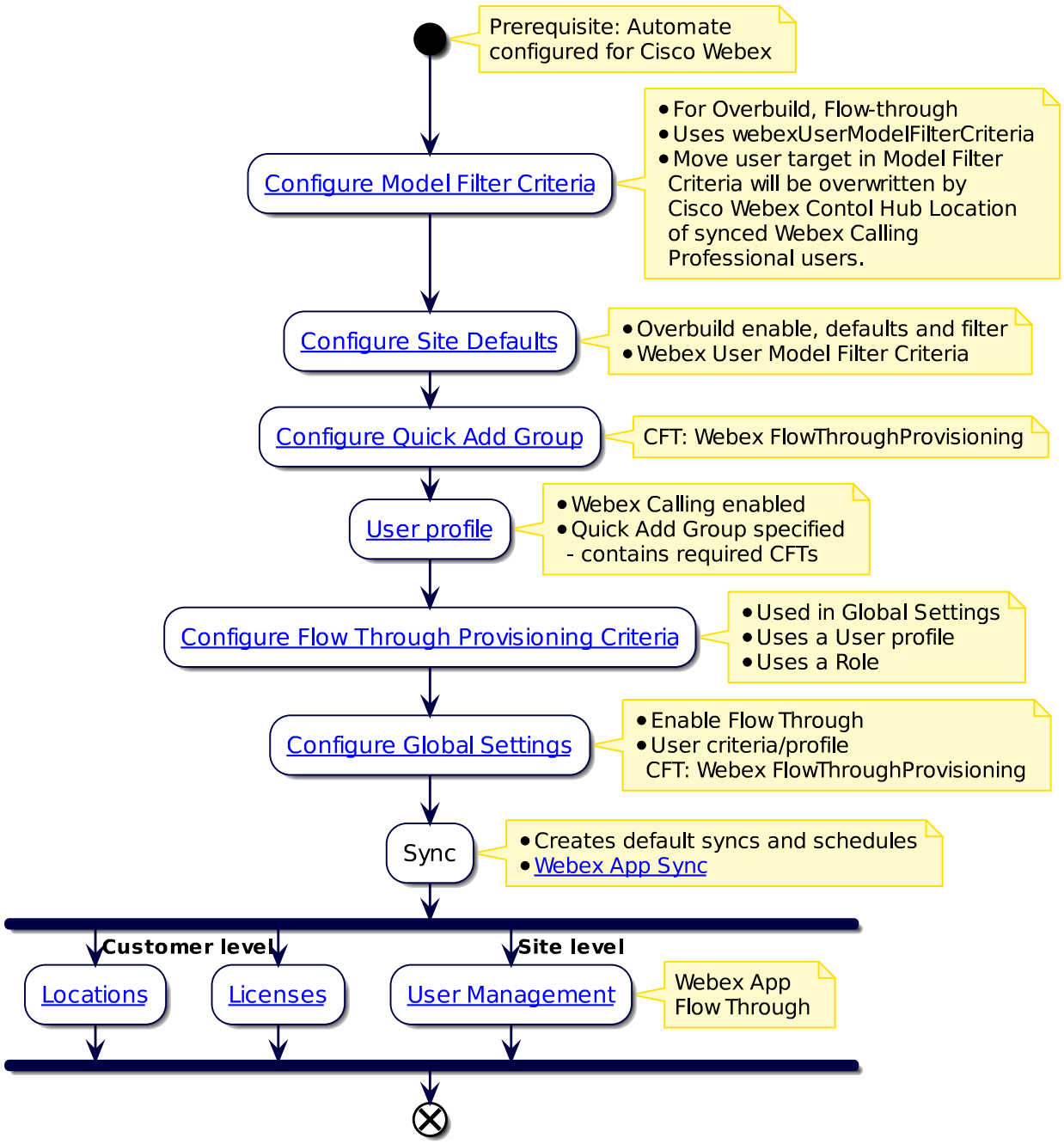
- Enable flow through provisioning in the Global Settings for a hierarchy (see: *Global settings*)
- Configure Webex settings matching the user's location in the Site Defaults (see: *Site defaults*) so that the *move filter criteria* are `webexUserModelFilterCriteria`. These criteria are used as a part of a user profile.
- The `AddSubscriberFromProfile` workflow at site uses the following configuration template: `Webex_FlowThroughProvisioning_SubscriberFromProfile`

This set up allows Automate to apply the correct configuration, licenses, and services to imported users, and to move users to sites. Once you run the sync, users are imported, provisioned, licensed, and moved to the correct synced in sites, as users - in accordance with configured Webex App user model filter criteria and user profile.

Important: For Webex Control Hub users with Webex Calling Professional licenses and a location assigned, this location won't be overwritten by any site setting configured in the Automate user move component (model filter criteria) of flow through provisioning.

The flowchart sets out the sync with flow through of Cisco Webex users and services.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Flow Through Provisioning in the Core Feature Guide

Delete a Webex user

This procedure deletes an existing Cisco Webex App user (a synced in user, or one added via Automate).

1. Log in to the Admin Portal as a Provider, Reseller, Customer, or Site administrator.
2. Set the hierarchy to the Customer or Site level.
3. Go to **Webex User Services**. Choose an option to open a list view of users. See *View Webex user*.
4. From the list view, select users to delete, one or more; then, click the **Delete** icon.
5. Click **Yes** to confirm.

Note: When deleting a user with Cisco Webex App, the internal number inventory (INI) is updated as the number status is changed to *Available*, and the description, if any, is removed.

Provisioning users with Cisco Webex

This section describes how to provision Cisco Webex for a user, either via the Users list view, or via Webex Quick User.

Related topics

- *Webex User Details*
- *Add Webex App service using Quick Add User*

Provision Cisco Webex via Cisco User list view

This procedure provisions a user with Cisco Webex, via the Cisco User list view.

Prerequisite:

- The users entitlement profile must have Cisco Webex enabled (**Webex App** checkbox must be selected).
- Unless Cisco Webex service assigned is Message only, new users must have an input line specified, and existing users must have either a primary extension, or an input line must be specified.

  See *Webex User Details*

Copyright © 2025 VisionOSS Limited. All rights reserved.

To provision a user with Webex:

1. In the Admin Portal, go to **Cisco Users**.
2. From the **Users** list, click on a user you wish to provision with Cisco Webex.
3. On the **Webex App** tab/panel, at **Webex App User**, expand and then fill out settings:

   Note:

   - The **Invite Pending** checkbox is read-only, and defines whether the user's Webex account is active (checkbox is flagged). When the checkbox is clear, the Webex account is not active.
   - Options in the **Manager ID** field and **Location** field depend on the Cisco Webex server to which the Cisco Webex Service is synced.

   - At **Calling Behavior**, choose an option, either of the following:
     - Calling in Webex App
     - Calling in Webex App (Unified CM)
     - Cisco Jabber app
     - Third-Party app
   - At **Assigned Licenses**, select a license. Options depend on the Cisco Webex server to which the Cisco Webex Service is synced.
   - At **Roles**, select relevant roles.

No administrator privileges	.
Full administrator privileges	Access to all of Portal features, including: – Assign roles – Company policy and templates – Device management licenses and upgrades
Read-only administrator privileges	View only access to privileges available to a full administrator.
Support Administrator	Access to user information and support logs.
User and Device Administrator	.
Device Administrator	.

4. Save your changes.

   The user is provisioned with Cisco Webex. To verify, ensure the value in the **Webex App** column in the Cisco Users list view is set to *Enabled*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Provision Webex user via Webex Quick User

This procedure enables Cisco Webex for a user via Cisco Quick Add User.

Prerequisite:

- The user's entitlement profile must have Cisco Webex enabled (**Webex App** checkbox must be selected).
- Unless Cisco Webex service assigned is Message only, new users must have an input line specified, and existing users must have either a primary extension, or an input line must be specified.

  See *Webex User Details* and *Add Webex App service using Quick Add User*

1. In the Admin portal, select the relevant site.
2. Go to **Webex Quick User** (`view/WebexTeamsSubscriberQas`).
3. At **Username**, select the user to be provisioned with Cisco Webex.
4. Select the **Webex App** checkbox to enable Cisco Webex for the user.
5. From the **Webex Teams User Template** drop-down list, choose the template you want to assign to the user.
6. Click **Save**. Cisco Webex is provisioned for the user.

   To verify that Cisco Webex is enabled for the user, ensure the **Webex App** column in the Users list view displays the text, *Enabled*.

Note: When Cisco Webex Calling (with UCM) is removed from a Webex User, the 'On-Prem UCM Calling' license is removed from the Webex User.

5.4.2. Role Management

Role Management

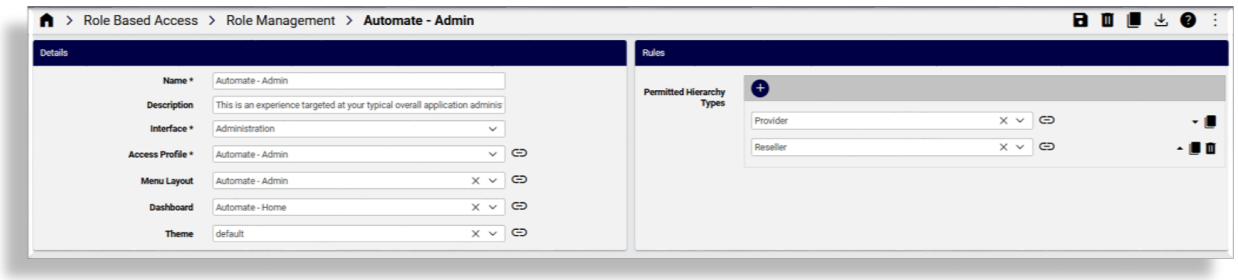
Tip: *Use the Action search to navigate Automate*

Overview

Provider administrators can manage the roles that are available for administrators, operators, and users at lower levels in the hierarchy.

Note: You cannot change your own role.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Edit a role

To edit an existing role:

1. Log in as provider administrator.
2. Go to the **Role Management** page.
3. Locate the role you want to change; then, click on the role to open it.
4. Update the role settings, as required.

   Note: The following settings are read-only for existing Self Service roles and cannot be modified:

   - Interface
   - Access Profile
   - Menu Layout
   - dashboard

5. Save your changes.

Note: If hierarchy node types are removed from the **Permitted Hierarchy Types** list while users or Site Defaults reference this node type, the transaction fails with the following message:

"Cannot update Role. Some User(s) or Site Defaults exist with the hierarchy rules defined in this role."

Add a role

To add a new role:

1. Log in as provider administrator.
2. Go to the **Role Management**.
3. Click **Add**.
4. Fill out details and hierarchy rules for the role:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Name	Mandatory. The name of the role.
Description	Description of the role.
Access Profiles	Mandatory. Specifies permissions for resources.
Menu Layout	Mandatory. Controls navigation and available actions.
Dashboard	Mandatory. Defines the landing page and widgets shown after login.
Interface	Defines whether the role applies to the Administration or Self Service interface. When selecting the *Self Service* interface the following fields are auto-populated and change to read-only (disabled) fields: • Interface (with value *Self Service*) • Access Profile (with value *default_selfservice_access_profile*) • Menu Layout (with value *selfservice*) • Dashboard (with value *selfservice_dashboard*)
Theme	Controls the visual appearance of the interface.
Self Service Links	Provide useful links to Self-service end users.
Permitted Hierarchy Types	Hierarchy types the role you're working with can be added under. If no hierarchy types are specified, the role can be added under any (non-sys) hierarchy. Once you add a permitted hierarchy type, the system validates that a user you're creating with this role is at that hierarchy level before it creates that user. If the user does not exist at that hierarchy the transaction fails. Refer to *Permitted Hierarchy Types List Impact* below. When the role is saved, the selected **Hierarchy Type** is added to the **Hierarchies Allowed** list if it is not included.

5. Click **Save** to add the role.

Permitted Hierarchy Types List Impact

The following areas in the system are impacted by list entries available in the **Hierarchies Allowed List** of a role:

- *Authorized Admin Hierarchy Roles*
- *Move user & services*
- *Add admin user*
- *Create a filter to move users*
- *Move users*
- *Move user*
- *Site defaults*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Microsoft-only role

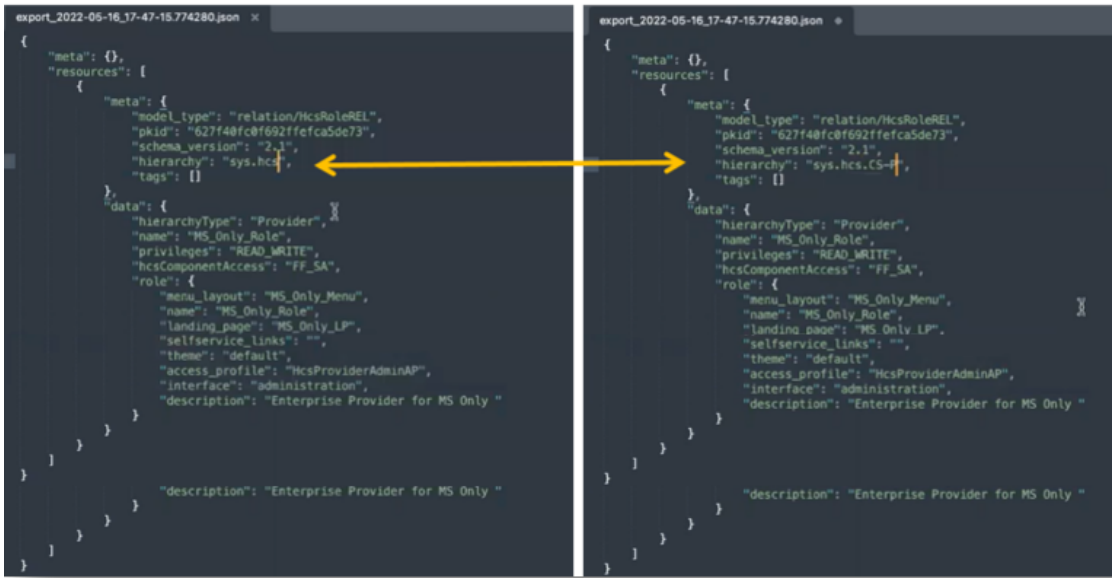
Starting with version 21.3-PB1, Automate ships with a Microsoft-only role (`MicrosoftOnlyRole`) and accompanying role-based access control elements, which are predefined for a Microsoft-only user interface experience. These elements include predefined field display policies, dashboards (`MicrosoftOnlyDashboard`), and menus (`MicrosoftOnlyMenu`). Installing these templates provides the baseline for a Microsoft-only version of Automate, and hides non-Microsoft GUI elements, such as the FDPs, menus, and dashboards reflecting functionality used for managing Cisco devices.

To use the `MicrosoftOnlyRole` in Automate:

1. Log in to Automate as *hscadmin*.
2. Go to the **Roles** page.
3. Locate **MicrosoftOnlyRole** in the list view.
4. Select the role in the list (or click on the role to open it).

> **Note:** This role ships with a standard access profile and a predefined menu layout and dashboard.

5. Click **Export** to export the role to a JSON file, and save the file to your local computer.
6. Edit the JSON file to specify the hierarchy where you want to use the role.



7. Go to the **Import** page.
8. Browse to the location you saved the JSON file, then click **Import**.
9. Go to the **Role Management** list view to verify that the role now exists also at the hierarchy you specified.
10. At the hierarchy where you wish to assign the role to a user (Provider or Customer), go to the **Admins** page. Choose a user (or add a user), then on the **User Details** tab, from the **Role** field, choose the role (`MicrosoftOnlyRole`) you imported to this level, and save your change.

Copyright © 2025 VisionOSS Limited. All rights reserved.

5.4.3. Authorized Admin Hierarchy Roles

Authorized Admin Hierarchy Roles

Tip: *Use the Action search to navigate Automate*

Overview

The **Authorized Admin Hierarchy Roles** feature in Automate addresses two general use-cases in administrator management (a combination of these solutions can also be applied).

1. For an administrator who needs a single user account configured as both an end user (with services) and an administrator.

   This supports the following:

   - A single set of credentials for administration and end user access
   - Simplified external authentication (LDAP and SSO)
   - Support for concurrent use of both admin and self-service portals in same browser

   For further details, see: *End User and Administrator details*.

2. For an administrator who needs to manage administrative domains outside of a single hierarchy, access to a matching subset of hierarchies can be configured, for example, for a customer administrator who administers only a subset of sites in customer hierarchies (one or more), the feature allows access to the matching subset of sites.

   This restricted access applies to any hierarchy-related activities and items - tasks and elements that rely on or reside at a specific hierarchy.

   Note:

   - If a hierarchy is authorized, the authorization *also applies to any child hierarchy* nodes of this hierarchy.
   - The `LinkedSite` hierarchy node type is included in the `Site` node type authorization.
   - An administrator who is configured as both an end-user and administrator can therefore also be an administrator who has been set up with an authorized admin hierarchy role.
   - Some functionality in Automate requires access to *all* lower hierarchies, so that an authorized admin hierarchy role needs be configured accordingly to use the feature. For example, for the Overbuild feature, the administrator must have permissions to the customer "From" hierarchy, which implies access to *all* sites under the customer. On the default dashboard and menu items providing access to the Overbuild feature, a macro condition with a hierarchy node type set to `Customer` needs to evaluate to `true` before the items are accessible:

     ```
     (( fn.authorized_admin_allowed_hierarchy_level Customer == fn.true ))
     ```

     For details on the macro, see the Hierarchy functions topic in the Macro Functions section of the Advanced Configuration Guide.

   The following areas are for example impacted by the subset of hierarchies:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- List views reflecting items at a hierarchy
- Drop-down lists on a form that are related to hierarchy elements
- Filtered views and lists
- Tree views showing a hierarchy exposed to the administrator

  Items within hierarchy trees but outside of the allowed subset of hierarchies will not be available to be managed and are only be shown to indicate where allowed hierarchy elements reside in the hierarchy tree. For example, if sites from multiple customer hierarchies are allowed, then the display of these sites in the hierarchy tree may require showing the parent customer node, but the customer hierarchy will not be available for management.
- Dashboard data displayed in widgets - obtained from resources that reference data at allowed hierarchies
- Transactions and transaction views
- Search results

  When a global search is performed, the results that are returned are filtered by the administrator's allowed hierarchies.
- Workflows and actions carried out by the system API involving macro queries
- Management activities on items at a hierarchy (Modify, Add, Create, Delete). This includes bulk load activities.

Important:

- Where this feature is used by an administrator, the administration tasks and concepts described in the documentation should be read and understood in accordance with the restricted access that applies to such an administrator.
- The selection of hierarchies for authorized admin hierarchy roles is carried out by means of transfer boxes. This feature supports a maximum of 500 entries, so that a **Selected** list can be up to 500 hierarchy entries. Customers wishing to select more hierarchies must contact VOSS through their account manager or support. Significant performance degradation might be experienced with more than 500 entries.

For further details, see: *Administrator access to a subset of a hierarchy details*.

Manage Authorized Admin Hierarchy Roles

Note: If the authorized admin hierarchy role is to be applied to an administration user, this hierarchy needs to be the same or above the hierarchy as the user (`data/User`).

To create an instance of an authorized admin hierarchy role at the relevant hierarchy level:

1. Log in and go to the **Authorized Admin Hierarchy Roles** page.
2. To add or modify an **Authorized Admin Hierarchy Roles** instance, either add or modify the instance **Name** and select the **Role**.

   Available roles will also include those roles containing the current hierarchy where the created Authorized Admin Hierarchy instance resides, in their **Hierarchies Allowed** list - see: *Role Management*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. The **Available** list of the **Allowed Hierarchies** transfer box (displayed in a shortened format, with type indicator added) shows the items below the hierarchy of the **Authorized Admin Hierarchy Roles** instance to which the current administrator has access, for example:

   Using the side-by-side controls, move the required hierarchies to the **Selected** list in accordance with your needs, for example, so that they correspond with the administrative domains needed by the administrator that you wish to create. Recall that if a hierarchy is selected, the authorization *also applies to any child hierarchy* nodes of the selection.

   Note:

   - The transfer box in this feature supports a maximum of 500 entries, so that a **Selected** list can be up to 500 hierarchy entries.
   - The selection of hierarchies in the transfer box is not mandatory: if no hierarchies are selected, the created authorized admin hierarchy role will have access to the hierarchies as per the role settings and position in the hierarchy structure.

4. Click **Save**

This authorized admin hierarchy role can now be assigned to:

- an administrator on the **Admins** page
- a user on the **User Details** page

The created **Authorized Admin Hierarchy** is available in the drop-down list *at the created hierarchy* on the form and can then be selected.

Important: If an **Authorized Admin Hierarchy** is assigned to a user, the allowed hierarchies of this authorized admin hierarchy role override the default **Hierarchies Allowed** to a user if they were only assigned a role - see: *Role Management*.

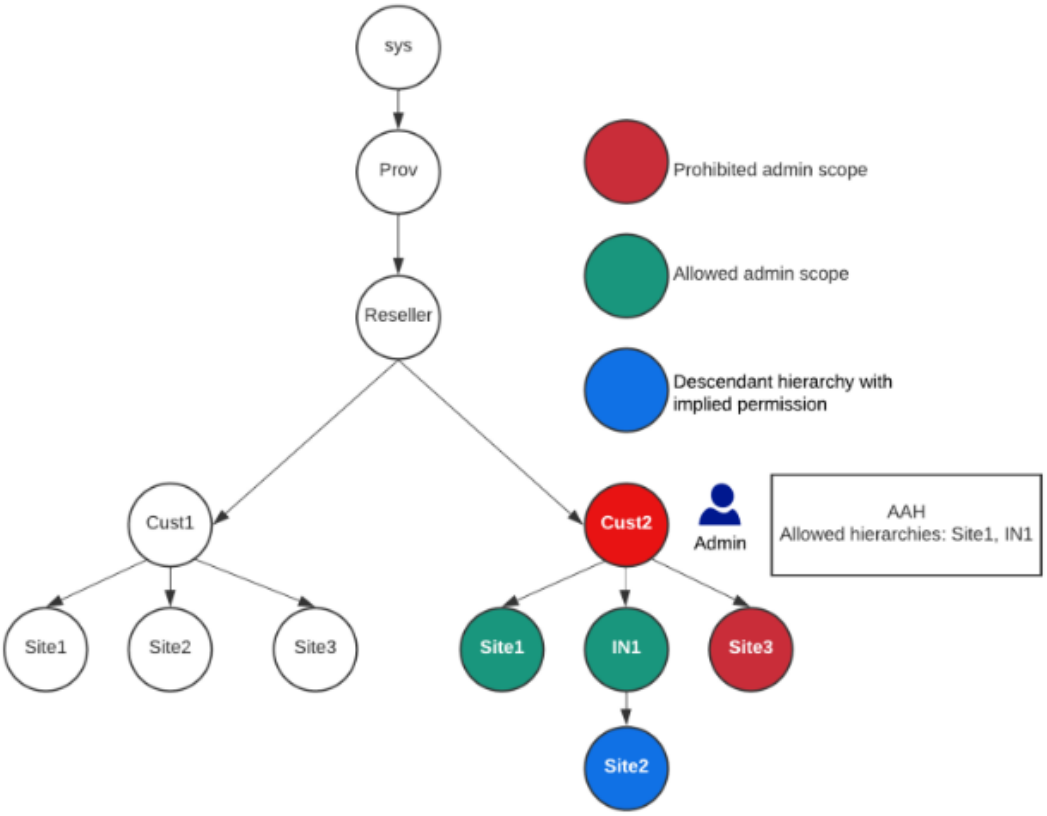
Copyright © 2025 VisionOSS Limited. All rights reserved.

Administrator access to a subset of a hierarchy details

This section provides further details on and examples of the behaviour of Automate when an administrator has been assigned an Authorized Hierarchy Roles instance.

Hierarchy access illustration

Consider an administrator added at a customer level hierarchy (`Cust2`) where the selected hierarchies of the assigned **Authorized Admin Hierarchy** (AAH) are: `Site1` and `IN1` (Intermediate Node 1) (green nodes in the diagram below).



This administrator can only view and manage resources at:

- `Cust2.Site1`
- `Cust2.IN1.Site2`, since `IN1` is authorized and `IN1.Site2` is a child hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Authorized Admin Hierarchy and user management

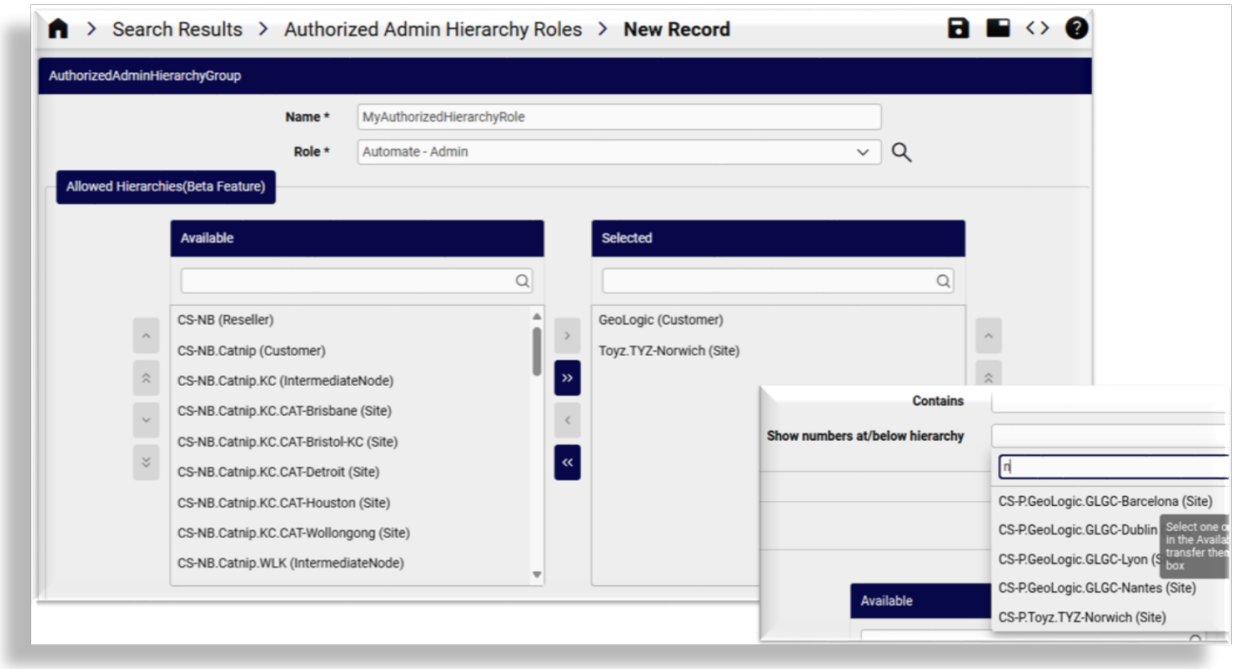
For an administrator with an authorized admin hierarchy role that also manages the authorized admin hierarchy role of a user, this management (for example, selection/removal of hierarchies) is restricted by the allowed hierarchies of the administrator. In other words, an administrator can only add/modify `data/AuthorizedAdminHierarchy` instances with `allowed_hierachies` that are set to those hierarchies that the administrator has access to.

For user management, a site administrator cannot for example carry out updates on a user who has administrator access to both the parent customer hierarchy and who also has self-service user access to the same site.

For example, an administrator with access to a limited subset of hierarchies can only change the password of another user on condition that the administrator has access to all the hierarchies that the other user has access to. This prevents privilege escalation by password change.

Authorized Admin Hierarchy Roles display on the user interface

Below are a number of examples on the user interface that reflect the display seen by an administrator with an authorized admin hierarchy role that contains the following selected hierarchies in a hierarchy tree:



- a customer hierarchy node: `Geologic (Customer)`
- a single site hierarchy node below a customer `Toyz (Customer)` called `TYZ-Norwich (Site)`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Hierarchy tree

Note that the displayed tree reflects nodes that are not selected hierarchies: `Toyz (Customer)` and `CS-P (Provider)`. These nodes are included in the tree view in order to show the hierarchy context for the selected hierarchies.

List view (users)

A user list only shows users located at hierarchy nodes matching the authorized admin hierarchy role associated with the administrator.

	User Name	Role	Located At
	Filter	Filter	n
	Abel.Timoteo	GLGC-LyonSelfService	GLGC-Lyon (Site)
	AlissaS@lrzg.onmicrosoft.com	ToyzSelfService	TYZ-Norwich (Site)
	Ardelia.Mobley	GLGC-DublinSelfService	GLGC-Dublin (Site)
	BethanK@lrzg.onmicrosoft.com	ToyzSelfService	TYZ-Norwich (Site)
	Carla.Noone	GLGC-LyonSelfService	GLGC-Lyon (Site)
	Chanda.Powley	GLGC-LyonSelfService	GLGC-Lyon (Site)
	ClydeM@lrzg.onmicrosoft.com	TYZ-NorwichSelfService	TYZ-Norwich (Site)
	Cris.Torrey	GLGC-BarcelonaSelfService	GLGC-Barcelona (Site)

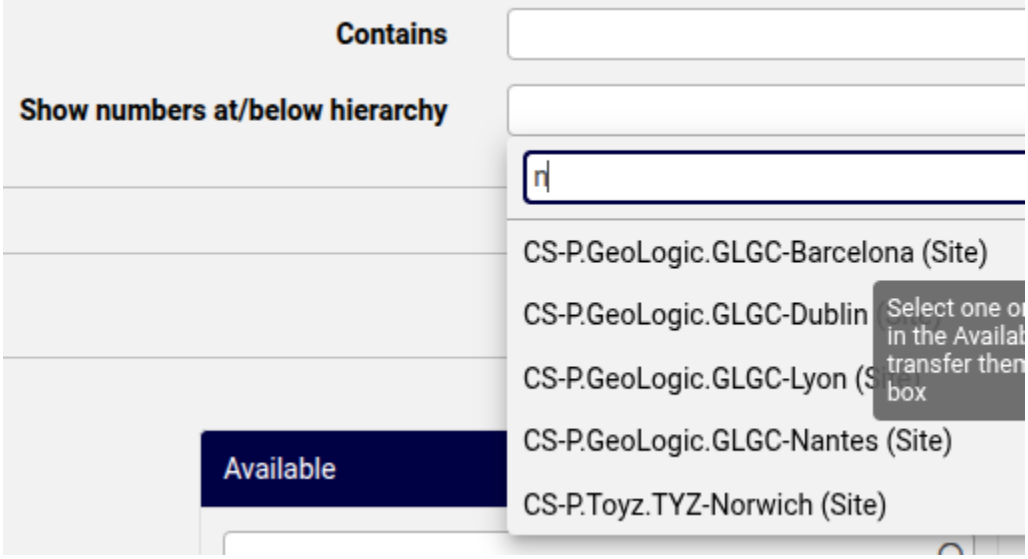
Copyright © 2025 VisionOSS Limited. All rights reserved.

Filtered lists

Authorized hierarchy filtered drop-down lists include:

- List of users on the Quick User form
- Hierarchy choices when Quick User is triggered while at non-site hierarchy
- Network Device Selection pop-ups
- Hierarchy choices in Internal Number Inventory forms

Example of filtering during number management:



Overbuild

The administrator *must* have permissions to the customer "From" hierarchy, which implies access to all sites under the customer.

On the default dashboard and menu items providing access to the Overbuild feature a macro condition at the customer hierarchy needs to evaluate to `true` before the items are accessible:

```
(( fn.authorized_admin_allowed_hierarchy_level Customer == fn.true ))
```

See: the Introduction to Overbuild in the Core Feature Guide.

Microsoft License Allocation

Where Microsoft 365 user licenses are available to an organization as a whole on a single Microsoft tenant and Automate is used to support for the allocation of these licenses to various business units and departments within such an organization represented as hierarchies in Automate, the number of un-allocated licenses shown as **Maximum Limit Allowed** on **Microsoft License Allocation** will however show total values that *include* hierarchies excluded from the administrator's allowed hierarchies.

This complete total is shown to ensure that such an administrator has an accurate view of available licenses for allocation.

For details on this feature, see *Microsoft license management and alerting* in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Authorized Admin Hierarchy Roles and number management

Number range management is only available for specific authorized admin hierarchy roles: if the authorized admin hierarchy role associated with an administrator does not include customer-level hierarchies, it is not available, since the Automate API only allows for the creation of a number inventory at the customer hierarchy.

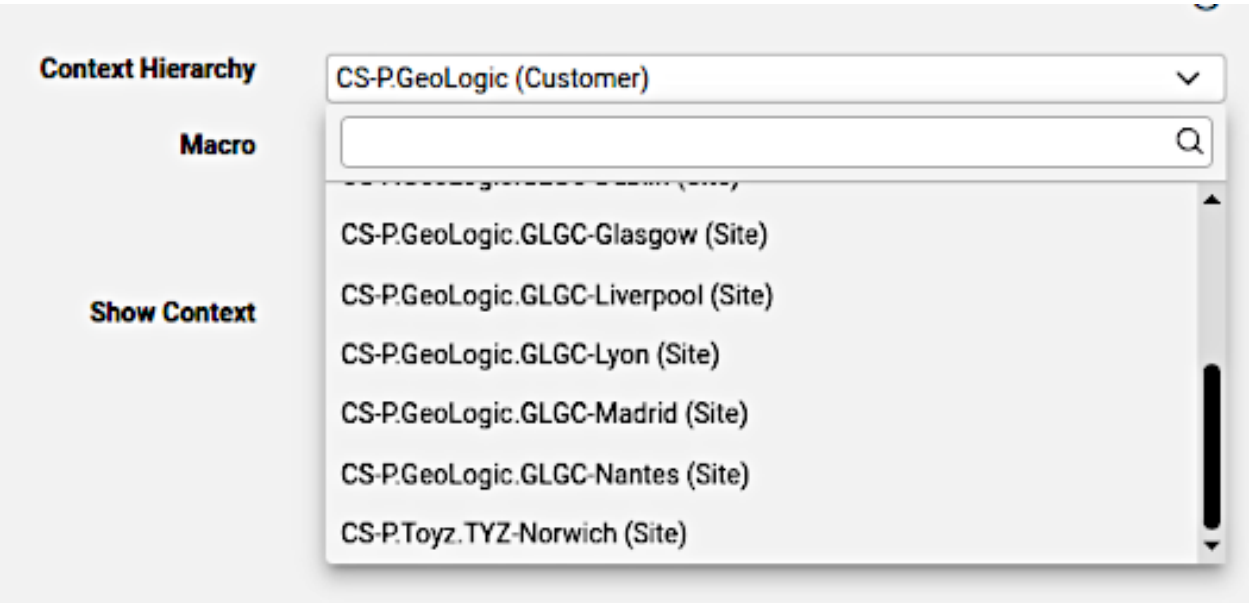
As an example of number range visibility by hierarchy, consider an administrator with authorized admin hierarchy roles access to intermediate level A and thus has access to all the sites under this level. In addition the administrator has access to only one or two sites from intermediate level B. In accordance with the site the administrator is at, the visibility of numbers will be from that site level upwards in the hierarchy. The intermediate level A numbers will thus not be visible if the administrator is at a site under intermediate level B.

See: *Number range management*.

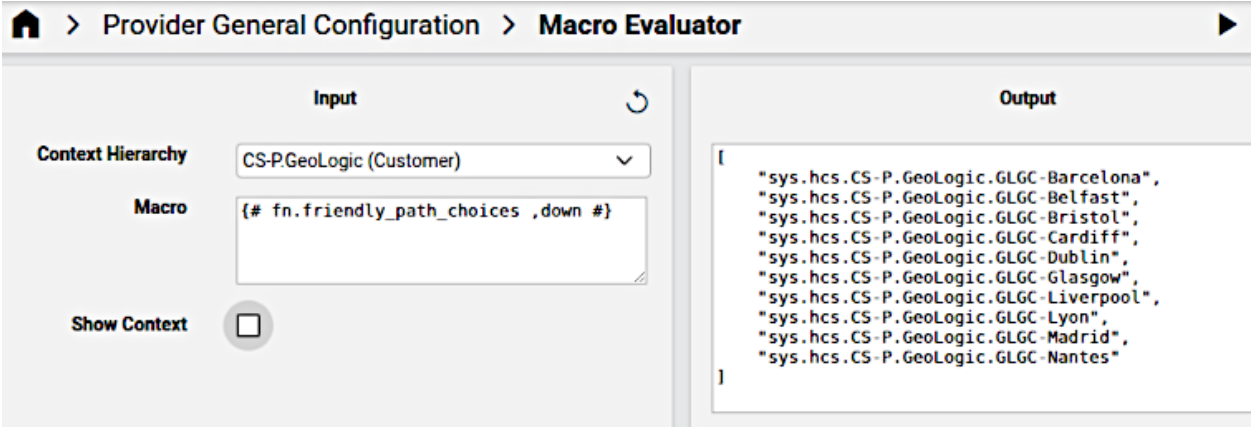
Authorized Admin Hierarchy Roles on the system API

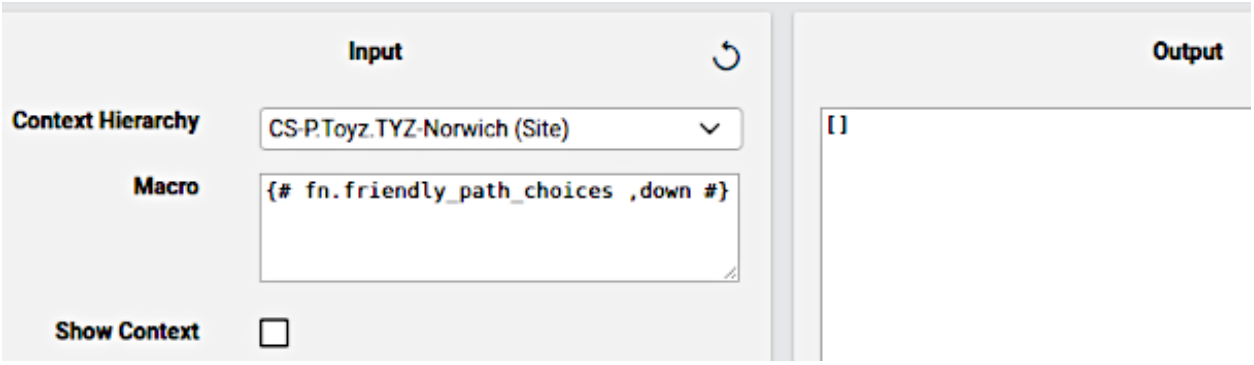
Tasks and activities involving the system API are also in accordance with the authorized admin hierarchy role associated with the administrator.

This can for example be seen when using the **Macro Evaluator**



Copyright © 2025 VisionOSS Limited. All rights reserved.





Macros and macro functions are integrated into API related system workflows and elements such as configuration templates and GUI rules.

Similarly, a **Bulk Load** JSON file or MS Excel sheet load transaction containing an update request for a user outside of the authorized admin hierarchy role associated with the administrator will yield an appropriate error:

```
The current request user does not have sufficient
allowed hierarchy access to modify a
user with Authorized Admin Hierarchy set to ...
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

End User and Administrator details

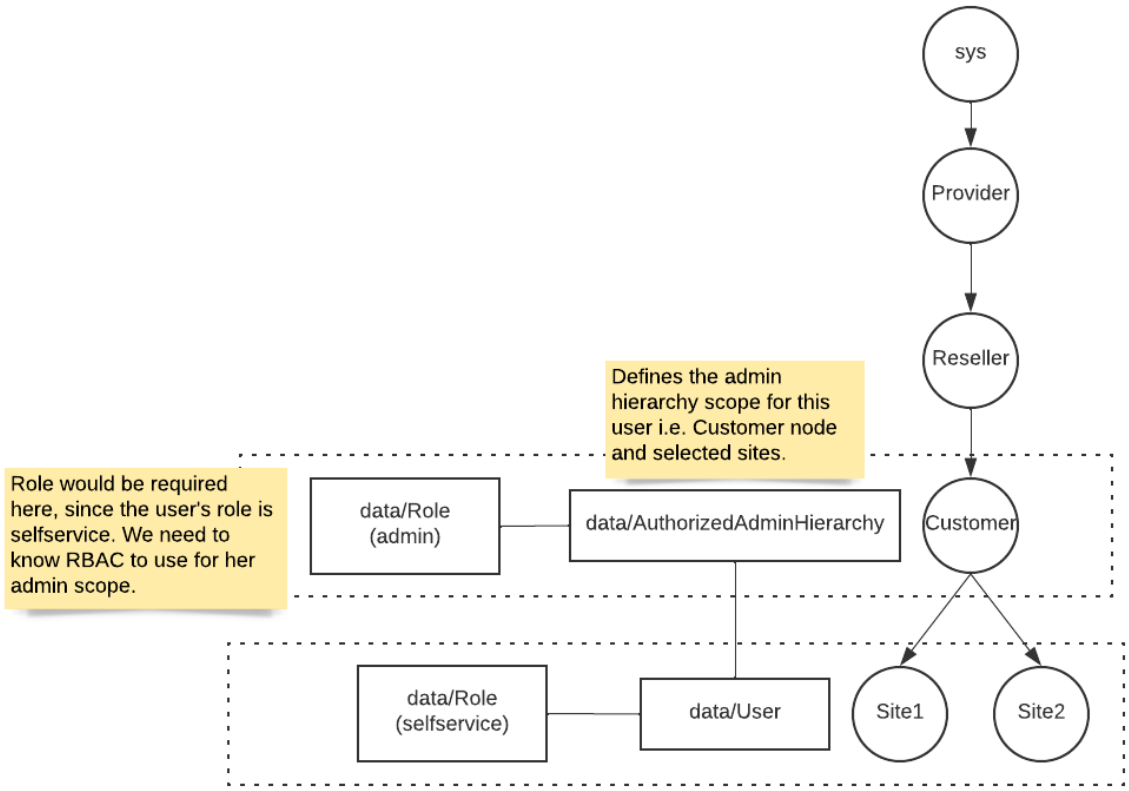
- Provision the end user as usual.
- Associate the end user with an **Authorized Admin Hierarchy Roles** instance.

An authorized admin hierarchy roles instance contains a role. This instance can then be assigned to a user so that if the user is then also assigned a self-service role, the user is then an end user with admin access: a user with multiple user roles - both a self-service role and this role from the **Authorized Admin Hierarchy Roles** instance. See: *Introduction to role-based access control*.

Important:

- When an Authorized Admin Hierarchy is set for a user, the hierarchy of that instance (the model `data/AuthorizedAdminHierarchy` instance) as well as its descendants will be visible as authorized hierarchies for administration purposes.
- An administrator who is also a self-service user, cannot update own user settings control level (e.g. hierarchy access) - only provisioned elements for the user (number, license, etc.) can be updated.

Users with multiple user roles then have a **User Type** of “End User + Admin”. See: *Add admin user*.



Upon user login, the Automate system then assigns the appropriate role to the user in accordance with the requested portal:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Portal	Role
Automate Self-service	selfservice
Automate Admin	administration

Note:

- A user with multiple roles can also access both self-service and admin portals during one login session, but a logout on any portal would end the login session on both portals.
- For multi-role admin user SSO login options, see: *SSO Scenarios for Multi User Roles* under *Configure Self-service SSO SP settings*.
- When multi-role users perform administrative actions, they can manage their own services such as adding new Phones and Lines. However, the administrators would not be able to make modifications that altered their own role-based access configuration, such as change of role and associated Authorized Admin Hierarchy.

Related Topics

- *Add admin user*
- *Introduction to Self-service*
- *Configure Self-service SSO SP settings*
- For API details, see the `REQUEST-PORTAL` API request header in:

  the API Request Headers section in the API Guide.

5.5. Role Configuration

5.5.1. Dashboards

Introduction to Automate dashboards

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Dashboards are customizable pages made up of widgets that provide quick access to frequently used tasks and data visualizations. They can serve as default landing pages or be added to user menus.

Widget types

Dashboards can include:

- **Counters**: Show numerical data
- **Tables**: Display structured data
- **Charts**: Visualize trends and metrics
- **Text**: Add notes or instructions using Markdown or HTML
- **Links**: Provide quick navigation to other pages

Data filtering and sync behavior

- Widget data values and counts are filtered based on the hierarchy level where the dashboard is viewed.
- Dashboard fields showing the item hierarchy (similar to "Located At") update only after a full sync and not during real-time refreshes. For example, if users are added and moved to a site, any dashboards (at system or site level) won't reflect the change until a full sync is run. Refer to *Dashboard sync and refresh*.

Dashboard access

API access

Dashboards can also be accessed via direct URLs:

```
/portal/#/admin/dashboard;name=<dashboard_name>
```

Use URL encoding for spaces, for example, `/portal/#/admin/dashboard;name=Dashboard%20Call%20Groups`. This link format allows support for cross-launching from portals where the name of the dashboard is known.

Admin permissions

Admins with roles that have access profiles for creating and updating dashboards can design and add dashboards to menus. For details, refer to the *Dashboard permissions* section in *Access profiles*.

By default, admins have permissions to modify their own menu layouts and dashboards. If the menu layout or dashboard is at a higher hierarchy, they can clone and then modify the menu layout or dashboard at their hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Access profile permissions and operations* (Dashboard permission groups)

Landing page conversion (v24.1 upgrade)

When upgrading to Automate version v24.1:

- **Landing pages** are automatically converted to dashboards. New `data/Dashboard` records are created from `data/LandingPage` records.
- **Welcome headers** become Markdown-formatted dashboard *Text* widgets, with with the header prefix as `##` and the text prefixed with `###`.
- **Sections** become dashboard *Links* widgets.

  Where a landing page link setting had **Set default Model Type** enabled for a link, this setting is also enabled in the dashboard *Links* widget for each corresponding link. Long lists of links may result in a scrollbar showing on the widget. In this case, the number of links can be divided into multiple widgets by modifying the converted dashboard.
- **Counters** are grouped into dashboard *Counter* widgets

  Each widget will have up to three counters. The counters use Automate models as their source. Converted counters can be modified as required.
- **Charts** from landing pages are not converted but can be manually recreated. Refer to *Introduction to Automate dashboards*.

  Examples are:
  - Cisco Headset Summary
  - Number Inventory Chart
  - Cisco UCCX Agent Stats Chart
  - Usage Growth Chart
  - Webex Teams License Chart

Additional changes

- Saved searches now appear on the user's **Account** page.
- Default and custom landing page names with `LP` suffix are renamed with `Dashboard`.

  For other custom landing pages (landing pages without this suffix) detected on an upgraded system and converted, the original landing page names are retained as dashboards with the same name.
- Conditions from landing page sections are applied to individual dashboard links using logical `AND`.

  This describes instances where a condition is set on the landing page as well as a condition at section level, where the converted *Links* dashboards provide both conditions for each individual link, joined with a logical `AND`.
- A new database and resource model for its data has also been added: Insights reporter resources (`data/ReporterResource`).

  An additional resource model called `data/CustomResourceModel` has been added to allow for the custom creation of calculated fields for a reporter resource, which can then be selected for use when creating a widget based on the resource. For details, see: *Custom Reporter Resource fields*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dashboards created from converted landing pages allow for the same functionality as landing pages, but have an enhanced editing interface where, for example, a wide variety of chart widgets can be added to enrich the dashboards.

Note: It is recommended that dashboard conversions be inspected and edited if needed. For more details on dashboards, their maintenance and initial sync requirements after adding dashboard widgets, refer to *Introduction to Automate dashboards*.

Related element updates

During the conversion of landing pages to dashboards in an upgrade, the following related elements are also migrated:

- **Roles** referencing landing pages are updated to dashboards.
- **Access Profiles** get new dashboard permissions to Insights reporter resources. Refer to the *Dashboard Permissions* section in Access Profiles: *Access profile permissions and operations*.
- **Menu Layouts**: Menu items containing landing pages as `type` are replaced with dashboard and the converted dashboard is matched and added. Any landing page `display_as` entries are converted to dashboard entries.
- **Configuration Templates** are updated to reference dashboards instead of landing pages.
- **Field Display Policies**: The `groups` and `field_overrides` roles containing references to landing pages are updated to reference dashboards instead of landing pages.

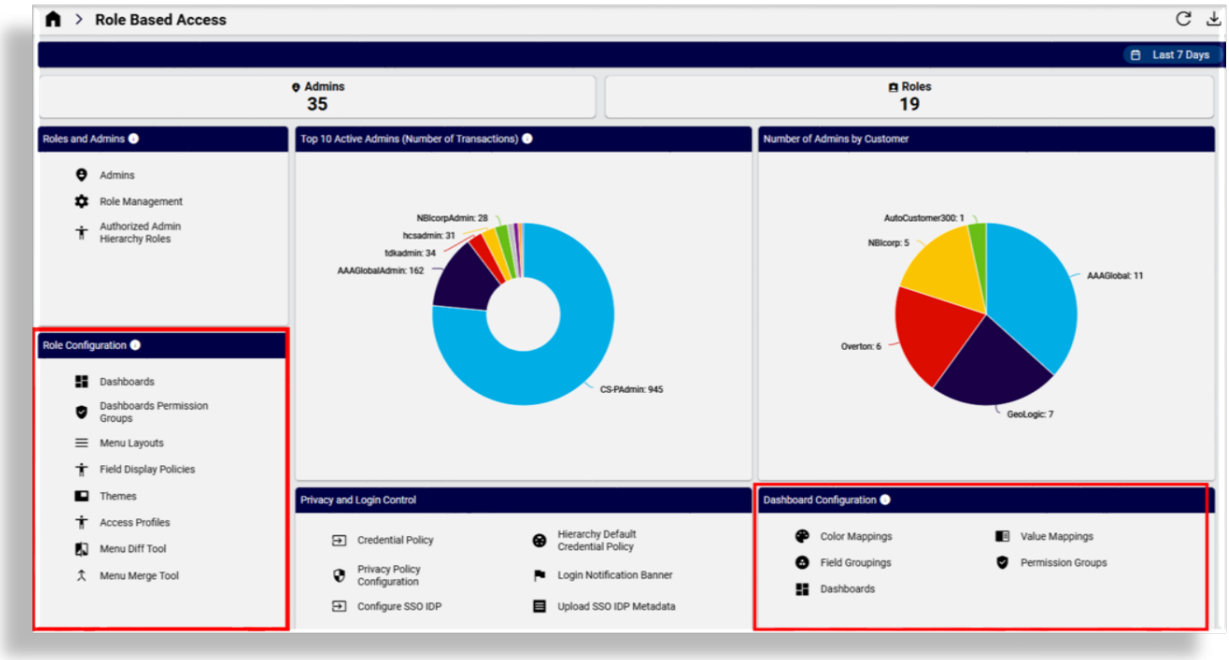
Manage dashboards and widgets

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

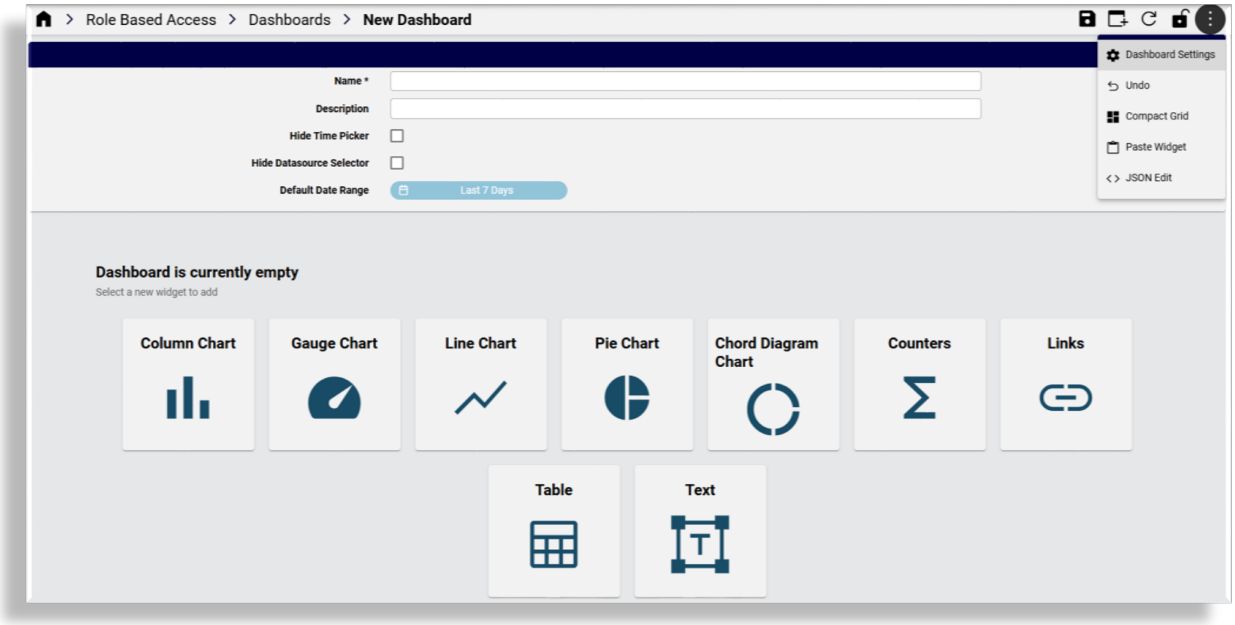
Overview

Administrators can manage dashboards via the **Dashboards** link on the **Role Based Access** dashboard.



Add or edit a dashboard

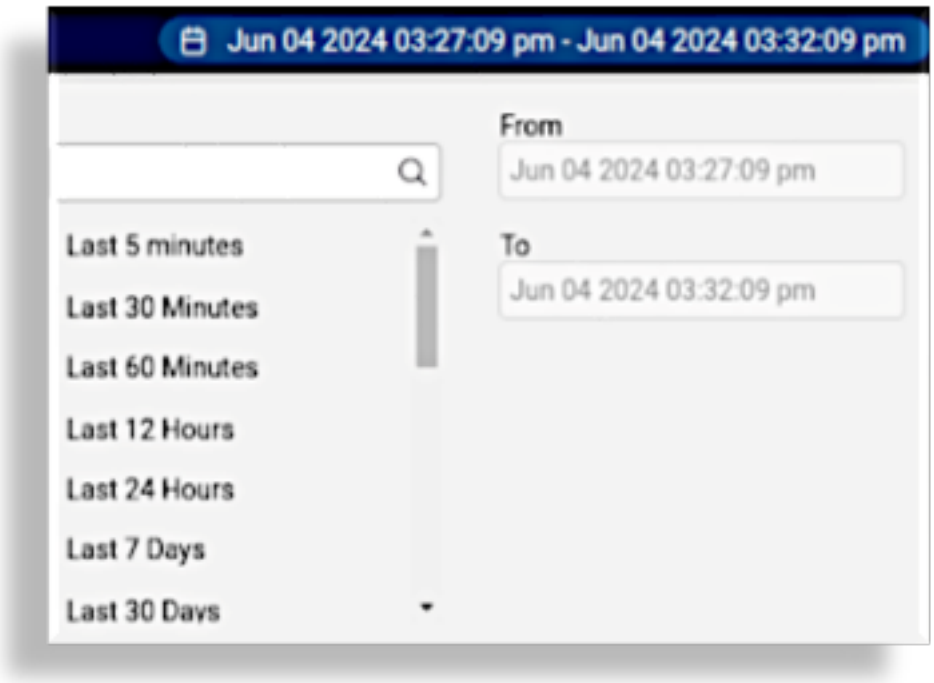
Automate provides several configuration options for working with dashboards.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Add or edit

- **Name**: Display name of the dashboard
- **Description**: Provide a description for the dashboard for the **Dashboards** list view.
- **Hide Time Picker**: By default, a time picker is available to filter dashboard data by start and end date. Any selected dates are reset when you log out. You can't specify a date in the future. Select the checkbox to hide the time picker.

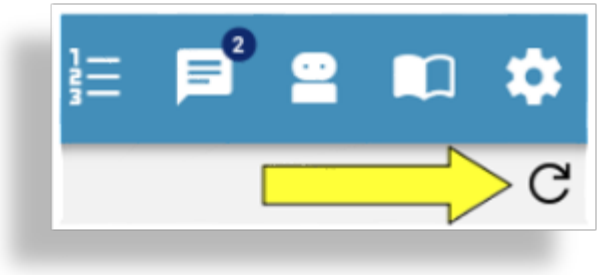


- **Hide Datasource Selector**: This setting applies in the case where multiple instances of a dashboard data type is available. Not enabling the setting on a widget allows for selection of a data source instance and updates widget data based on the selected data source. Enabling the setting implies that the data source set on the widget is always used. Also used with "Insights Netflow" deployment option. For details, contact VOSS.
- **Default Date Range**: Select this option to open the date range picker and to set up a default date range for the dashboard. This range will then apply to widgets on the dashboard that use the date range picker.
- **Clone**: Use the toolbar **Clone** icon to create a copy of the dashboard you're viewing. The cloned dashboard opens with the breadcrumb name appended with the text, `[CLONE]`, and contains all the widgets of the source dashboard. The cloned dashboard name is the same as the original source dashboard name and can be modified as required.

  Note: Dashboards with the same name can be available at different hierarchies. When such a dashboard is referenced, this first one found higher up from the administrator user's login hierarchy is selected.

- **Refresh Dashboard**: Used to update synced data on the dashboard to reflect any system data changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: Dashboard widgets each also provide a similar **Refresh** button when hovering over the top bar of the widget - similarly to refresh individual widget data.

- **Lock**: Used to lock the arrangement of widgets
- **Dashboard Settings**: Toggles (shows/hides) the dashboard name, description, and properties.
- **Undo**: Reverts the dashboard to the state of the last unlock. So, if the lock has been used even once on the dashboard, the unlock will always return the dashboard to the state it was after it was unlocked, even if multiple changes were done since. If the dashboard was never locked, **Undo** will lock it, forcing the user to unlock and create a snapshot point. This snapshot is the same as the uploaded dashboard. Note that the *Undo* functionality is currently under review.
- **Export**: Exports one or more instances. Refer to *Bulk export of model data*. Exported dashboards can then be modified and imported at a required hierarchy via the **Import** menu.
- **Compact Grid**: Automatically optimizes the arrangement of widgets on the dashboard, given their current size.
- **Paste Widget**: Pastes a widget you have selected, using the **Copy Widget** option on the widget menu, into the current dashboard. This allows you to copy widgets between dashboards.
- **JSON Edit**: Used for editing the dashboard data in JSON. For details, refer to *Manage items*.
- **Export Dashboard Data**: Used to export the data available in the widgets of a dashboard: in CSV or MS Excel format. The exported data contain header rows labelled with the friendly names of the data field names and is then available for off-line use.

  Where multiple widgets are available on a dashboard, widget data is exported as either a CSV file or as a sheet in a MS Excel workbook. All the CSV files are archived in a `.zip` file. The export filenames follow the following convention:

  ```
  Export_<dashboard-name>_data_<all|displayed>_<timestamp>.<zip|xlsx>
  ```

  The available export options are determined by the **Data Source** of the widgets on the selected dashboard:

  - If there is a widget with **Data Source** as **Automate** present, only two export options will be available:
    - CSV - Displayed records
    - Excel - Displayed records

    This means that exported data will reflect the displayed records as per current **Time Picker** interval.
  - If all widgets have **Data Source** set to **Automate Analyzed** , **Netflow** or **Assurance**, there will be four export options:

Copyright © 2025 VisionOSS Limited. All rights reserved.

* CSV - Displayed records
* CSV - All records
* Excel - Displayed records
* Excel - All records

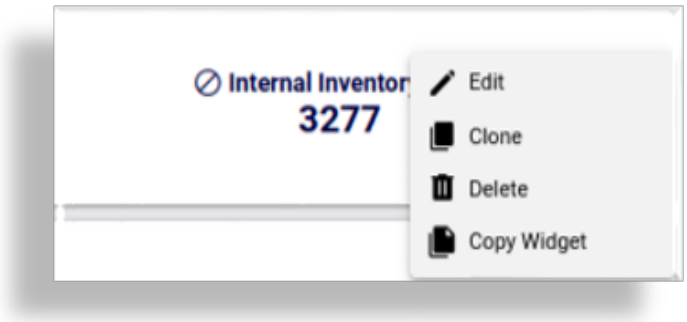
Selecting an “All records” option will include all available data, regardless of the selected **Time Picker** interval.

Add or edit widgets

When a dashboard is added or updated, widgets can be added, removed or edited.

To add a widget, click the **Add Widget** toolbar icon; then, on the design form, either select the widget from the toolbar or from the provided list of icons:

To edit a widget on a dashboard, select the dashboard from the list and choose **Edit** from the widget’s menu. The widget menu provides a number of operations.



- **Edit**:
  - Use the **Edit** icon from the widget menu to edit the current widget. refer to the details below on available edit options.
- **Clone**:
  - Use the **Clone** icon from widget menu to clone the widget on the dashboard. The clone can then be edited as required.
- **Delete**:
  - Use the **Delete** icon from the widget menu to remove the widget from the dashboard.
- **Copy Widget**:
  - Use the **Copy Widget** icon to copy the current widget in order to paste it into a dashboard using the dashboard **Paste Widget** menu item.
- **Export data**:

  Where a widget offers data in a compatible format, the **Export data** on the widget menu allows for a MS-Excel or comma-separated value (CSV) export to a file, as in the Number Status example below:

```
Status,Count
Used-Utility,6
Cooling,35
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
Used,63
Reserved,106
Available,3850
```

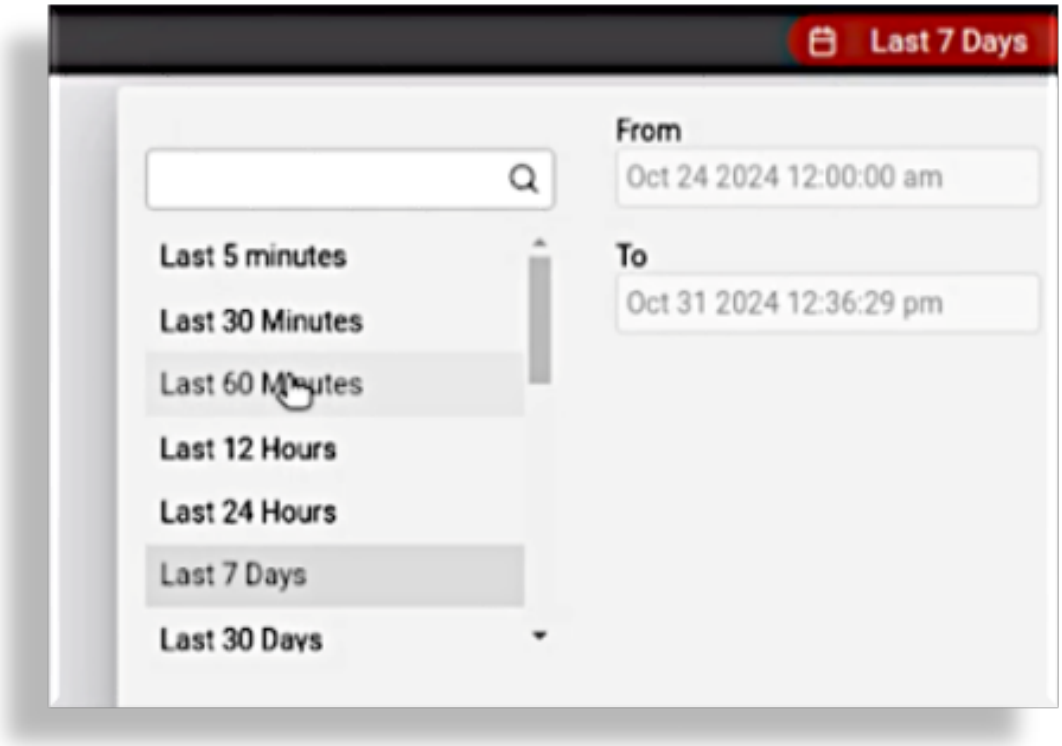
Note:

- For widgets where the Resource is an Insights resource, the option to export All Records is not available.
- For 24.2 installations where the "Insights Netflow" deployment option was selected, widget **Data Source** dropdown fields also show **Netflow**. For details, contact VOSS.

Note:

- When editing a dashboard, the widget order and position on the dashboard will follow the order and position as managed during the editing process.
- Not all widget options and possible combinations are covered in this document. The widget refresh option can be used to inspect the impact of an option. For assistance in creating widgets, you can also contact VOSS support.

Where a widget resource references data over a time period (such as transactions), the widget interface provides a time picker control to indicate and change the interval for the data shown on the widget.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Dashboard sync and refresh

A real-time sync process is running to maintain Automate and Insights databases in sync. After upgrade to release 24.2, dashboard management is available after 30 minutes, since the scheduled `delta-sync` process initially carries out a *full sync* and thereafter an incremental resource sync.

See: *Insights Analytics* in the Platform Guide.

Important: Dashboard fields showing the item hierarchy (similar to *Located At*) are updated only when a delta sync runs. For example, if you've added users to the system and then moved them to a site, any charts, counters, or tables showing a count of users (at that site or at the system level), will only reflect the correct number of users once a delta sync runs and not when simply refreshing the dashboard or widget in a real-time sync. Until the delta sync runs, the hierarchy fields for these users display on dashboard charts, tables, or widget counters as with no (empty) hierarchy value. See *Dashboard sync and refresh*.

Dashboard export and scheduling

Automate allows for dashboards - including dashboard data - to be exported to:

- an email address
- a target SFTP destination

1. Go to **DashboardExport**
2. Add an export instance on the input form:
    - **Name** of the dashboard export
    - **Description** of the dashboard export (optional)
    - Select one or more dashboards from **Dashboards** list
    - Indicate the **Export format**: MS Excel file or CSV file format
    - Add SFTP and/or SMTP (email) destinations:
        - Ensure a SFTP server is set up and fill in corresponding details.
        - Add a SMTP Server in the Licensing and Subscriber Data Export Guide
        - *Email*
3. Choose to execute the export or add a schedule for the export.

Note:

- At least one destination is required, either SMTP/SFTP.
- Dashboard export instances can only be modified by the user who created it or by the upper level user.
- Dashboard export will be executed in the RBAC context of the user who created it (in accordance with the hierarchy at which the export instance is created).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Schedule dashboard export report*
- *Dashboard Exports*

Value mapping

The **Value Mappings** page defines a list of value mappings used when retrieving data for dashboard widgets. This allows a dashboard designer to substitute a stored value with a friendlier value that will be displayed to the user.

Note: Updating existing grouping configs has a refresh delay of 30 mins.

Value mappings allow for custom, alternative field values of resources to be displayed in chart widgets by using the **Value Mapping** field. This optional value is applied during the design of a widget and is typically used to present a more user-friendly field value in a chart widget, for example, to map the value of `Cisco Codec Mappings` originally: `0` to mapped: `No Media Established`.

The **Value Mappings** page (data model: `data/DashboardValueMapping`) is available to provider administrators and higher to add, delete and manage mappings. The model contains the default individual mapping value: `NO MAPPING`.

The design of a mapping allows for the selection of an evaluation operator to apply to the original value as an input condition and then to provide the replaced value in accordance with the evaluation operator test result.

Evaluation operators that can be applied to the original field values are:

- Regex
- Greater than
- Less than
- Range (with “Max” and “Min” parameters)
- Equals

Note:

- More than one original field value can be mapped to a single mapping key.

Examples:

- If name: `Cisco Codec Mappings` Equals `0`, then the mapping key is `No Media Established`.
- Microsoft 365 service plan mappings by matching Microsoft Entra ID values:
  - If string ID Regex `(^SPB$)` matches, then mapping key is `Microsoft 365 Business Premium`.
  - If string ID Regex `(^O365_BUSINESS_PREMIUM$)` matches, then mapping key is `Microsoft 365 Business Standard`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Color mapping

The **Color Mappings** page defines a list of color mappings used to style data in dashboard widgets.

Automate provides options to allow for custom, alternative display colors and icons of **Automate Analyze** resources to be displayed in table widgets by modifying the **Field Type** of the resource and by creating instances of a dashboard color mapping. The mapping instance name is then selected in the **Text Color Mapping** and/or **Cell Color Mapping** dropdown lists under **Table Options > Renderers** when designing a table widget.

The **Field Type** of the field needs to be set to one of:

- Text
- Traffic Light: an icon

Refer to the **Format Type** of the field in the *Table* topic above.

This optional mapped value is applied during the design of a widget and is typically used to present a more user-friendly color or icon in a table widget, for example, to map a range of field values to have a specified color.

The design of a mapping allows for the selection of an evaluation operator to apply to the original value as an input condition and then to render the replaced color in accordance with the evaluation operator test result.

Evaluation operators that can be applied to the field values are:

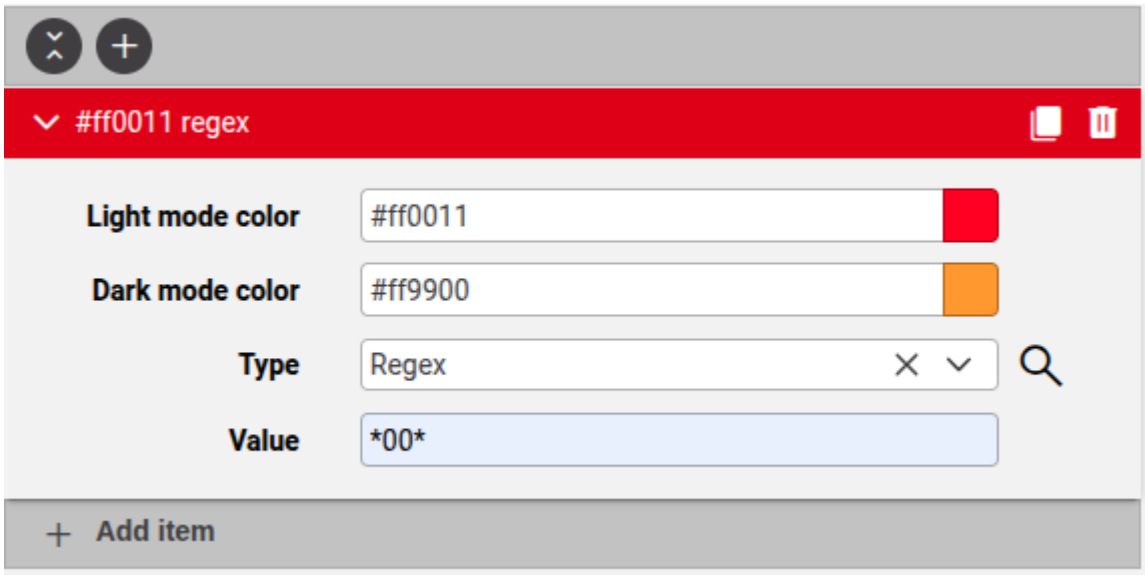
- Regex : for fields with text or numeric values
- Greater than : for fields with numeric values
- Less than for fields with numeric values
- Range (with “Max” and “Min” parameters): for fields with numeric values

The **Color Mappings** page (data model: `data/DashboardColorMapping`) or **Color Mappings** link on the **MVS-RoleManagement-Dashboard** dashboard is available to provider administrators and higher to add, delete and manage mappings.

Examples:

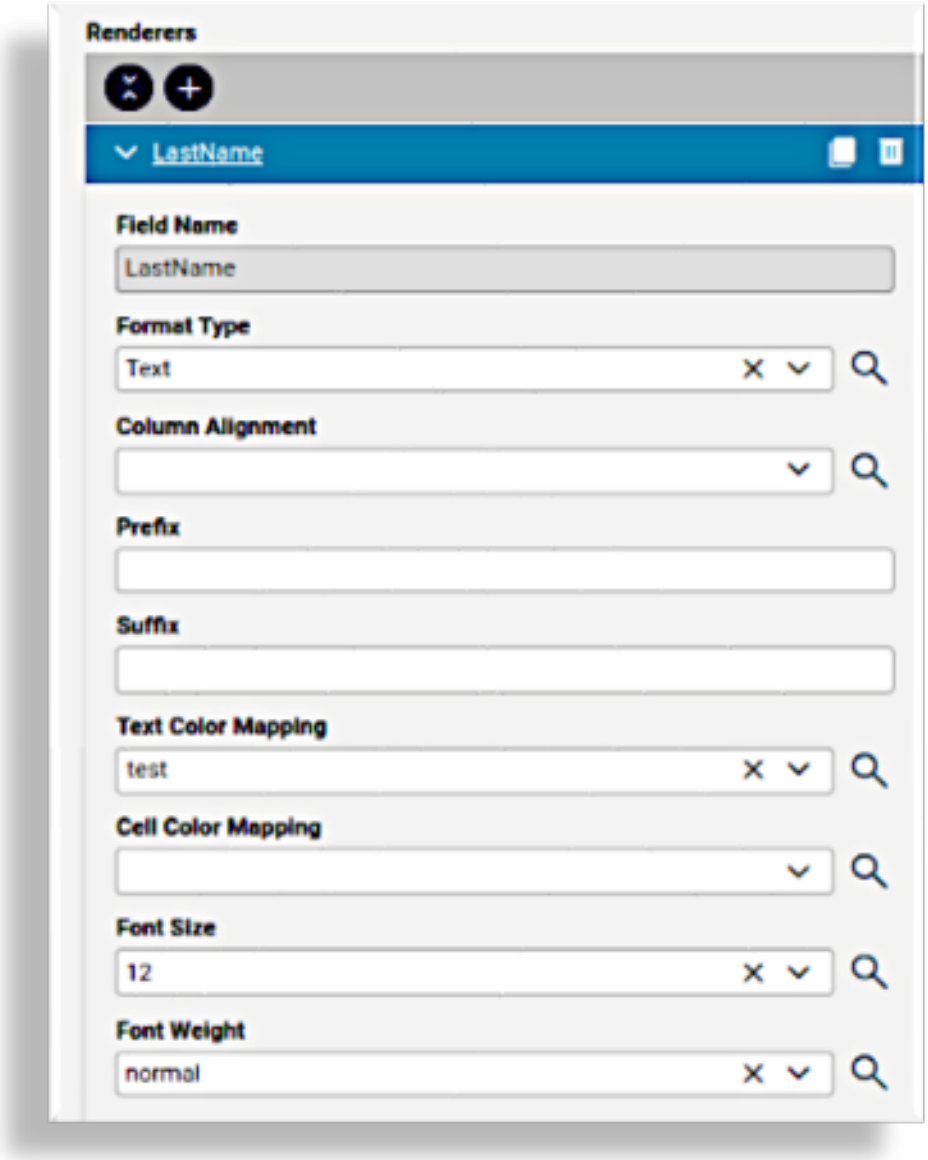
1. If a Dashboard Color Mapping instance exists that matches the Regex `.*00.*`, then render the text as color: `#ff0011`.

Copyright © 2025 VisionOSS Limited. All rights reserved.



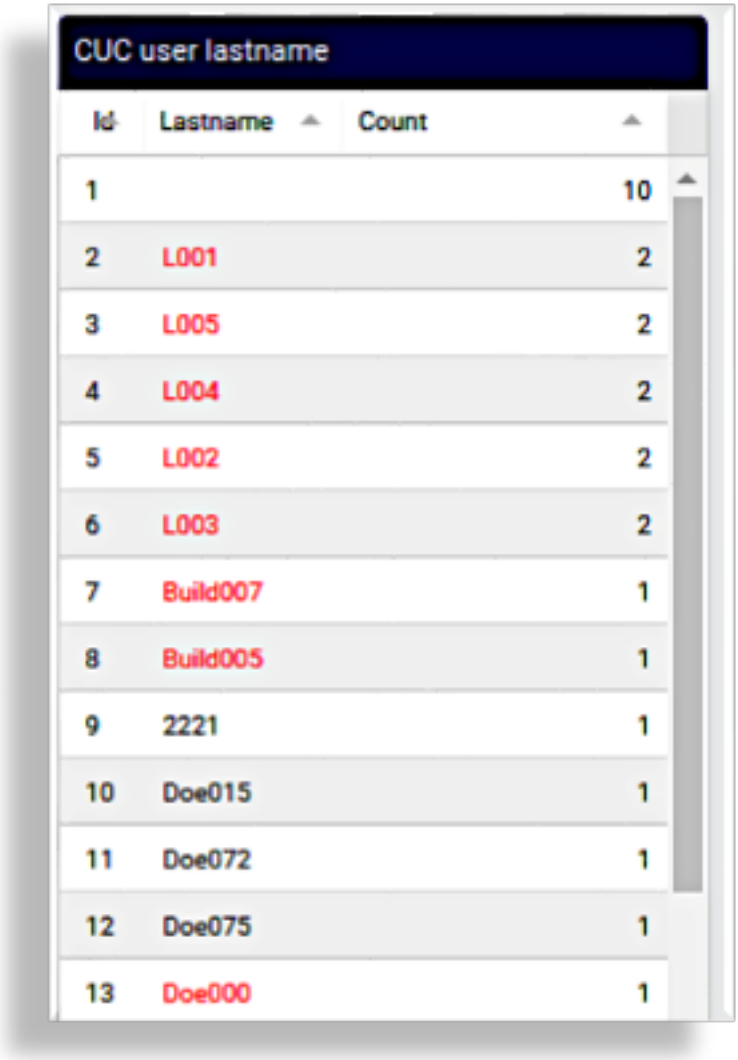
The **Render** section of a table widget has a field with **Field Type** set to “Text” and the **Text Color Mapping** dropdown selection is the created Dashboard Color Mapping.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table then displays the text the matching text accordingly, acording the selected **Dashboard Color Mode** (Light/Dark) of the theme that is applied - see: *Manage themes*. The example below shows the `Light` theme applied.

Copyright © 2025 VisionOSS Limited. All rights reserved.

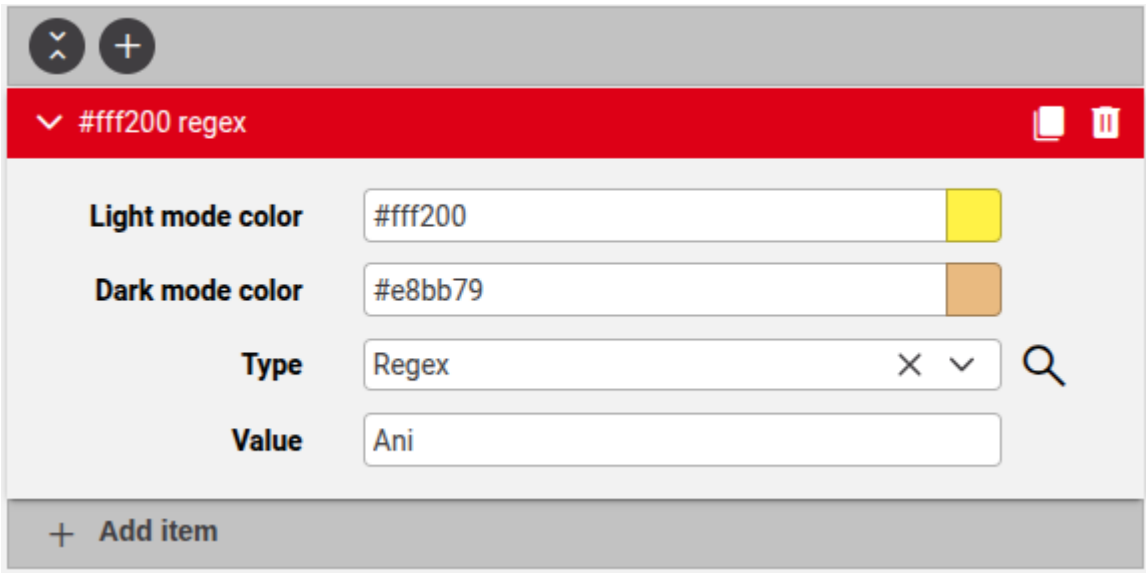


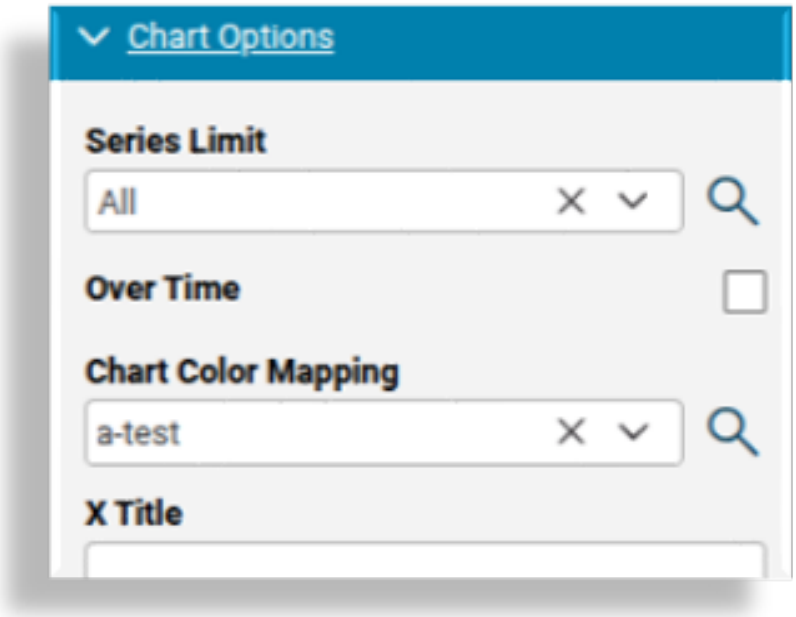
CUC user lastname

Id	Lastname	Count
1		10
2	L001	2
3	L005	2
4	L004	2
5	L002	2
6	L003	2
7	Build007	1
8	Build005	1
9	2221	1
10	Doe015	1
11	Doe072	1
12	Doe075	1
13	Doe000	1

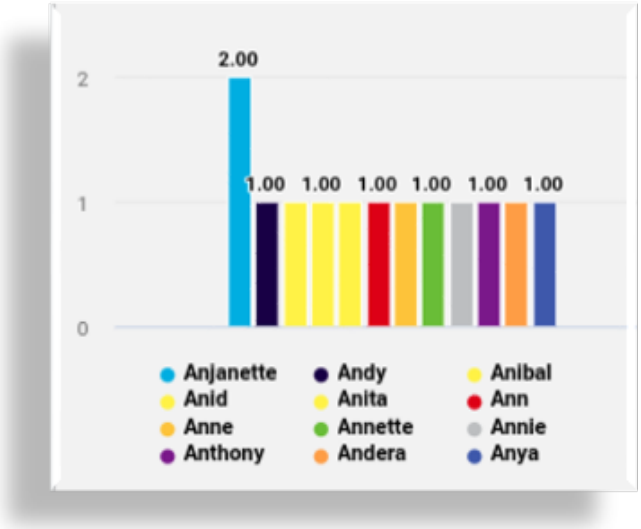
2. If a **Dashboard Color Mapping** instance exists that maps the Regex value `Ani`, with the color: `#fff200` and this instance is applied (selected under **Chart Options**) to a chart showing user first names that start with `An`, then names starting with `Ani` will be rendered in the chart mapping color (example below for `Light` theme):

Copyright © 2025 VisionOSS Limited. All rights reserved.





Copyright © 2025 VisionOSS Limited. All rights reserved.



Field Groupings

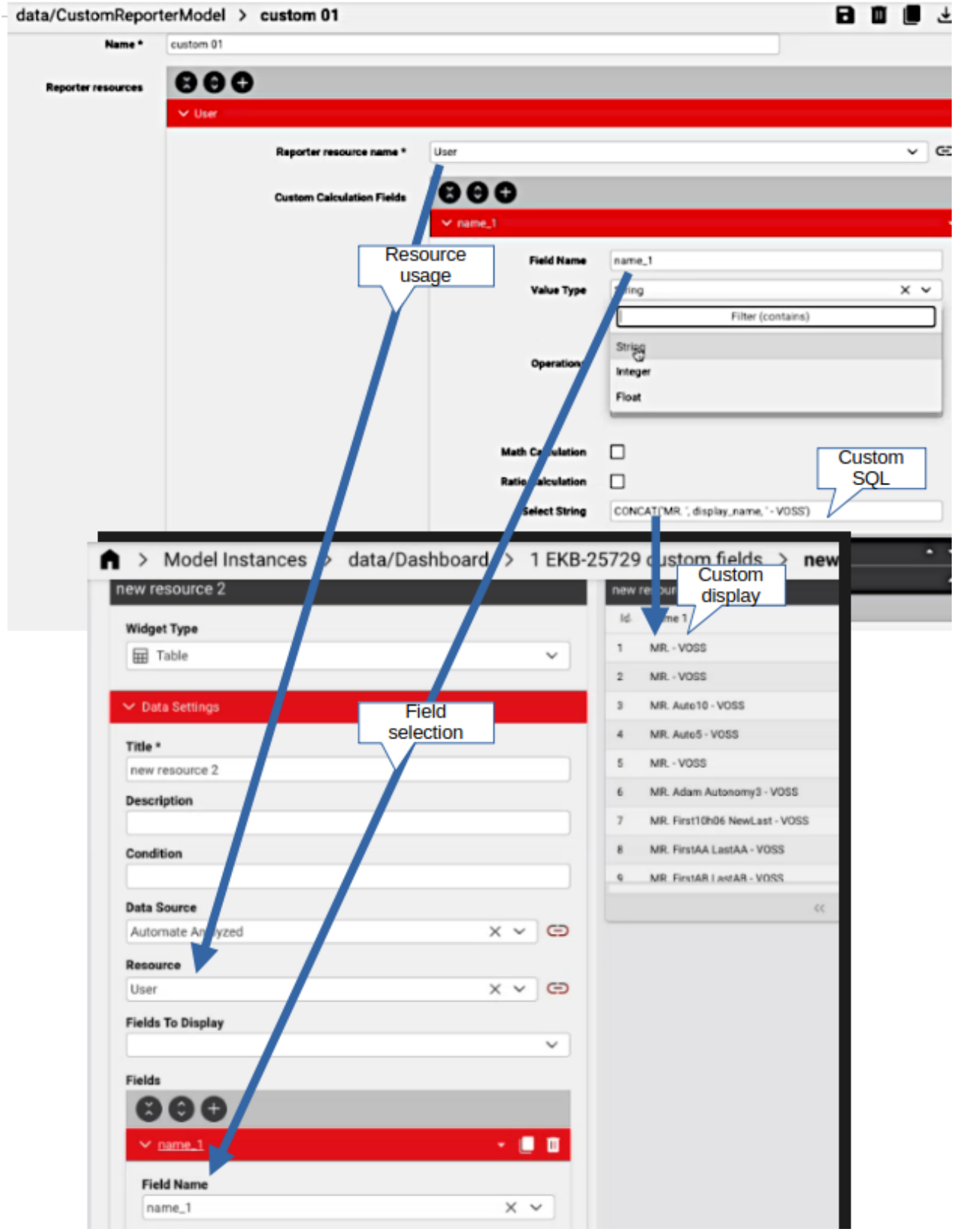
The **Field Groupings** page defines groups of similar data to facilitate common analysis and drill-down functions on a single dashboard.

Custom Reporter Resource fields

Automate provides an options to allow for the custom creation of calculated fields for a reporter resource. The customizations are added to a resource model called `data/CustomResourceModel`, where they can be grouped by a name and the calculated fields can be mapped to a selected resource in the reporter resources.

The screenshot below illustrates the creation of a custom field for to be used as the `name_1` field as well as its selection in the design of a table widget.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- This feature is only accessible to administrators who have access to the `data/CustomResourceModel` model.
- Since the custom creation of calculated fields for a reporter resource requires knowledge of how the data is stored in the database in order to write the SQL for the field, contact VOSS if access to and usage of this feature is required.
- Since data added to the `data/CustomResourceModel` model requires an additional migration or upgrade step, contact VOSS if access to and usage of this feature is required.

Chart widgets

Tip: *Use the Action search to navigate Automate*

Overview

The dashboard widgets support the following chart types:

- Column Chart
- Gauge Chart
- Line Chart
- Pie Chart
- Chord Diagram Chart

When a chart widget is selected, it is also possible to switch to another widget format during the edit and design process.

The chart type can be updated from the **Widget Type** drop down. Changes are reflected in real-time during the design of a widget or by using the widget's **Refresh** icon.

Copyright © 2025 VisionOSS Limited. All rights reserved.

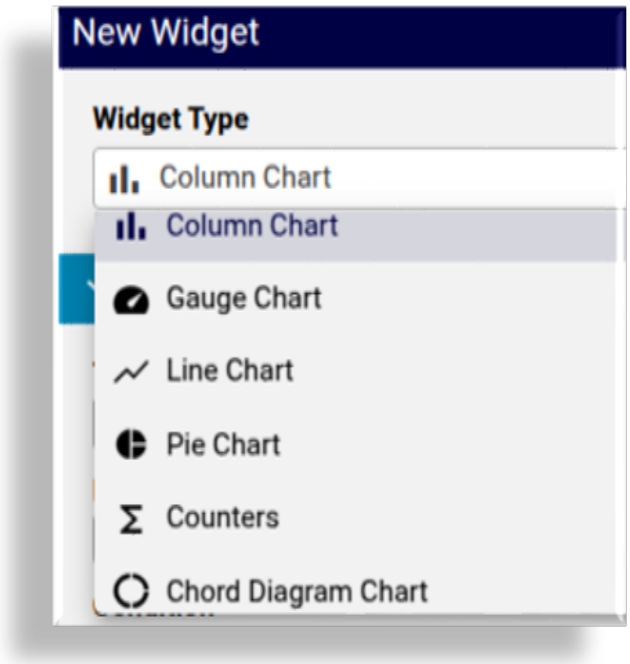


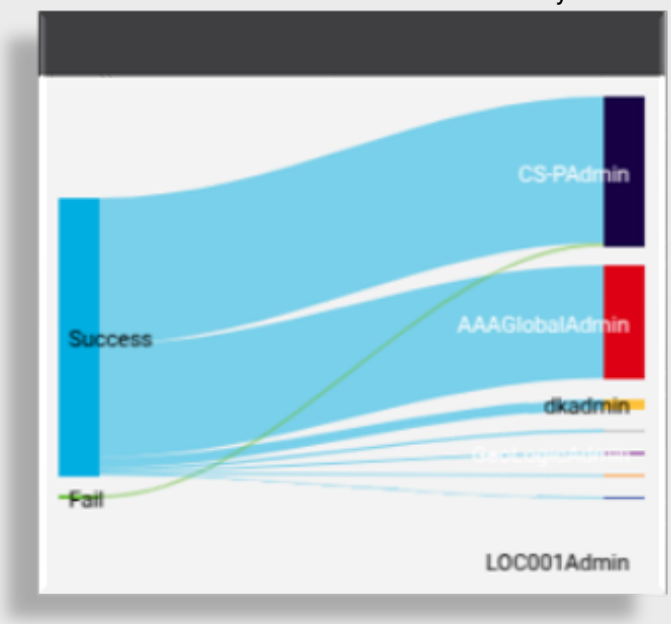
Chart widget data settings

The table describes the common list of data settings for chart widgets:

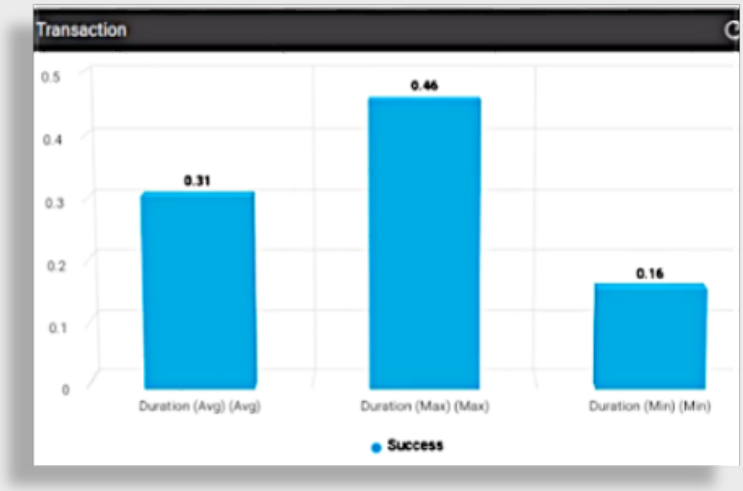
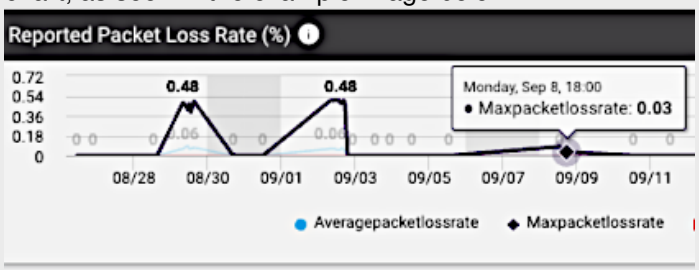
Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Title	The text to display above the chart.
Description	This text displays as an informational pop-up when hovering over the circled **i** icon adjacent to the title.
Condition	The display of the widget on the dashboard can be controlled by entering a condition that resolves to boolean True or False, for example in accordance with enabled features, services, and devices, as in the **Global Settings**. The conditions are in the form of system macros. See for example the macros listed under the *Links* topic below.
Data Source	Charts can access the **Automate Analyzed** and **Assurance** sources. The **Assurance** data source is also available if an Arbitrator is configured. See *Arbitrators*.
Data Source Instance	Displays if **Assurance** is selected as the data source as multiple instances can be configured. A selection of these can then also be made if **Allow Data Source Selection** is enabled.
Resource	Depends on the selected data source, a drop-down list of resource items available to be referenced in the chart. For example, for **Automate Analyzed**: `Number Inventory`, `Cisco CUC User`, `Cisco UCM Phone`, `Microsoft O365 User`. **Note:** • Where the data source is **Automate Analyzed**, Automate provides an additional list of **Resource** instances that can be used to represent trends on a widget. For details, see *Automate dashboard trends resources* • Based on the selected hierarchy when working with a dashboard, the real-time display of data updates according to the current hierarchy, so that a widget that for example shows a count of users, displays values relevant to the selected hierarchy. **Important:** For charts, **Resource** data is accessed from an Automate Analyze database: reporter resources (`data/ReporterResource`). When creating charts for the first time, *prior to the first scheduled full sync*, it will be necessary that a manual sync of the Automate Analyze database is carried out with the Automate database. This requires the execution of a Platform Command Line Interface command. Refer to the *Dashboard Refresh* section below.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Fields	Depending on the selected **Resource**, one or more fields from the resource can be selected as items for the chart. • **Field Name**: A drop-down of fields belonging to the **Resource**. For example, for **Chord Diagram Chart** (**Sankey** type in the example image below), the **Transactions** resource **status** and **username** field names can be selected to show the transaction success/fail breakdown by user:  • **Friendly Name**: A text field to provide the **Field Name** with a custom name. • **Field Type**: A read-only field indicating the data type of the selected **Field Name**. For example, if the **Data Source** is **Arbitrator**, a **Resource** instance may show the **Field Type** as `Calculated - Text`. • **Operation**: Select the operation to be carried out on the **Field Name**. Refer to the example below showing: `Grouping Count`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Fields (continued)	**Note:** A different operation can be applied to the same field. In the example below, average, minimum, and maximum is applied to the transaction duration field:  • **Value Mapping**: Default is `NO MAPPING`, otherwise a selected value mapping to display the value on the chart widget. See *Value mapping* • Minimum and maximum values: where values on a chart range across a minimum and maximum, this range will be used on the y-axis in order to improve the display of the chart, as seen in the example image below: 

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Filters	Data referenced in widgets can also be filtered by selecting: • **Field Name** of the **Resource** • **Operation** to be used to filter the values of the field selected by **Field Name**. The availability and function of the operators depends of the data type of the selected field name: text or integer. Select the required operation. For details on the filter options, see *Filter options availability and definitions*
Filter Value	Value to be used by the selected **Operation** to carry out the filter. Such filters provide options to make use of a selection of the resource data in the widget.
Sorts	One or more **Field Name** entries can be added and used to carry out sorting by **Sort Type**: Ascending or Descending
Chart Options	Available Chart Options can vary according to the selected chart widget type. For a detailed reference of chart options, see: *Chart options availability and definitions*
Drill-down options	See *Drill-down options and conditional syntax*
Dashboard chart background colors	Managed by the theme **Panel Color**. See *Theme element color references for the Admin portal*

Chart widget example

As an example, consider the following column chart values, with charts illustrating various data and chart settings:

- Title: `CUCM User Departments`
- Resource: `Cisco UCM User`
- Field Name: `Department`
- Operation: `Grouping Count`

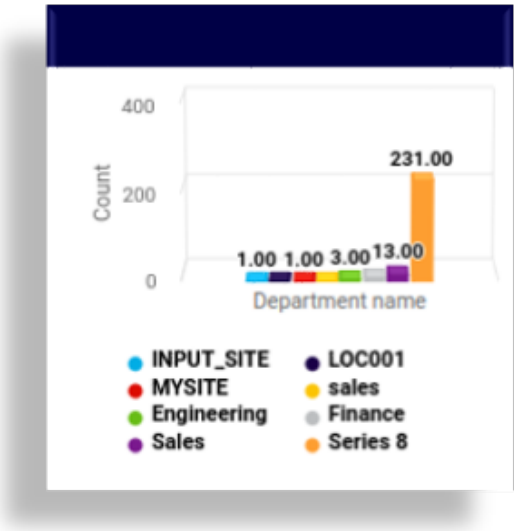
  Shows a column chart with counts of grouped `Cisco UCM User` departments in columns.
- Filter:
  - Field name: `department`
  - Operation: `Exclude Regex (Case sensitive)`
  - Filter Value: `SITE`
- Filter:
  - Field name: `department`
  - Operation: `Exclude Regex (Case sensitive)`
  - Filter Value: `LOC`
- Filter:
  - Field name: `department`
  - Operation: `!=`

Copyright © 2025 VisionOSS Limited. All rights reserved.

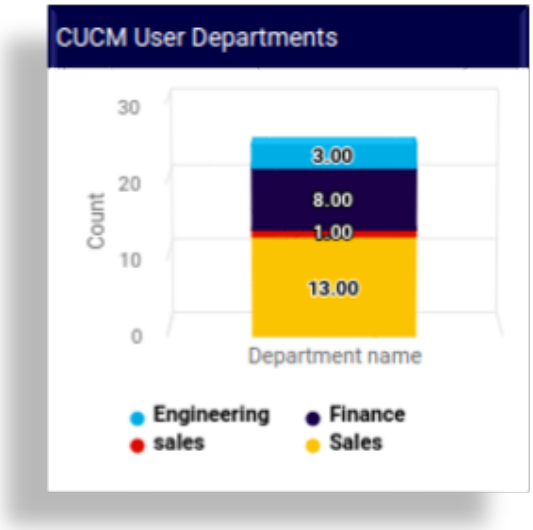
  - Filter Value:
- Sorts:
  - Field Name: `department`
  - Sort Type: `Ascending`
- Chart Options:
  - Series Limit: All
  - Stack Type: `Normal`

The examples below show the chart with settings on some of the properties as *not set* or *set*, in the example above:

- Unfiltered, unsorted (related settings above are *not set*):



- Filtered, sorted, stacked (related settings above are *set*):



Copyright © 2025 VisionOSS Limited. All rights reserved.

Counter widgets

Tip: *Use the Action search to navigate Automate*

Counters are typically used to provide a quick count of a resource, and have the option to display a list view of the values when selecting the counter.

Note: Counter values reflect the hierarchy at which the counter is viewed.

- **Condition**: The display of the widget on the dashboard can be controlled by entering a condition that resolves to boolean True or False, for example in accordance with enabled features, services, and devices as in the **Global Settings**. The conditions are in the form of system macros. See for example the macros listed under the *Links* topic below.
- **Data Source**: Insights or Automate
- **Resource**: only available for Insights
- **Fields**: For Insights resources, one or more instances of **Field Name** can be selected in counters. These field names will then be shown as individual counters in a set of counters. An **Operation** can be selected for these in order to modify the counter.

  For example, if a **Field Type** is "Text" and has duplicate values, and the **Operation** on the field is:

  - **Grouping Count**, then counters will be shown grouping the duplicate fields into separate totals.

  Alternatively, where **Resource** provides values for **Field** that have a **Field Type** of "Integer", additional **Operation** options are available that apply to integers, for example:

  - **Avg**: a ratio of the current field over a total, for example, users with MS Teams Voice over total users
  - **Sum**: for example, the sum total users with MS Teams Voice

  The **User Overview** dashboard counters can for example be inspected to see the application of operations on integer fields.

  Counters can also for example show a count that is grouped by additional fields. Consider a counter with:

  - **Data Source**: Insights
  - **Resource**: Multi vendor user count view
  - **Field Name**, **Field Type**, **Operation**: count_data_users, Integer, Count
  - **Field Name**, **Field Type**, **Operation**: Provider, Text, Group By
  - **Field Name**, **Field Type**, **Operation**: Customer, Text, Group By

  The counter displays the number of users as grouped by each Provider-Customer

Copyright © 2025 VisionOSS Limited. All rights reserved.

When a counter widget is selected, it is also possible to switch to another widget format during the edit and design process. The **Widget Type** can be updated from the dropdown. Changes are reflected in real-time during the design of a widget or by using the widget's **Refresh** icon.

- One or more **Filters** can be applied to a selected **Field Name**, using an **Operation** and **Filter Value**.

  Examples for **Resource** = "Cisco UCM User":

  1. Settings:
     - **Fields** - **Field Name**: "firstName", **Operation**: "Grouping Count"
     - **Filters** - **Field Name**: "firstName", **Operation**: "Regex (Case sensitive)", **Filter Value**: `^An`.

     The resulting counter shows grouped counts of the first names of Cisco UCM users where the first name starts with "An" (case-sensitive).

     If for **Fields** above, the **Operation** was "Count", then a *single value* of the total of all users with first name starting with "An" (case-sensitive) would display in the counter.

  2. Settings:
     - **Fields** - **Field Name**: "userid", **Operation**: "Count"

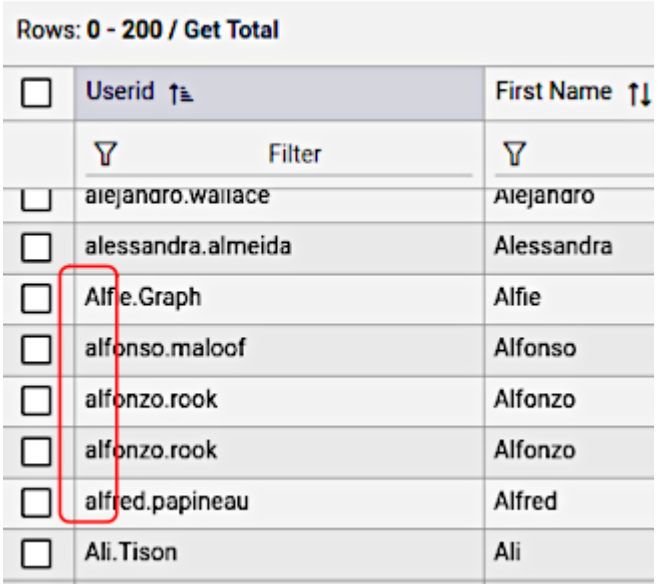
     Then:
     - **Filters** - **Field Name**: "userid", **Operation**: "LIKE (Case sensitive)", **Filter Value**: `alf%`.

       The resulting counter shows a count (4 - see image below) of the userid's that start with "alf" (case-sensitive).

     Or:
     - **Filters** - **Field Name**: "userid", **Operation**: "ILIKE (Case insensitive)", **Filter Value**: `alf%`.

       The resulting counter shows a count (5 - see image below) of the userid's that start with "alf" (case-insensitive), which is larger, given data as in the example image of userids below.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: The **Filter Value** can contain `%` characters, indicating variable string values at the position of the `%` character. For example: `%alf%` will match `norman.alfred`; `alf%` will match `alfred.norman` and `%alf` will match `norman.fredalf`.

- **Type**: only available for Automate resources. This is the selected model type (e.g. `data/Countries`). A **Title**, **Icon**, **Field Display Policy**, **Condition** and **Configuration Template** can also be applied to the selected model type.
- **Filters**: For Insights resources, field names can be selected and a matching operator selected to apply to the name in order to filter a counter value (as in the example under **Fields** above). For Automate resources, see the topic *Fixed and Configurable Filters in Counters and Links* - that will then be applied when the counter is selected to open the filtered list view.
- **Counter Settings**: a limit on the value can be specified, prefix and suffix text can be inserted for the value, as well as default values for empty groups.

Links widgets

Overview

Links on widgets provide shortcuts to data or external URLs. They can be customized with icons, display text, and conditional logic to control visibility.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Link widget configuration

- **Type**: Choose a data model from Automate to link to.
- **Link text and icon**: Customize the display label and icon.
- **Condition**: Use a system macro to set a condition that controls whether the link displays. The condition evaluates to either *True* or *False* based on enabled features. If the condition evaluates to false, the widget is hidden and the dashboard layout adjusts automatically.

  Example macro syntax:

```
{{ macro.is_avaya_enabled }}
{{ macro.is_cisco_ccx_enabled }}
{{ macro.is_cisco_cucm_enabled }}
{{ macro.is_cisco_cucx_enabled }}
{{ macro.is_cisco_microsoft_enabled }}
{{ macro.is_cisco_webex_enabled }}
{{ macro.is_cisco_webex_teams_enabled }}
{{ macro.is_cisco_zoom_enabled }}
{{ macro.is_microsoft_enabled }}
{{ macro.is_pexip_enabled }}
{{ macro.is_session_border_control_enabled }}
{{ macro.is_voss_phones_enabled }}
{{ macro.is_zoom_enabled }}
```

- **Display As**:
  - **External Link**: Requires a URL in the **Href** field.
  - **Form and List**: Display format of data when *type* is selected.
  - **Dashboard**: Links to another dashboard. Select the target dashboard from the drop-down.

    Note: When linking to a dashboard, *Href* and *Type* are hidden. Note that a dashboard link cannot launch another dashboard.

  - **Field Display Policy** and **Configuration Template**: Can be applied based on the selected *type*.

Note: For long lists of links, use multiple Link widgets to avoid scroll bars.

- See also the topic *Fixed and Configurable Filters in Counters and Links*.

Related topics

- *Text widgets*
- Global Settings in the Core Feature Guide
- *Filters in counters and links*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Filters in counters and links

Links widgets contain fixed and configurable filters.

- *Fixed filters*
- *Configurable filters*

Fixed filters

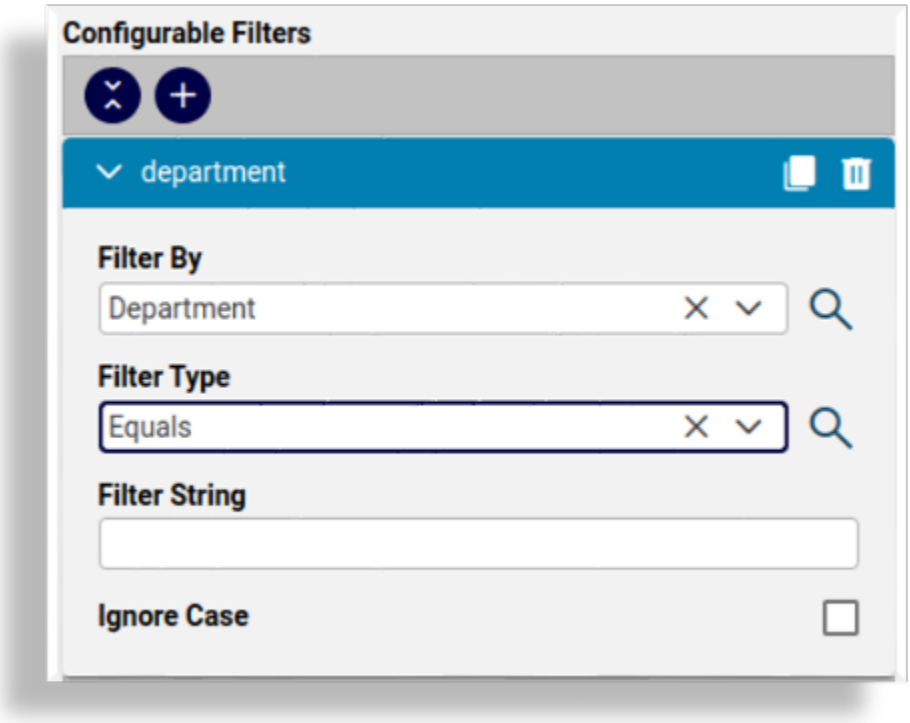
- Set by high-level admins.
- Always apply when the widget is used.
- Results can be further refined by configurable filters.

Configurable filters

Add one or more configurable filters when setting up a widget:

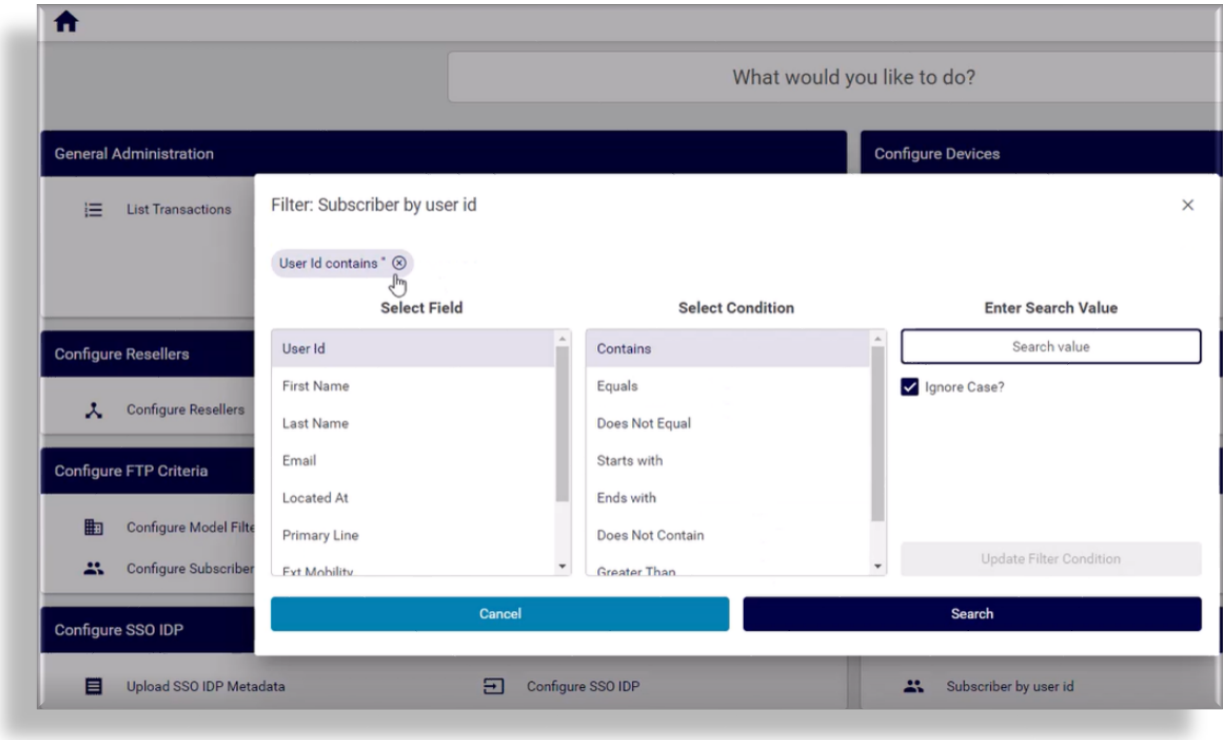
Note: Adding multiple filters using the **Add** option results in a logical AND of the filter application.

- **Filter By**: Select attributes from the chosen *Type*.
- **Filter Type**: Choose the matching operator to apply when the attribute is matched to the *Filter String* value (Contains, Does Not Contain, Starts With, Ends With, Equals, Not Equal).
- **Filter String**: Enter the value to match.
- **Ignore Case**: Toggle case sensitivity of the *Filter String* value.

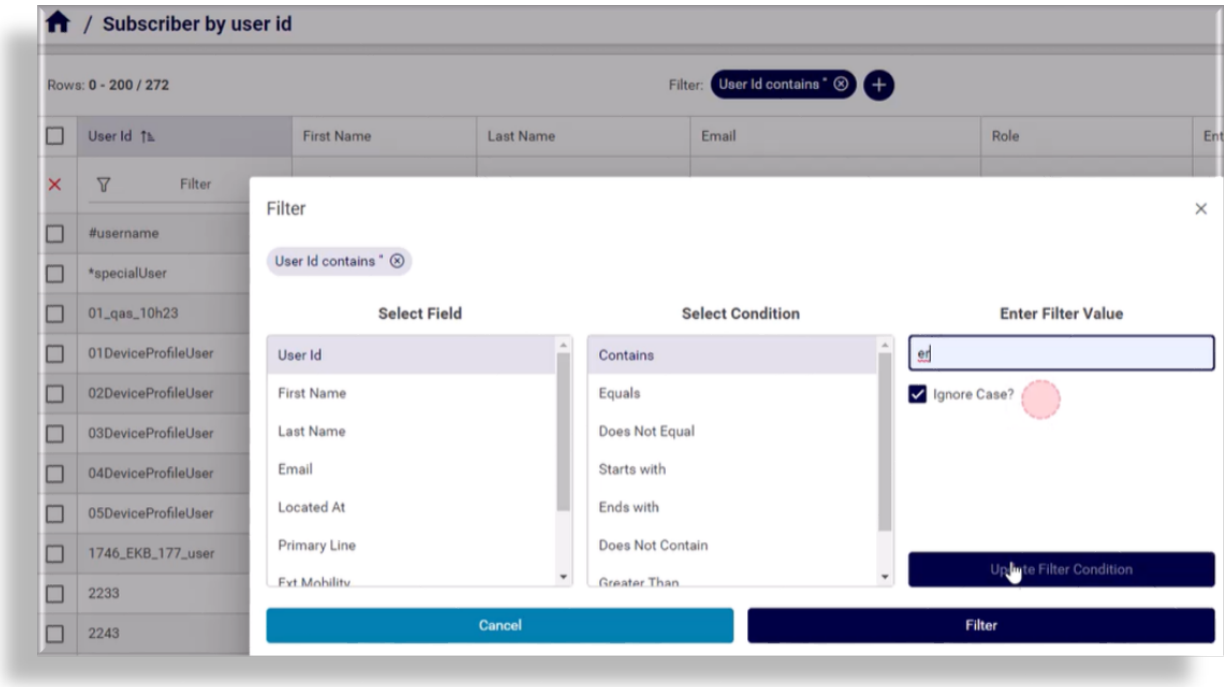


Copyright © 2025 VisionOSS Limited. All rights reserved.

Once you apply the configurable filters, selecting the counter or link in the GUI launches a dialog where you can adjust the filters, including the filter string value (if applicable) before viewing the data.



Note: The list view footer will indicate active filters, which can be modified or removed. See *Working with lists*



Copyright © 2025 VisionOSS Limited. All rights reserved.

Table widgets

Overview

- **Condition**: The display of the widget on the dashboard can be controlled by entering a condition that resolves to boolean True or False, for example in accordance with enabled features, services, and devices as in the **Global Settings**. The conditions are in the form of system macros. See for example the macros listed under the *Links* topic.
- **Data Source**: **Automate**, **Automate Analyzed** and **Assurance** sources can be accessed.

Available menus and fields upon **Data Source** selection:

- **Automate Analyzed**
  - **Resource** options available in accordance with the Insights database

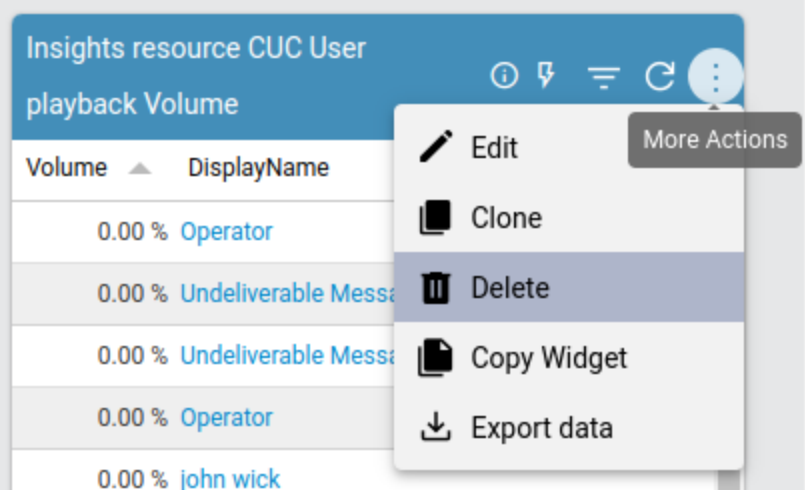
    Automate provides an additional list of **Resource** instances that can be used to represent trends on a widget. For details, see *Automate dashboard trends resources*.
  - From the **Fields to Display** dropdown, select either **All Fields**, **Summary Attributes** or **Clear All**.
  - **Filters**: filter field values from the table
  - **Sorts**: order the table (ascending, descending) by a selected field value
- **Automate**
  - Model **Type**, **Field Display Policy** and **Configuration Template** can be selected.
  - A **Fields** multiselect list allows for the selection of columns to show.
- **Assurance**: if selected, options are available to choose a **Data Source Instance**, since multiple instances can be configured. A selection of these can then also be made if **Allow Data Source Selection** is enabled. For Arbitrator configuration, see *Arbitrators*.
- **Table Options** are available for both data sources.
  - Options to limit, show, hide or format table data and elements
  - Additional field display customization using **Renderers** for fields, including a **Hide Column** option (if the column is for example only used for filtering purposes).

    For fields that represent a date, such as a timestamp, the **Format Type** can also be adjusted to be a **DATE STRING**, allowing for a user friendly format.
- **Drilldown options**: see *Drill-down options and conditional syntax*

Besides standard menu options, a displayed table can also show additional menu options in accordance with enabled features such as:

- Description (circled `i` icon)
- Drill-down (lightning bolt)
- Filter (funnel icon)

Copyright © 2025 VisionOSS Limited. All rights reserved.



When a table widget is selected, it is also possible to switch to another widget format during the edit and design process. The **Widget Type** can be updated from the dropdown. Changes are reflected in real-time during the design of a widget or by using the widget's **Refresh** icon.

Table widget example with Select Query and Partition By

The example below shows a table widget configuration using an Automate Analyzed resource, with **Select Query** and **Partition By** operations on fields, as well as a **Filter** on one of the fields. Consider the following **Data Settings**:

- **Resource**: Cisco UCM User
- **Fields**:
  - Site. **Operation**: Select Query
  - firstName. **Operation**: Partition By
  - firstName. **Operation**: Select Query
- **Filters**
  - firstName. **Operation**: Regex (Case sensitive), **Filter Value**: `^Be`

In this case, sites and user first names are selected where first names are used to

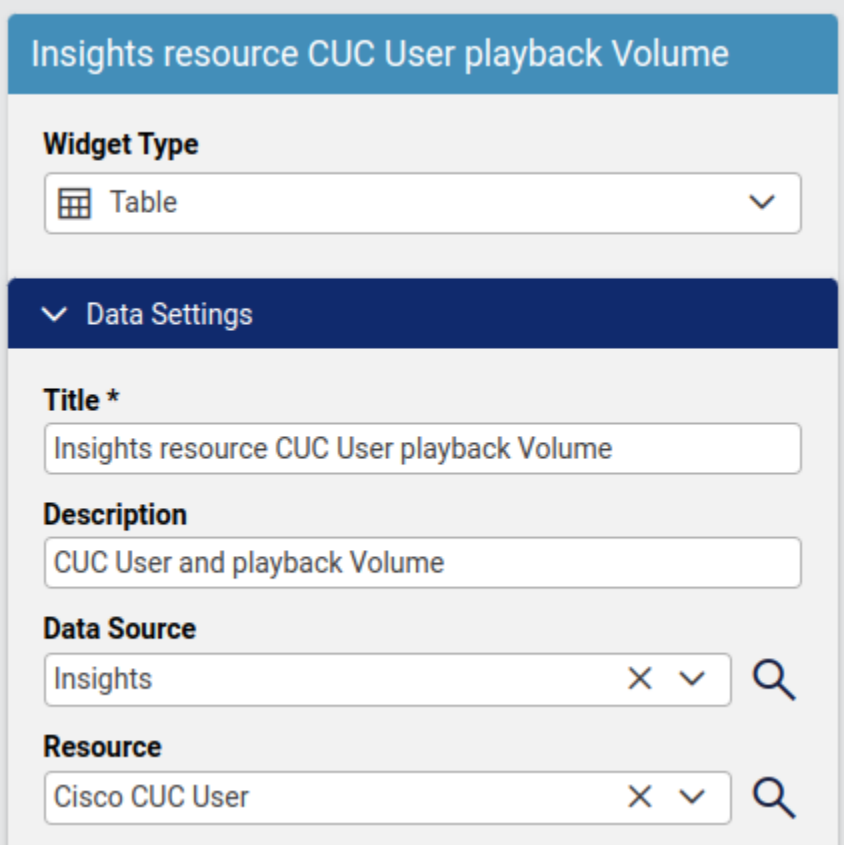
Table widget example with drill-down

The example below shows a table widget configuration using an Automate Analyzed resource, the resultant output display and also a drill-down result.

Copyright © 2025 VisionOSS Limited. All rights reserved.

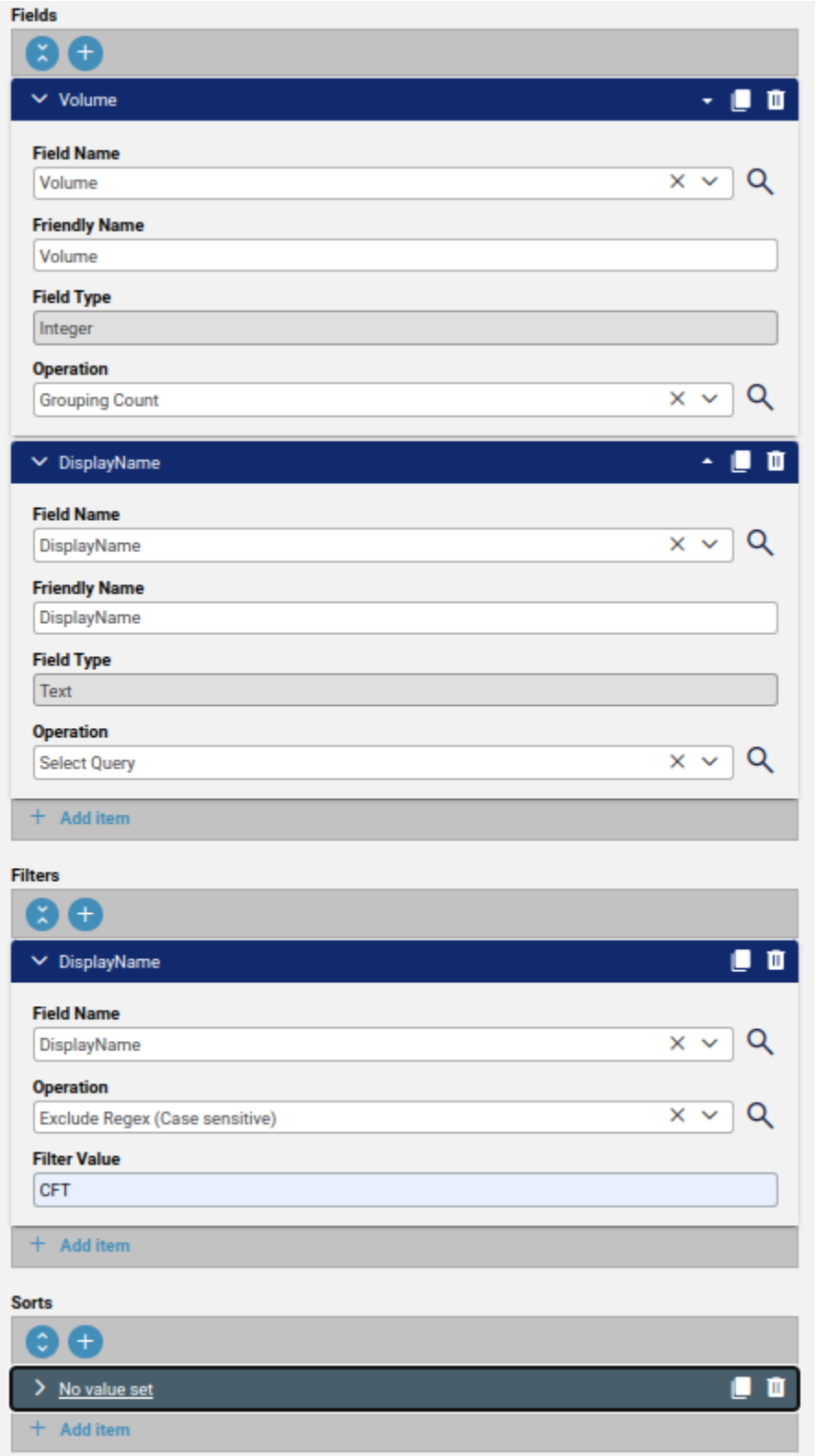
Configuration

- **Resource**: Cisco CUC User



- **Fields**:
  - Playback volume (integer) is selected as a table column and similar values are grouped using **Operation**: Grouping Count
  - The user's DisplayName is as a table column
  - **Field Type**: A read-only field indicating the data type of the selected **Field Name**. For example, if the **Data Source** is **Arbitrator**, a **Resource** instance may show the **Field Type** as `Calculated - Text`.
- **Filters**
  - DisplayName values containing regex `CFT` are excluded with a filter.
- **Sorts**: no sorting is done on any column.

Copyright © 2025 VisionOSS Limited. All rights reserved.

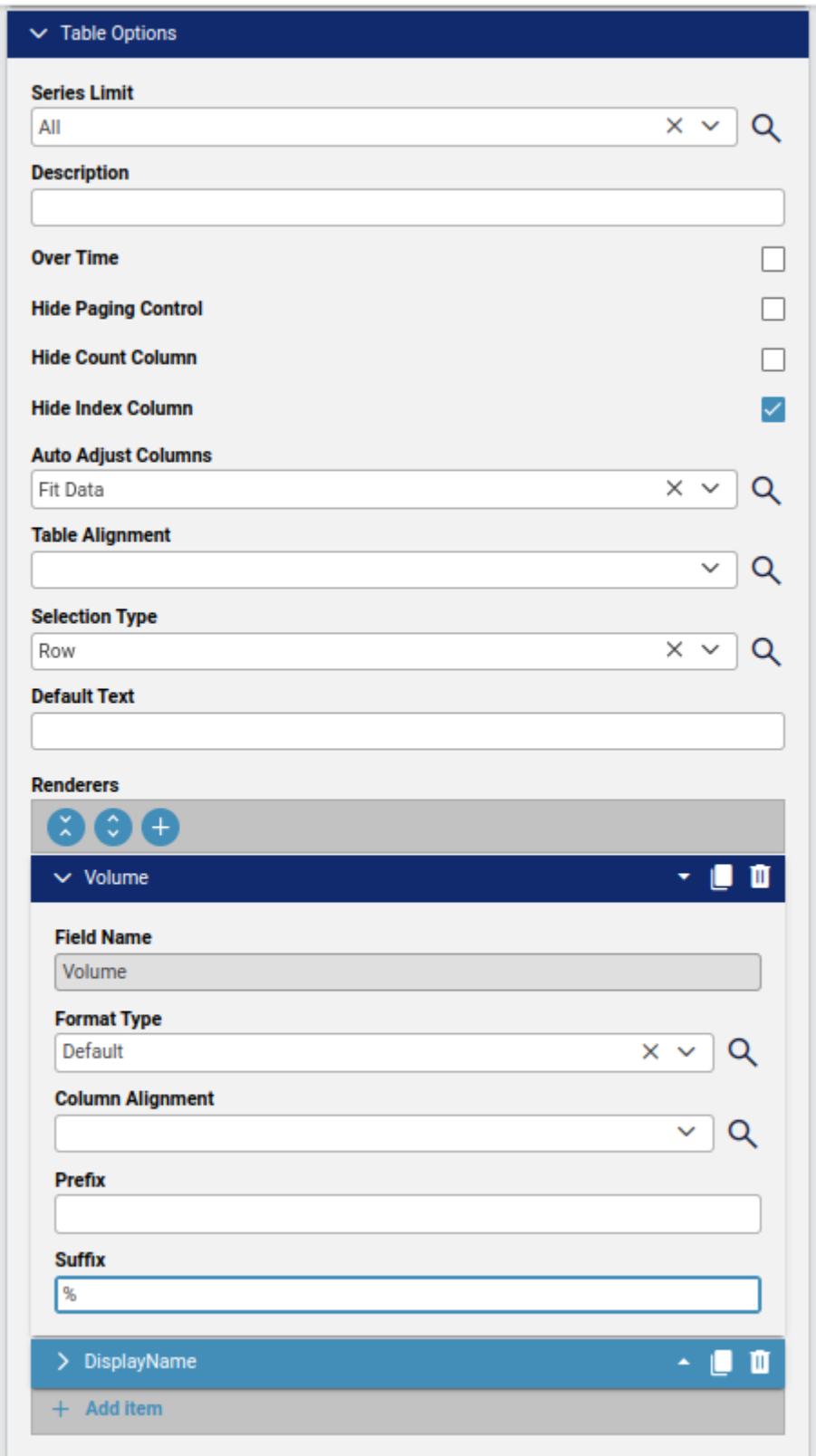


- **Table Options**
  - **Series Limit**: left at default All so no restriction on the number of values to show.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Over Time**: For table data containing timestamp columns, this option can be enabled to expose a **Use Over Time Day Pagination** checkbox and an **Interval** dropdown so that table paging of data can be grouped and the paging range can be shown according to the selected interval.
- **Hide Count Column**: enabled so an additional column containing the **Count** is not shown.
- **Hide Index Column**: enabled so an additional first column containing an index value (row number) is not shown.
- **Selection Type**: left at default so that a table entry selection selects an entire row.
- **Renderers**: the Volume field configured so that its integer value has **Suffix**: `%`.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Other **Renderers** options:

A field on a table can also be modified if the **Resource** is **Automate Analyze**:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Format Type** = **Default**: field type remains as defined (default)
- **Format Type** = **Text**: field value rendered as text - allows for a default theme-related color mapping of text (**Text Color Mapping**) and table cell (**Cell Color Mapping**) to apply.

  Contact VOSS if a custom color mapping is required.
- The **Font Size** and **Font Weight** can also be set here if the **Format Type** of a field is Text.
- **Column Alignment**: for text - to override the table alignment for the selected field.
- **Prefix** and **Suffix**: for text and numbers - options to add a string prefix or suffix to the field value.
- **Format Type** = **Traffic Light**: field value replaced by a "traffic light" colored icon - allows for default theme-related color mapping.
- **Format Type** = **Tick Cross**: field value replaced by a "cross" (`X`) colored icon - *does not* allow for color mapping.
- **Format Type** = **Number**: number-specific options are available:
  - **Number Type**:
    - **Default**: standard value: 2 decimals
    - **Abbreviation**: no decimal
    - **Bandwidth** and **Throughput**: additional options to specify **Bit**/**Bite** type
    - **No Format**: e.g. no thousands comma
  - **Float Precision**: for float numbers, the decimal precision (default = 2)
  - **Factor**: multiply the value by a factor (default = 1)
- **Hide Column**: hide the field column on a table (e.g. if the field is used for calculation, other purposes)

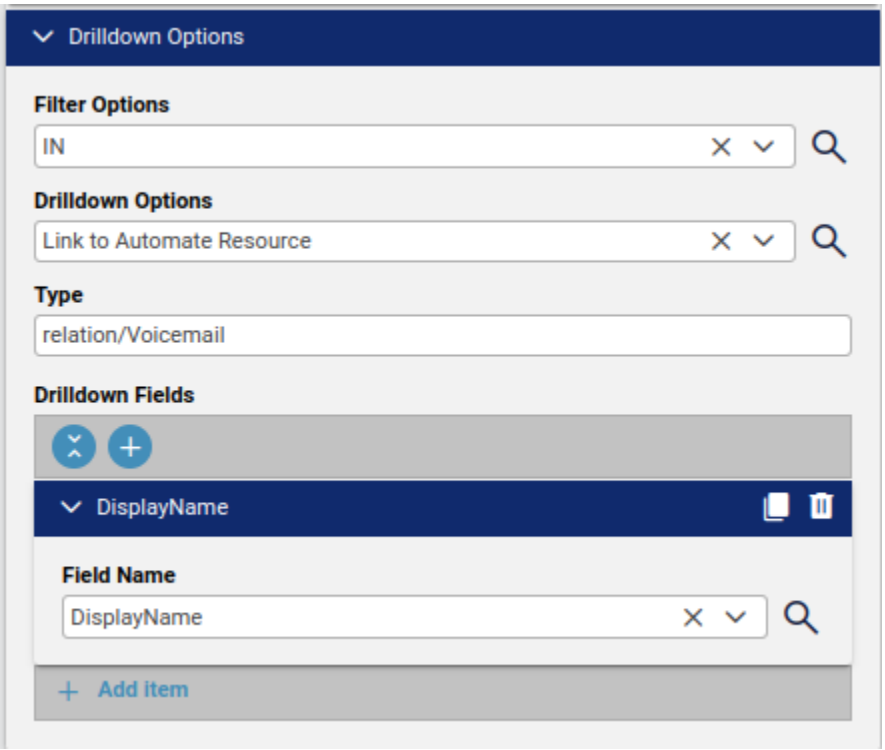
Note: By default, a number of table colours are matched with the current GUI theme. For details on these colours, see the *Branding tab* section under *Manage themes*.

In particular:

- Table backgrounds match **Panel Colour**
- Table text colour match **Panel Text Colour**

- **Drill-down options**
  - **Filter Options**: set to IN so that a drill-down display contains DisplayName.
  - **Drilldown Options**: selecting a row - the choice will `Link to Automate Resource` specified as **Type**
  - **Type**: the Automate resource type: selected the related Automate resource: `relation/Voicemail`.
  - **Drilldown Fields**: the field to highlight in the table as a drill-down link: selected DisplayName.

Copyright © 2025 VisionOSS Limited. All rights reserved.

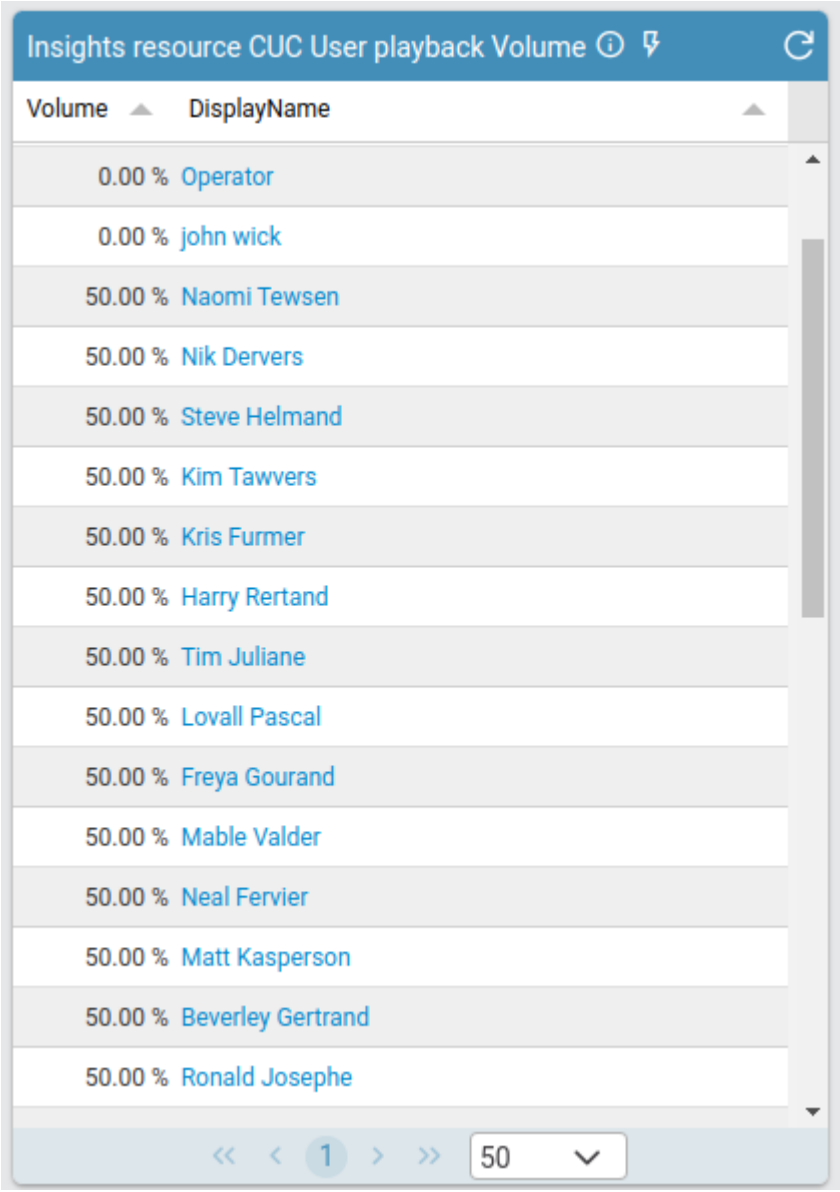


- Output

  The table shows 2 columns:

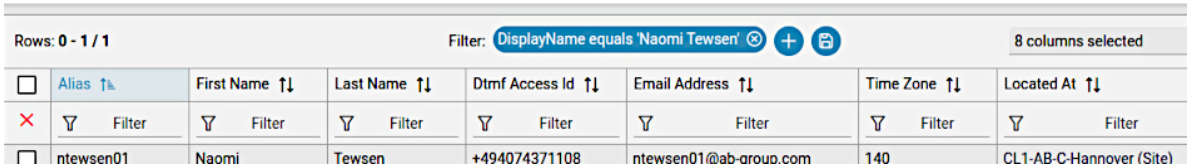
  - Volume values with % suffix
  - DisplayName with drill-down link

Copyright © 2025 VisionOSS Limited. All rights reserved.



- Drill-down result

  Selecting a row link from the table shows the item as listed in the selected **Drilldown Options**.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Text widgets

Overview

Text widgets are used to display custom text on a dashboard.

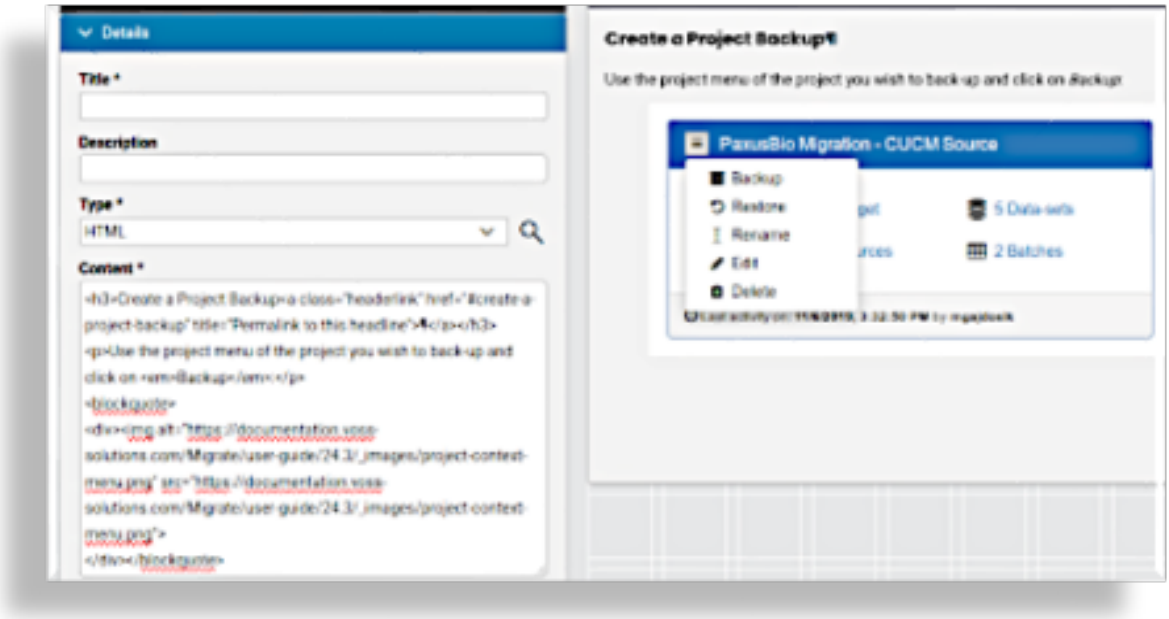
Related topics

- *Links widgets*
- Global Settings in the Core Feature Guide

Input and preview

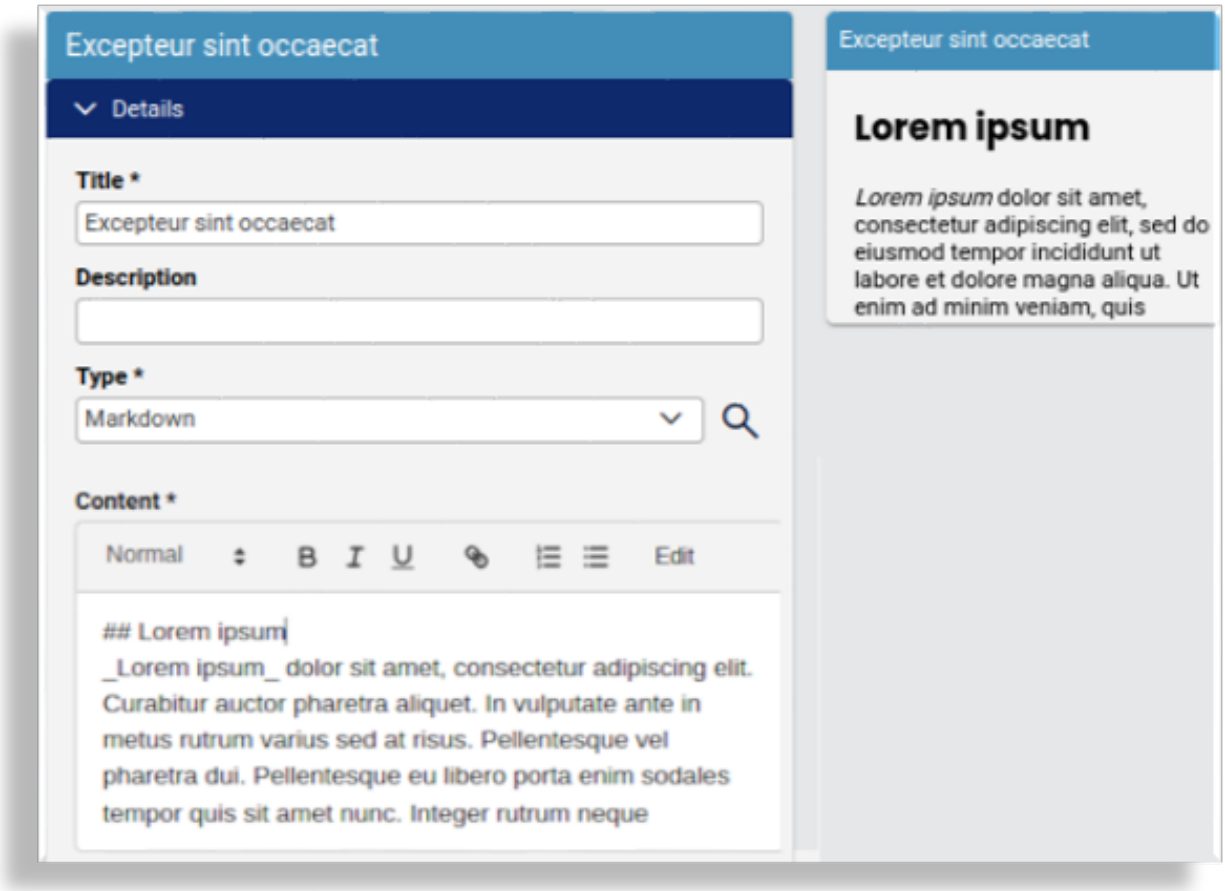
Text widgets are flexible and can be styled using either HTML or Markdown formats. Use the **Preview** option to see how your formatted text will appear in the **Content** input box before saving.

The image shows an example of a text widget with HTML input:



The image shows an example of a text widget with markdown input:

Copyright © 2025 VisionOSS Limited. All rights reserved.



Conditional display

You can use a system macro to set a condition that controls whether a text widget appears on a dashboard. This condition must evaluate to either True or False, based on features, services, and devices enabled in the Global Settings. See for example the macros listed in *Links widgets*.

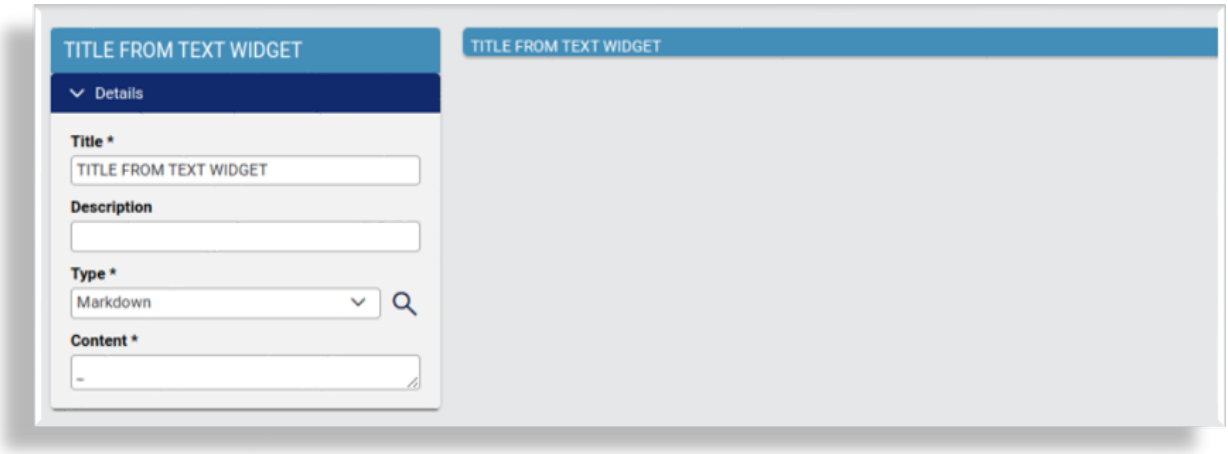
Use cases for text widgets

Text widgets are ideal for:

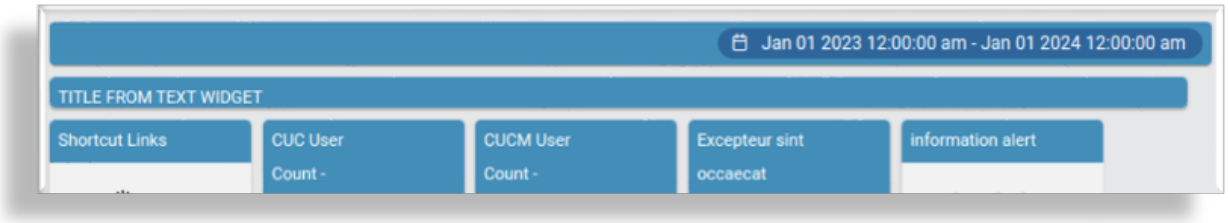
- Adding headings or section labels
- Displaying instructions or notes
- Highlighting important information

The image shows the design phase for a text widget:

Copyright © 2025 VisionOSS Limited. All rights reserved.



The image shows the display once you save your design:



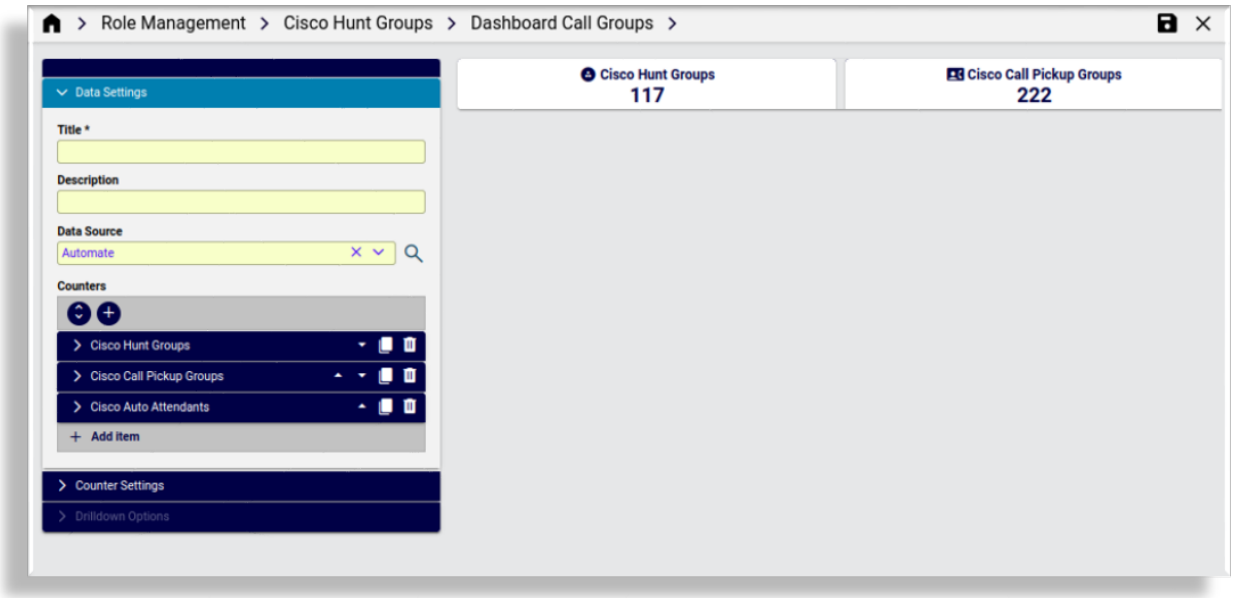
Dashboards for a Business Admin role

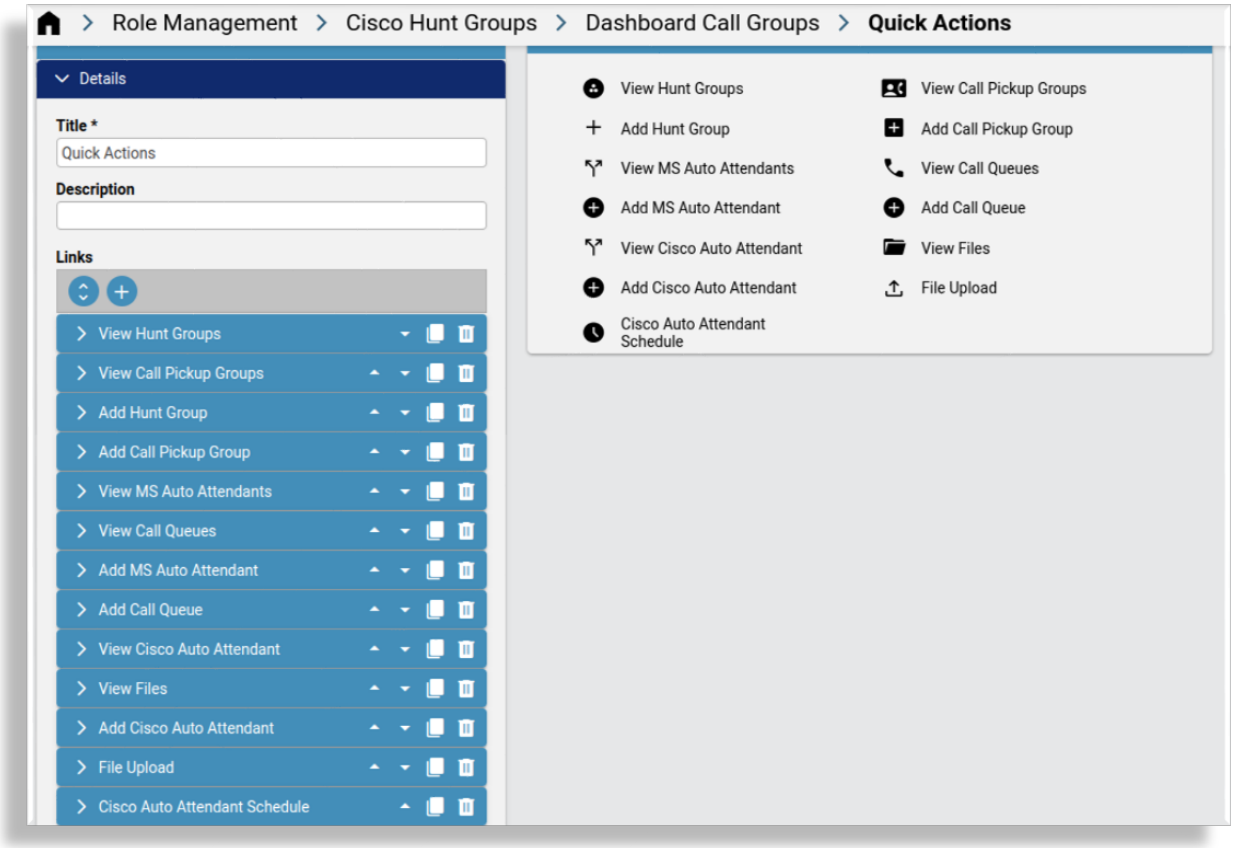
Automate provides a set of dashboards, menu layouts, and field display policies that are used in two sample menu layouts - for use or customization as a Business Administration Portal menu layout to be added to a user's role.

Example dashboards - Business Admin role

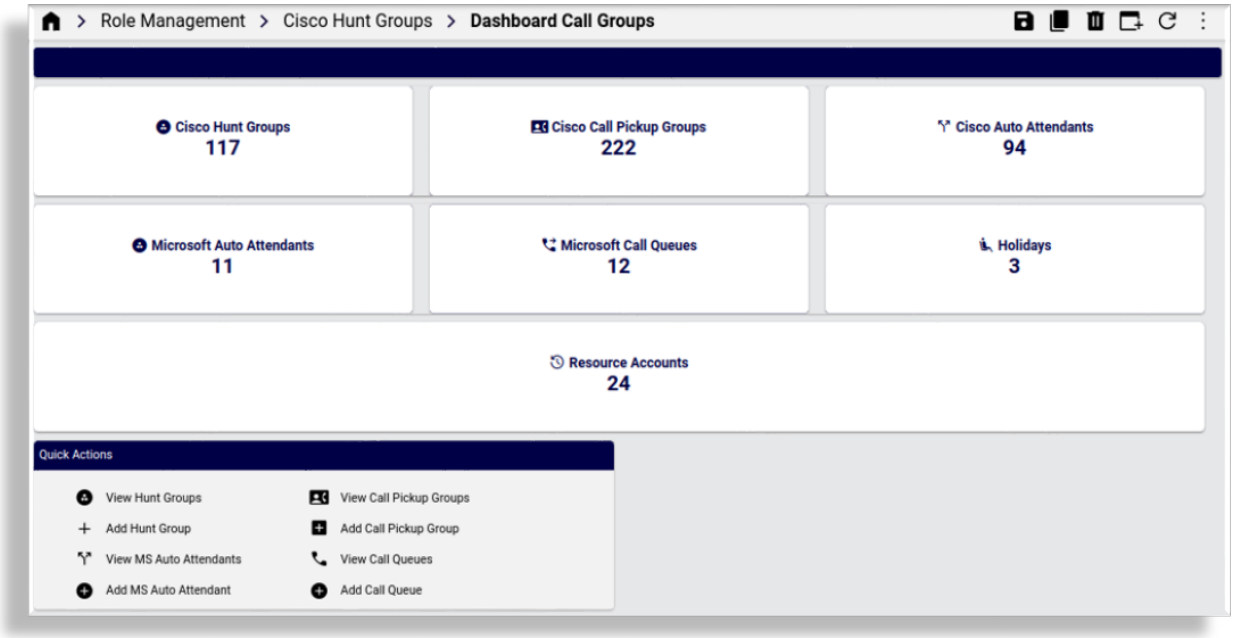
Copyright © 2025 VisionOSS Limited. All rights reserved.

Example - Call groups setup and display

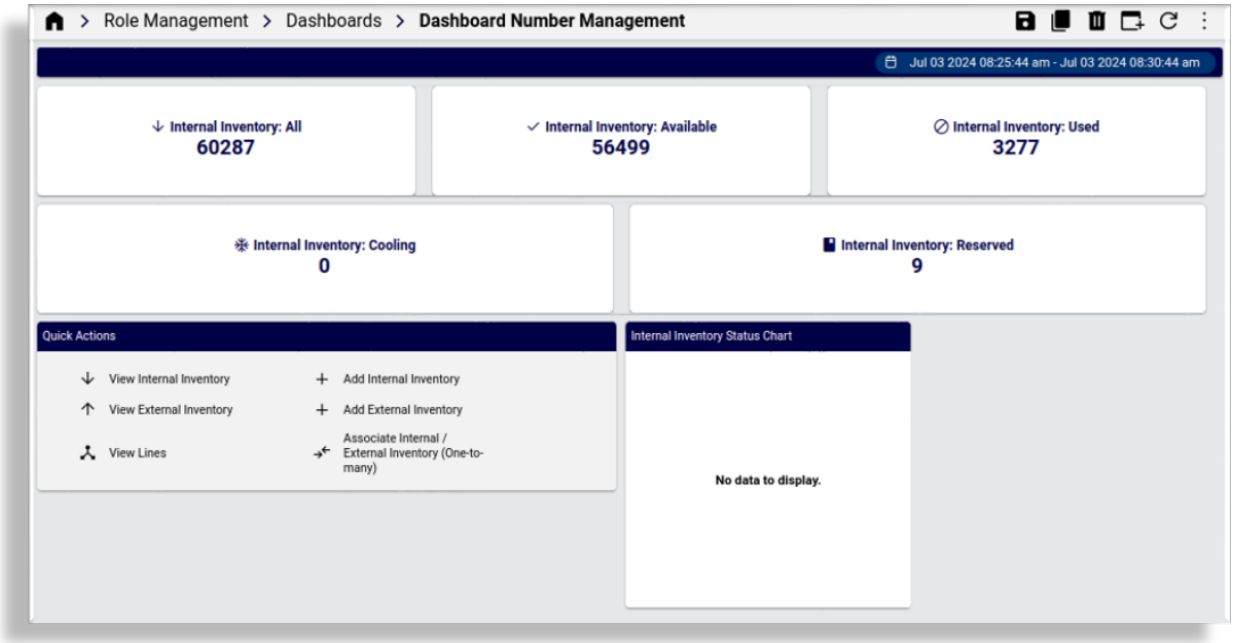




Copyright © 2025 VisionOSS Limited. All rights reserved.



Example - display of Number Management dashboard



Dashboard names grouped by sample menu layout names The following lists are the dashboard names grouped by the provided sample menu layout names.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field Display Policies

- Field display policies with `customer_admin` in their names are also provided and used for some of the links in the dashboards.
- Field display policies with `BusinessAdmin` in their names are also provided and used for some of the links in the dashboards.

Dashboards: MenuSiteAdmin

- Dashboard Number Management
- Dashboard MV Users
- Dashboard Phones
- Dashboard Headsets
- Dashboard Voicemail
- Dashboard Collaboration
- Dashboard Conferencing
- Dashboard Contact Center
- Dashboard Call Groups
- Dashboard MS Exchange
- Dashboard Tools

Dashboards: MenuCustomerAdmin

- Dashboard Site Management
- Dashboard Number Management
- Dashboard MV Users
- Dashboard Phones
- Dashboard Headsets
- Dashboard Voicemail
- Dashboard Collaboration
- Dashboard Conferencing
- Dashboard Contact Center
- Dashboard Call Groups
- Dashboard MS Exchange
- Dashboard Tools

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dashboard management reference

Automate dashboard trends resources

For the Data Source: **Automate Analyzed**, Automate provides additional list of **Resource** instances that can be used to represent *trends* on a widget.

Note:

- Currently, trends resources themselves cannot be managed (added, modified). Only existing, provided trends resources can be used on a dashboard.
- A trend resource requires associated data to be available in the system. For example, to use the **Cisco UCM Phone Trend Metrics** resource, Cisco UCM phones need to be present on your system.

Trends resources have the following properties:

- **Frequency**: how often data is recorded, for example: Daily or Weekly.
- **Retention period**: how long data is retained in the database for trend purposes. The retention period for all provided trend resources is: 3 months.
- **Filters**: a list of data resources processed. For example, multi vendor users would include Microsoft Licensed Users, Cisco UCM Users, Webex Calling in Webex App Users and so on.

The available trends resources and their properties are indicated below:

- Cisco UCM Phone Trend Metrics
  - frequency: daily
  - retention period: 3 months
  - filters:
    - Total Phones
- Multi vendor user view trend metrics
  - frequency: daily
  - retention period: 3 months
  - filters:
    - Total Users
    - Licensed Users
    - Voice Users
    - Microsoft Licensed Users
    - Microsoft Teams Collaboration Only Users
    - Microsoft Teams Phone System Users
    - Microsoft Teams Users with LineURI configured
    - Microsoft Email Exchange Users
    - Webex Calling in Webex App Users
    - Webex Calling in Webex App (Unified CM) Users

Copyright © 2025 VisionOSS Limited. All rights reserved.

    - Cisco UCM Users
    - Cisco Extension Mobility Users
    - Cisco Unity Connection Users
- Number Inventory Trend Metrics
  - frequency: daily
  - retention period: 3 months
  - filters:
    - Total Numbers
    - Available Numbers
    - Used Numbers
    - Reserved Numbers
    - Cooling Numbers
    - Cisco Numbers
    - Microsoft Numbers
    - Webex Numbers
    - Non-vendor Numbers
- Site Trend Metrics
  - frequency: weekly
  - retention period: 3 months
  - filters:
    - Total Sites

Filter options availability and definitions

The operators below are available as filter options for Insights resource field types:

Text

- LIKE (Case Sensitive) - based on the pattern entered in the filter field, will return the data that matches the pattern from the extracted string. This function is case sensitive. An underscore (_) in the pattern indicates matches any single character while a percentage sign (%) indicates matches any sequence of zero or more characters.
- NOT LIKE (Case Sensitive) - based on the pattern entered in the filter field, will return the data that does not match the pattern from the extracted string. This function is case sensitive. An underscore (_) in the pattern indicates matches any single character while a percentage sign (%) indicates matches any sequence of zero or more characters.
- ILIKE (Case Insensitive) - based on the pattern entered in the filter field, will return the data that matches the pattern from the extracted string. It is *not* case sensitive. An underscore (_) in the pattern indicates matches any single character while a percentage sign (%) indicates matches any sequence of zero or more characters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- NOT ILIKE (Case Insensitive) - based on the pattern entered in the filter field, will return the data that does not match the pattern from the extracted string. This function is *not* case sensitive. An underscore (_) in the pattern indicates matches any single character while a percentage sign (%) indicates matches any sequence of zero or more characters.
- Equals (=) - based on the pattern entered in the filter field, will return the data that is equal to the pattern from the extracted string.
- Not Equal (!=) - based on the pattern entered in the filter field, will return the data that is not equal to the pattern from the extracted string.
- IN - based on the pattern entered in the filter field, will return the data that exists within a comma separated list, i.e. 1, 2, 3, 4.
- NOT IN - based on the pattern entered in the filter field, will return the data that *does not* exist within a comma separated list, i.e. 1, 2, 3, 4.
- REGEX (Case Sensitive) - utilizes POSIX Regular Expressions to extract data. It is case sensitive.
- REGEX (Case Insensitive) - utilizes POSIX Regular Expressions to extract data. It is *not* case sensitive.
- EXCLUDE REGEX (Case Sensitive) - utilizes POSIX Regular Expressions to extract the data that does not match the pattern. It is case sensitive.
- EXCLUDE REGEX (Case Insensitive) - utilizes POSIX Regular Expressions to extract the data that does not match the pattern. It is *not* case sensitive.

Integer

- Less Than (<) - based on the value entered in the filter field, will return the data that is less than the value from the extracted string.
- Greater Than (>) - based on the value entered in the filter field, will return the data that is greater than the value from the extracted string.
- Less Than or Equal (<=) - based on the value entered in the filter field, will return the data that is less than or equal to the value from the extracted string.
- Greater Than or Equal (>=) - based on the value entered in the filter field, will return the data that is greater than or equal to the value from the extracted string.
- Equals (=) - based on the value entered in the filter field, will return the data that is equal to the value from the extracted string.
- Not Equal (!=) - based on the value entered in the filter field, will return the data that is not equal to the value from the extracted string.
- IN - based on the values entered in the filter field, will return the values that exists within a comma separated list, i.e. 1,2,3,4.
- NOT IN - based on the values entered in the filter field, will return the values that *does not* exist within a comma separated list, i.e. 1,2,3,4.
- REGEX (Case Sensitive / Insensitive) - utilizes POSIX Regular Expressions to extract data.
- EXCLUDE REGEX (Case Sensitive / Insensitive) - utilizes POSIX Regular Expressions to extract the data that doesn't match the pattern.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Chart options availability and definitions

Note: By default, a number of chart colours are matched with the current GUI theme. For details on these colours, see the *Branding tab* section under *Manage themes*.

In particular:

- Chart backgrounds match **Panel Colour**
- Chart text colour match **Panel Text Colour**

Chart Option Definitions:

- **Series Limit**: Maximum number of groups to display on a chart.
  - **All**: (default) show all values
  - <number>: show maximum <number> values
- **Description**: Allows you to enter a description of the chart to be displayed along the top portion of the chart.
- **Chart Color Mapping**: Available when a **Chord Diagram Chart** widget type is selected.
- **Label and Legend** (Font weight & size):
  - Pie chart: Label and legend font weight and size can be adjusted for key and value
  - Gauge chart: Label font weight and size can be adjusted (legends are not available on gauge charts)
  - Chord, Column, and Line charts: Label and legend font weight and size can be adjusted
- **Chord Diagram Type**: Available when a **Chord Diagram Chart** widget type is selected. **Sankey** (chords in a flat diagram) or **Dependency Wheel** (chords in circular diagram) are available as diagram types for this widget.
- **Over Time**: By selecting this check box the chart will display the data over the specified time based on the **Interval**, i.e. Minute, Hour, Daily, Weekly and Monthly.
- **Interval**: Used by **Over Time**: Minute, Hour, Daily, Weekly and Monthly.
- **X Title**: Text label displayed along the bottom of the X axis of column and line charts.
- **Y Title**: Text label displayed along the bottom of the Y axis of column and line charts.
- **Is Stacked**: By selecting this check box the chart will stack values by **Stack Type**.
- **Stack Type**: Only for column charts. By selecting this box the chart will stack the values based on the type selected:
  - **None**: (default) no stacking; individual columns for data
  - **Normal**: data stacked into a single column, color coded with values
  - **Percentage**: data stacked into a single column, color coded with percentages
- **Numeric Precision**: Select the decimal precision displayed for each point.
- **Is Horizontal**: By selecting this check box, the chart will display the columns/bars horizontally across the chart.
- **Is 3D**: By selecting this check box, column charts and pie charts will be displayed in a 3D representation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Show Labels**: By selecting this check box, each value that defines the chart will be labeled on the chart.
- **Show Legend**: By selecting this check box, the Field Definition for the values being charted will be displayed in the selected position on the chart with the associated color representation.
- **Gauge Label**: Labels the middle of the gauge with value from field extraction.
- **Min** and **Max**: Place the starting value (**Min**) and the ending value (**Max**) for the gauge needle to traverse, e.g. start at 0 and end at 60,000.
- **Label Inside**: By selecting this check box the value will be labeled with the definition based on the field extraction.
- **Show Bands**: By selecting this check box then the gauge will have a maximum of 3 colored bands indicating certain severity levels. These are user defined thus a good, minor and major severity can be easily defined based on the data elements extracted. Simply place values for each color in the associated box to represent the percentage of the gauge band that color is to occupy. Tip: Make your major issue (Red) 100 thus simply modifying the good and minor automatically recalculates the major.
- **Is Doughnut**: A pie chart is displayed with a hole in the middle.
- **Show Numbers**: A pie chart by default shows slices as a percentage. Use this option to instead show the values of the percentage.

Available **Chart Options** vary according to the chart type:

Chart Option	Column Chart	Gauge Chart	Line Chart	Pie Chart
Series Limit	X		X	X
Description		X	X	X
Over Time	X		X	
Interval	X		X	
X Title	X		X	
Y Title	X		X	
Is Stacked			X	
Stack Type	X			
Numeric Precision	X			
Is Horizontal	X			
Is 3D	X			X
Show Labels	X		X	X
Show Legend	X		X	X
Gauge Label		X		
Min		X		
Max		X		
Label Inside		X		
Show Bands		X		
Is Doughnut				X
Show Numbers				X

Copyright © 2025 VisionOSS Limited. All rights reserved.

Drill-down options and conditional syntax

Drill-down options

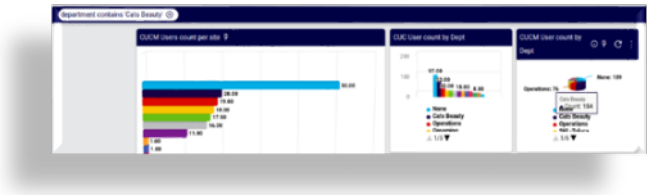
- **Filter Options**: apply to field value match of a selection of the chart or table data (IN, REGEX)

  For example, if **Filter Other Widgets** is selected, then IN will match “Ann” exactly in other widgets and REGEX will match “Ann”, “Anne”, “Annie”.

- **Drilldown Options**: the behavior when selecting an item in a chart or table
  - **None** (default)
  - **Filter Other Widgets**: a selected drilldown item will update any other widget that also references the same data instance.

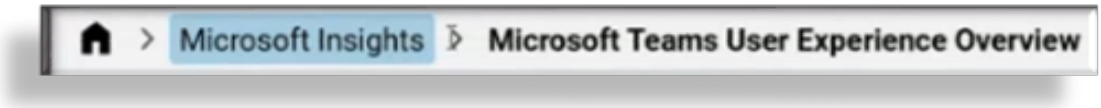
    For example a drilldown on a CUC user table where this is enabled, will similarly impact widgets such as charts, counters and tables related to CUC users, so that these widgets will then reflect data from only the single user from the drilldown.

    In the example below, the chart widget called **CUCM User count by Dept** has the **Filter Other Widgets** drilldown filter enabled, so that for example selecting a department from the chart also filters the **CUCM Users count per site** chart to only show users at sites belonging to the selected department. The department filter (here: `department contains 'Cats Beauty'`) is also displayed when the filter is active.



  - **Link to Another Dashboard**

    Used to open another existing dashboard during drilldown. A **Dashboards** dropdown shows to select the other dashboard. Navigation can then be carried out from the linked dashboard to the parent dashboard:



  - **Launch Third-party URL**
    * Launch a system URL in the system portal. The format of the input is an endpoint relative to the portal: `https://<hostname>/portal/`. For example, if the value entered is `#/admin`, then the drilldown will launch the admin home page dashboard: `https://<hostname>/portal/#/admin`.
    * Launch an external, non-system URL in the system portal (if allowed). The format of the input is the full external URL: `https://<eternal-host>`
  - **Conditional Drilldown**

    Provides a **Conditional Drilldown** input box into which a JSON formatted condition can be entered. For details on the format, see *Conditional Drilldown Format* below.

- **Drilldown Fields**:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Field Name**: if multiple **Field** values were added for a **Resource**, select a field for the drilldown.

Conditional drill-down format

When selecting the **Conditional Drilldown** option, the condition needs to be entered in JSON format into the input box. This section provides syntax details and examples for this configuration.

If an item matching the condition is selected from the dashboard, the conditional drilldown is then carried out.

The JSON format is outlined below.

- If `conditions` are all met
- then carry out `actions`
- else Defaults (`"default..."`)
- Structure:

```
{
  "conditions": [],
  "actions": [],
  "defaultDrilldown": 1,
  "defaultDashboardId": "",
  "defaultUrl": "",
  "defaultFilterFields": []
}
```

- `conditions`:

  `conditions`: list of conditions on `rules`.

  - `id`: “integer” - zero-based
  - `name`: “text” - condition name
  - `type` : “OR” or “AND”
    - `conditions.type`: “AND” means action will be taken when *all* conditions are met.
    - `conditions.type`: “OR” means action will be taken when *one* condition is met.

- `rules`:

  `rules`: list of rules:

  - `ruleid`: “integer” - zero-based
  - `field`: “integer” - zero-based

    Field order in the drilldown tab (0 base)
  - `fieldType`: “text”, “integer” or “float”
  - `operator`: “==”, “!=”, “<=”, “>=”, “<”, “>” or “regex”
  - `operator`: “==”, “!=”, “<=”, “>=”, “<”, “>” or “regex”
    - `fieldType` text `operator` choices: “==”, “!=”, “regex”
    - `fieldType` integer and float `operator` choices: “==”, “!=”, “<=”, “>=”, “<”, “>”
  - `value`: value of the field; according to `fieldType`: “text”, “integer” or “float”

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `actions`:

  List of actions:

  - `drilldown`: “integer”
    - Drilldown type:
      - 1 (drilldown to other widgets)
      - 2 (drilldown to other dashboard: `dashboardid`)
      - 4 (drilldown to external link: `url`)
  - `dashboardid`: “text”

    The ID is available as `dashboard_id` URL parameter value when on a dashboard.
  - `url`: “text”

    The value is a URL containing position variables for `filterFields` references, whose values in turn are substituted into the URL. The position variables are one based, for example:

    `"url": "https://{1}/ui/index.html?{2}"`

    refers to the first and second `filterFields` list entries, which in turn take the format

    `"filterFields": [0,1]`

    The value of the first `filterFields` entry is therefore for example substituted into the URL variable `{1}` above.
  - `filterFields`: list of fields (“integer” = index number)

    Field order in the drilldown tab (0 base)
- Defaults:
  - `defaultDrilldown`: “integer”
  - `defaultDashboardid`: “text”
  - `defaultUrl`: “text”
  - `defaultFilterFields`: list of fields (“integer” = index number)

    Field order in the drilldown tab (0 base)

Examples

- Drill-down to other widgets

  Explanation:

  - If 7th field (`"field": 6`) data != 0 and 6th field (`"field": 5`) <= 0 then
    - run action drilldown to other widgets (`"drilldown": 1`)
      - using filter values of first, second and 4th field (`"filterFields": [0,1,3]`).
  - If the condition is not met, then
    - run default action which is drilldown to other widgets (`"defaultDrilldown": 1`)
      - using filter values of first and second field.

  JSON:

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
{
  "conditions": [
    {
      "id": 0,
      "name": "first_condition",
      "type": "AND",
      "rules": [
        {
          "ruleid": 0,
          "field": 6,
          "fieldType": "integer",
          "operator": "!=",
          "value": "0"
        },
        {
          "ruleid": 1,
          "field": 5,
          "fieldType": "float",
          "operator": "<=",
          "value": "0"
        }
      ],
      "actions": [
        {
          "drilldown": 1,
          "dashboardid": "",
          "url": "",
          "filterFields": [
            0,
            1,
            3
          ]
        }
      ]
    }
  ],
  "defaultDrilldown": 1,
  "defaultDashboardId": "",
  "defaultUrl": "",
  "defaultFilterFields": [
    0,
    1
  ]
}
```

- Drill-down to other dashboard

  Explanation:

  - If second field data is “keller, texas” or 5th field is “TX” then
    - run action drilldown to other dashboard (`"drilldown": 2`, `"dashboardid":...`)
      - using filter values of first, second and 4th field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - If the condition is not met, then
    * run default action which is drilldown to other widgets
      · using filter values of first and second field.

JSON:

```
{
  "conditions": [
    {
      "id": 0,
      "name": "first_condition",
      "type": "OR",
      "rules": [
        {
          "ruleid": 0,
          "field": 1,
          "fieldType": "text",
          "operator": "==",
          "value": "keller, texas"
        },
        {
          "ruleid": 1,
          "field": 4,
          "fieldType": "text",
          "operator": "==",
          "value": "TX"
        }
      ],
      "actions": [
        {
          "drilldown": 2,
          "dashboardid": "M2OQQMVN3IWI1O2P1686581558847Y2FRT98M8V24GS",
          "url": "",
          "filterFields": [
            0,
            1,
            3
          ]
        }
      ]
    }
  ],
  "defaultDrilldown": 1,
  "defaultDashboardId": "",
  "defaultUrl": "",
  "defaultFilterFields": [
    0,
    1
  ]
}
```

- Drill-down to external link

  Explanation:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- If second field data is “keller, texas” or 5th field is “TX” then
  - run action drilldown to other external link
    - using filter values of first and second field.
- If the condition is not met, then
  - run default action which is drilldown to other widgets
    - using filter values of first and second field.

JSON:

```
{
  "conditions": [
    {
      "id": 0,
      "name": "first_condition",
      "type": "OR",
      "rules": [
        {
          "ruleid": 0,
          "field": 1,
          "fieldType": "text",
          "operator": "==",
          "value": "keller, texas"
        },
        {
          "ruleid": 1,
          "field": 4,
          "fieldType": "text",
          "operator": "==",
          "value": "TX"
        }
      ],
      "actions": [
        {
          "drilldown": 4,
          "dashboardid": "",
          "url": "https://{1}/ui/index.html?{2}",
          "filterFields": [
            0,
            1
          ]
        }
      ]
    }
  ],
  "defaultDrilldown": 1,
  "defaultDashboardId": "",
  "defaultUrl": "",
  "defaultFilterFields": [
    0,
    1
  ]
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
}
```

Dashboard Exports

This procedure adds a dashboard export.

Note: A dashboard export can contain one or more dashboards. In the schedule for the dashboard export you can choose the dashboard data to include in the export, for example, based on specific widget data (resource type and resource attribute).

1. In the Admin Portal, go to **Dashboard Exports**.
2. Click the Plus icon (+) to add a new record.
3. Fill out a name for the report.
4. Select one or more dashboards to include in the export and move them between the transfer boxes, from **Available** to **Selected**.
5. Select the export format, Excel or CSV.

   Note: PDF export is reserved for future development.

6. Add SFTP destinations, one or more, and for each SFTP destination, provide the following details:
   - Name (mandatory)
   - Hostname (mandatory)
   - Port (optional)
   - Username (mandatory)
   - Password (optional)
   - Destination directory (optional)

   Note: You can choose to send the exported report to a SFTP destination or to a SMTP destination, or to both.

7. Add SMTP destinations, one or more, and for each SMTP destination, provide the following details:

   Note: An email server is required for SMTP destinations.

   - Name (mandatory)
   - SMTP server (mandatory)
   - From address (sender email address, mandatory)
   - To address (recipient's email address, mandatory)
   - Copy to (recipient to copy, email address, optional)
   - Blind copy (recipient to blind copy, email address, optional)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Subject (mandatory)

8. Save the report.

Related topics

- *Schedule dashboard export report*
- *Introduction to Automate dashboards*
- *Manage dashboards and widgets*

Schedule dashboard export report

This procedure schedules the export of a dashboard report and defines the type of data to export in the schedule.

Note:

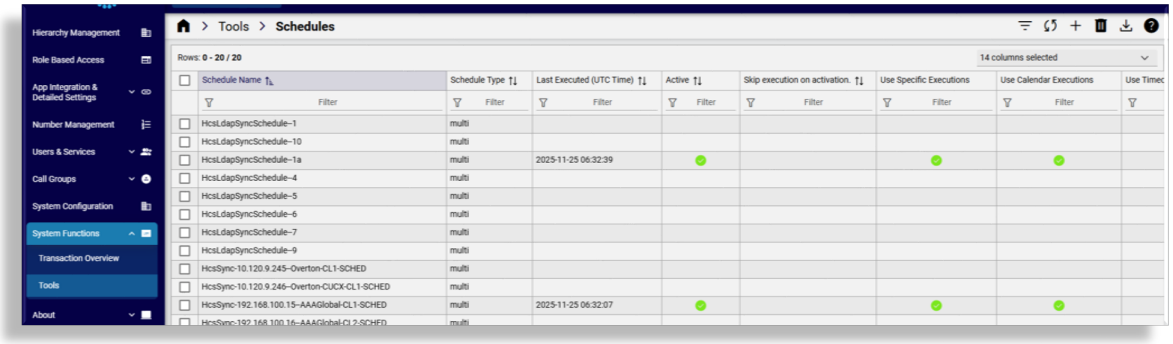
- Entire dashboards can be exported, or per widget.
- Report data is permissions-based for the user who owns the dashboard export, at their hierarchy and below.

Prerequisites:

- Add a dashboard export. See *Dashboard Exports*

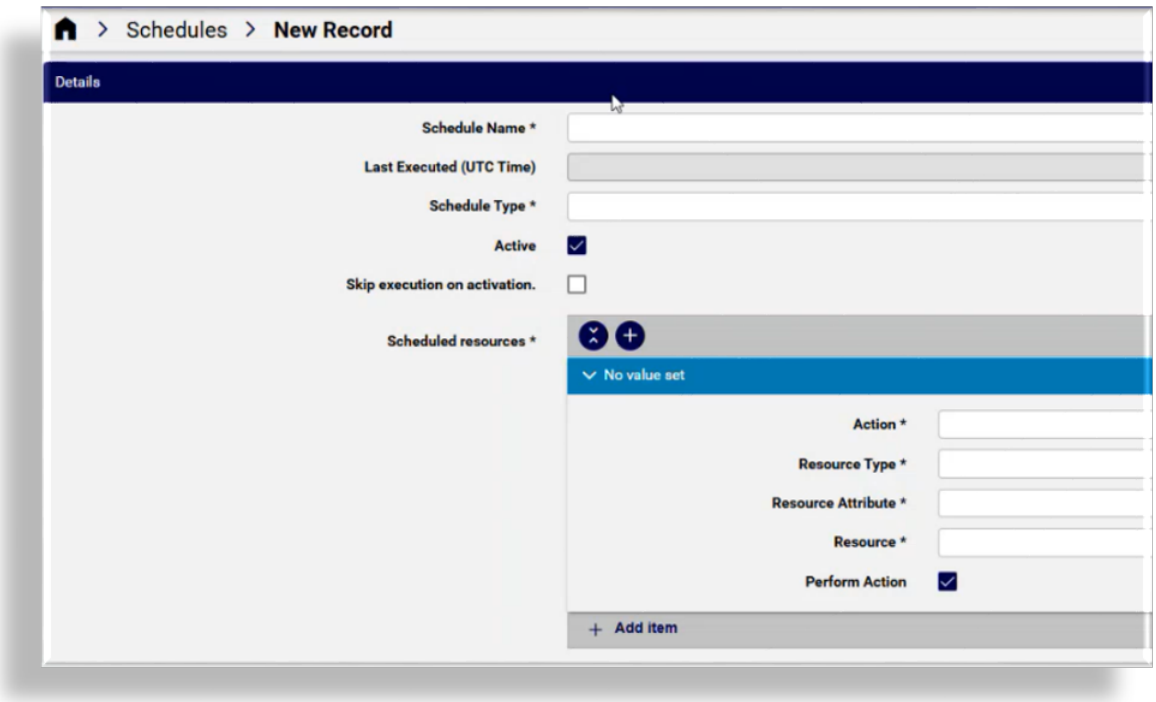
To add a schedule for a dashboard export report

1. Go to **Schedules**.



2. Click the Plus icon (+) to create a schedule.

Copyright © 2025 VisionOSS Limited. All rights reserved.



3. Fill out schedule details:
   - Schedule name (mandatory)
   - Schedule type (mandatory), either single execution or multi execution

     If selecting *multi execution* as schedule type, define whether to:
     - Use specific executions
     - Use calendar executions: Define schedule execution frequency by calendar month, day, hour, minute, and execution timezone (local)
     - Use timed executions
   - Define whether the schedule is active
   - Define whether to skip execution on activation
   - Add scheduled resources, one or more (mandatory), and provide the following details for each scheduled resource:
     - Action (mandatory): Select *Execute*
     - Resource type (mandatory): Select the model (for example, `data/DashboardExport`) to which the schedule will apply
     - Resource attribute (mandatory): Select the resource attribute (for example, `name`)
     - Resource (mandatory): Select the dashboard export you set up
     - Define whether to perform the action (*Execute*)

Note: Last executed (UTC time) is a read-only field to display the time the schedule was last executed.

4. Save the schedule.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Schedules*

5.5.2. Menu Layouts

Menu layouts

Tip: *Use the Action search to navigate Automate*

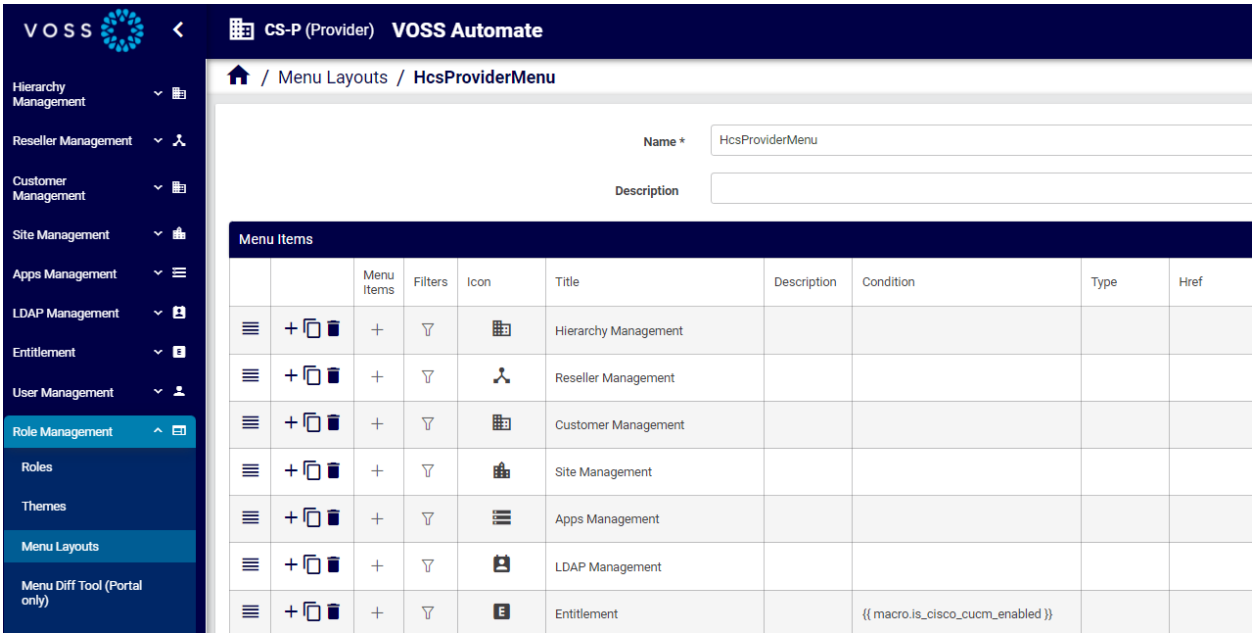
Overview

Menu layouts define the content and structure of menus in the Admin Portal, based on your user role at the hierarchy where you log in.

Automate allows an administrator (with appropriate permissions) to customize menu layouts for different user roles and hierarchy levels.

Note: By default, administrators have permissions to modify their own menu layouts and dashboards. If the assigned menu layout or dashboard is at a higher hierarchy, it can be cloned and modified at the administrator's hierarchy.

For example, the menu layouts at Provider level of the hierarchy can be different to menu layouts at Customer or Site level. Customizing menu layouts for different user roles at each hierarchy allows you to hide or show resources appropriate for different roles.



Copyright © 2025 VisionOSS Limited. All rights reserved.

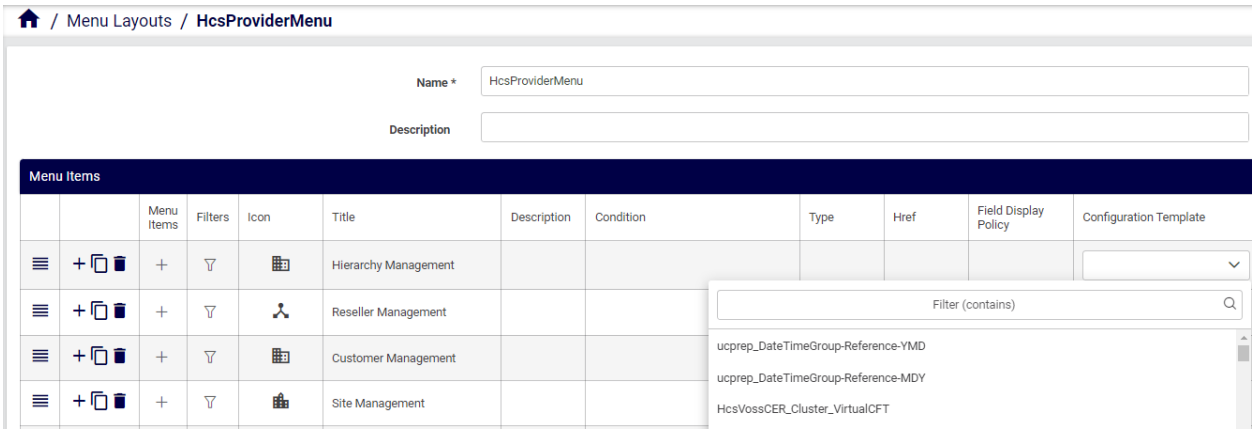
Related topics

- Navigation - Menu and Dashboards in the Best Practices Guide
- Advanced Configuration Guide
- Fixed and configurable filters in menus in the Core Feature Guide
- HCS Dial Plan Macros in Automate in the Core Feature Guide

Menu layouts, FDPs, and CFTs

When creating or editing a menu layout, you can (optionally) apply a field display policy (FDP) and configuration template (CFT) to refine the view of model entities for the user role. In this way, the FDP and CFT for a specific model is applied as part of the menu layout (in the menu structure); the FDP and CFT are attributes of the specific model entry for that menu layout. This means:

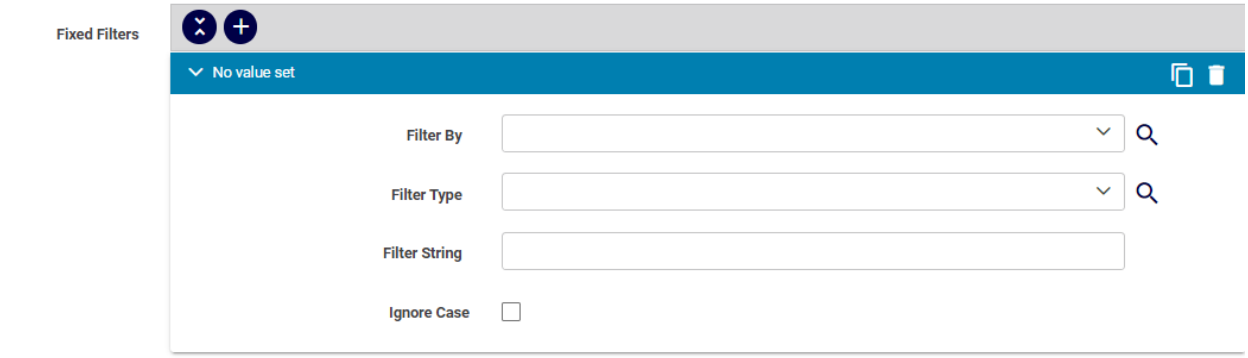
- Different FDPs and CFTs for a specific model can define menu layout variations for that model.
- The required FDP and CFT should be available before you create new menus.

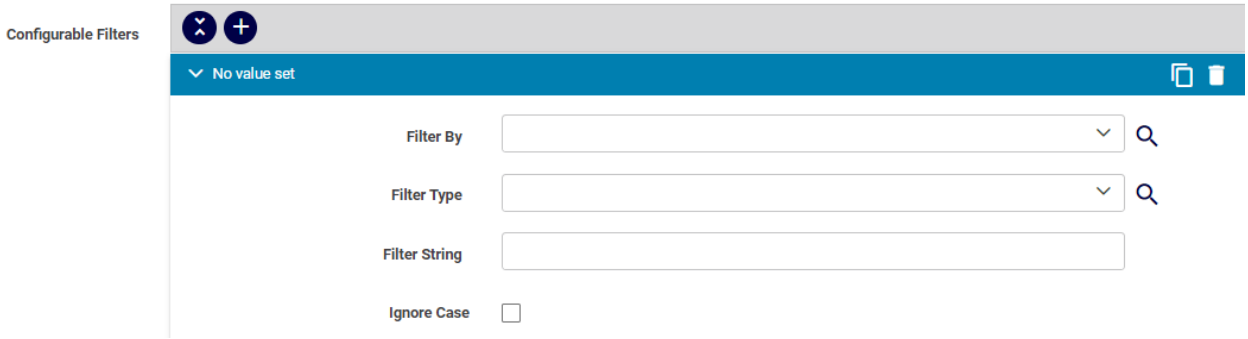


Copyright © 2025 VisionOSS Limited. All rights reserved.

Fixed and configurable filters

If a menu layout applies to the list view of a model, this list can be filtered by means of a number of filter options that apply to the displayed list. Only instances where the values of a model attribute that match the filter, are then shown. For details, see *Fixed and configurable filters in menus*





Default menu layouts

Automate ships with a number of default menu layouts for the following, hierarchy-based administrator user roles:

- System administrator
- Provider administrator
- Reseller administrator
- Customer administrator
- Site administrator

If you wish to create a new menu layout, you can create a copy (clone) of a default menu layout, edit the settings, and save it as a new, custom, menu layout.

You can also export a menu layout, edit it externally, and re-import it. For example, you can apply an alternative FDP or CFT, or change the order and grouping of items on the menu layout. Designers with access to tag or version tag can apply these to a menu layout so that it can be uniquely identified to track changes.

Note: The Automate documentation is based on the default, predefined menu layouts that ship with the system.

To work with menu layouts in the Admin Portal:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Go to **Menu Layouts** to view and edit menu layouts.
- Go to **Roles** to view the menu layout assigned to a particular role, then click on a role and view the value in the **Menu Layout** field (which displays the menu layout for users with this role).

Best practice menus

In addition to the default menu layouts, Automate provides best practice menus for Provider and Customer administrators, including the associated access profiles and dashboards.

The best practice menus are more business-oriented, and include additional options based on best practice adaptations that may also be included in Automate.

The table describes the key features of the best practice menus:

Feature	Description
Structure mapped to business use case	A menu order, nesting and naming convention based on common business use. Menus are ordered 'top-down, following the logical order of tasks and the system hierarchies that perform these tasks. Example: For Provider admins, the **Cisco UC App Management** menu has menus only for these devices, while SMTP server and other settings that Provider admins use are arranged under a menu called **Provider Configuration**. In a similar way, the **Cisco User Services** menu has sub-menus for all the functionality associated with Cisco users in Automate.
Naming convention	First word capitalized for menu names where the menu is for a *form view* (input or edit). For example **ADD Internal Number Inventory** Where such menu names start with abbreviations or acronyms, for example, E164, HCS, or LDAP, the capitalization rule applies to the next word in the name.
Menus for URLs	Included in the structure are menus that provide links to other Automate portals, allowing you to launch a another portal directly from a menu. For this to work, you must update these URLs to match your configuration.

Considerations when customizing and assigning a best practice menu

If you wish to modify a best practice menu and then assign the customized best practice menu to a user role, consider the following:

- To add or update menu layouts, see *Add or edit a menu layout*

  Note: A Menu Diff Tool allows you to easily modify menus. See the Advanced Configuration Guide for details.

- To view or configure FDPs (field display policies) associated with menu items, see *Add and edit field display policies*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To view or configure CFTs (configuration templates) associated with menu items, see *Configuration templates*.
- For details around access profiles available for the best practices menus, see the list in the **Access Profiles** menu. To modify any access profiles to align with a modified menu, see *Access profile permissions and operations*.
- Note the dashboards available for the best practices menus. See the list under the **Dashboards** menu.

Menu layouts for a Business Admin role

Automate provides two sample menu layouts for use or further customization as a Business Administration Portal menu layout. These sample menu layouts display in the **Menu Layouts** list view:

- MenuCustomerAdmin
- MenuSiteAdmin

Administrators can clone these samples to a hierarchy, customize them as needed, and assign them to a specific user role that requires a Business Administration Portal interface.

The sample menus also use sample dashboards to complete this Business Administration Portal interface. For details on the sample dashboards, see: *Introduction to Automate dashboards*.

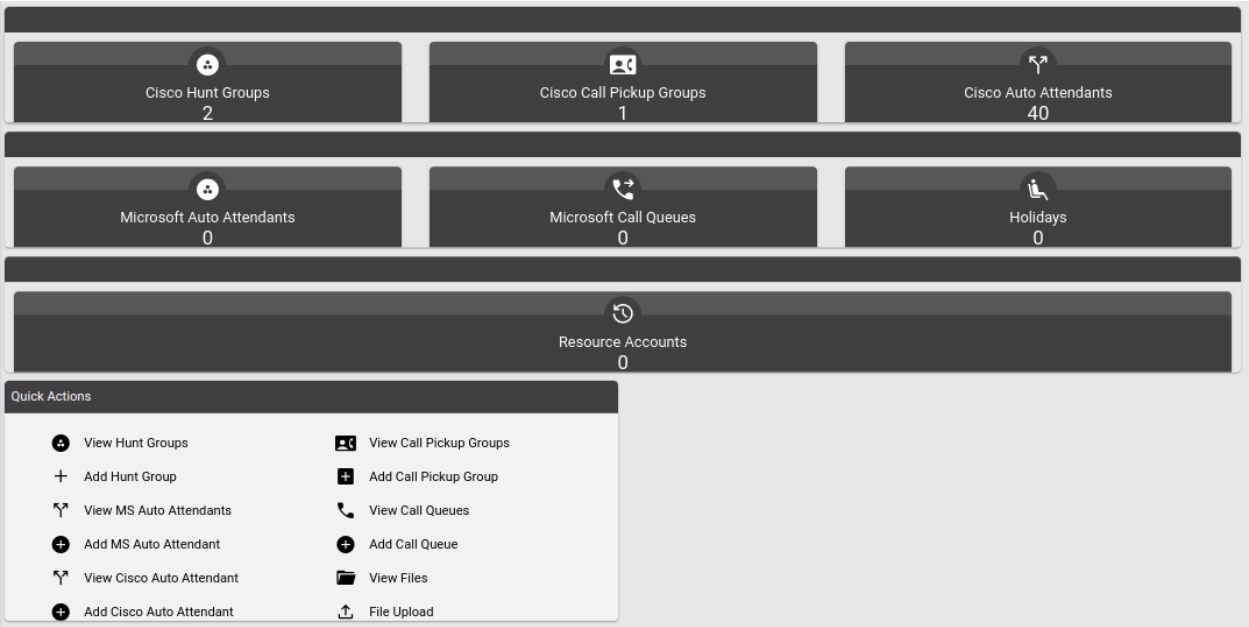
Note: The sample menus include conditions on the inclusion of dashboards in accordance with enabled features, services, and devices as in the **Global Settings**. The conditions are in the form of system macros, for example:

```
{{ macro.is_microsoft_enabled }}
```

or

```
{{ macro.is_cisco_cucm_enabled }}
```

The image shows an example of a sample menu displaying the sample Call Groups dashboard:



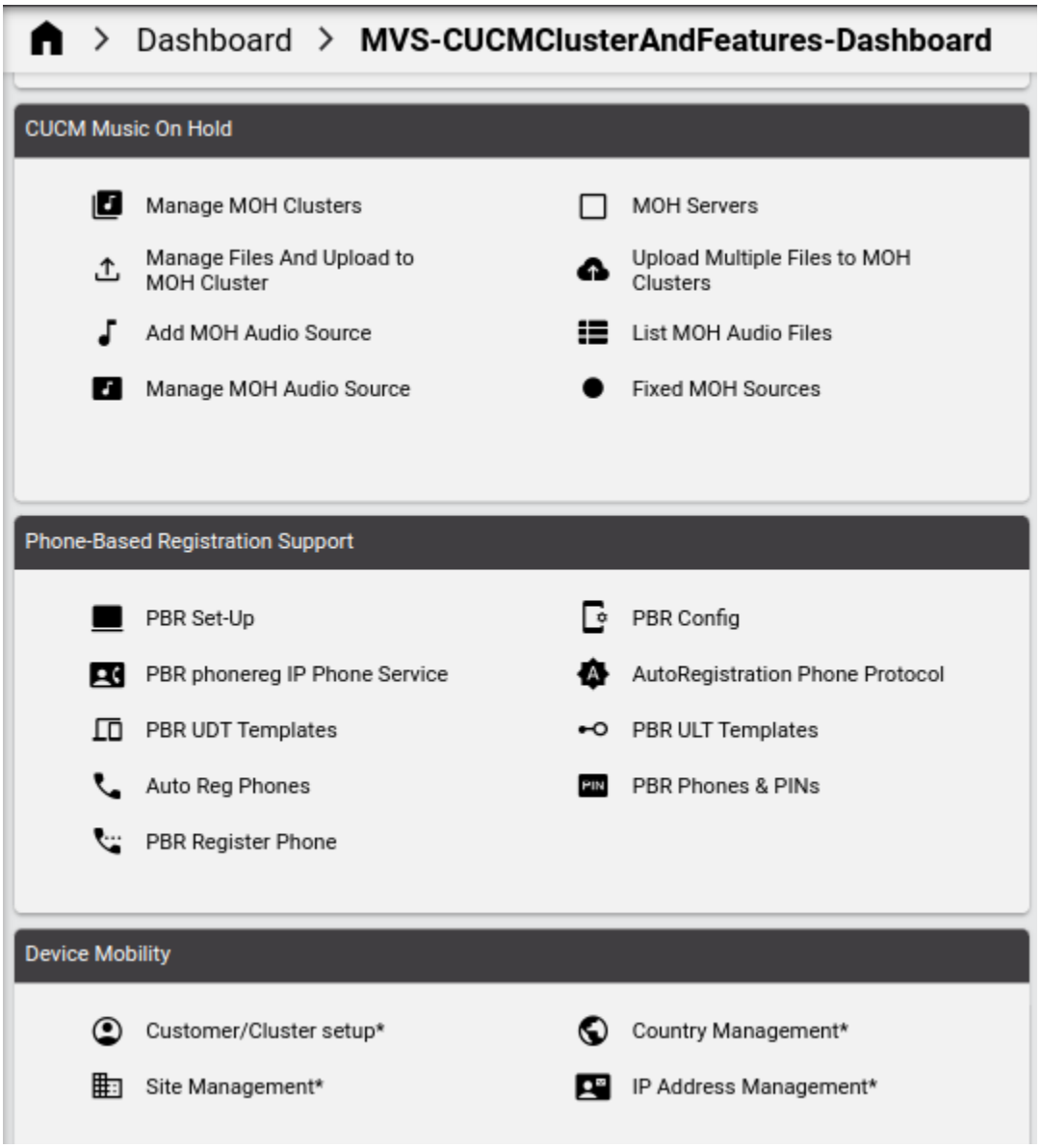
Copyright © 2025 VisionOSS Limited. All rights reserved.

Enhanced menu layouts and dashboards for multi vendor environments

Automate provides two sets of menus, dashboards, and access profiles for use or cloning and further customization for multi vendors scenarios. These sets offer best-practice reference role-sets that can be used by service providers.

The set of best practice menus and dashboards is comprehensive and includes some add-on options which are not currently included in the core solution. If you want to use a specific option and get a permission error when trying it using the `MVS-` set, please reach out to the Automate account team to discuss.

Note: Multi vendor user (mvs) dashboards and menu layouts that contain links referencing an adaptation (add-on), have an asterisk (*) postfix in the link text.



Microsoft-only deployment items contain `MS-Only` in the name, and menu names have the `MVS` prefix:

- `MVS-EnhancedProviderMenu`

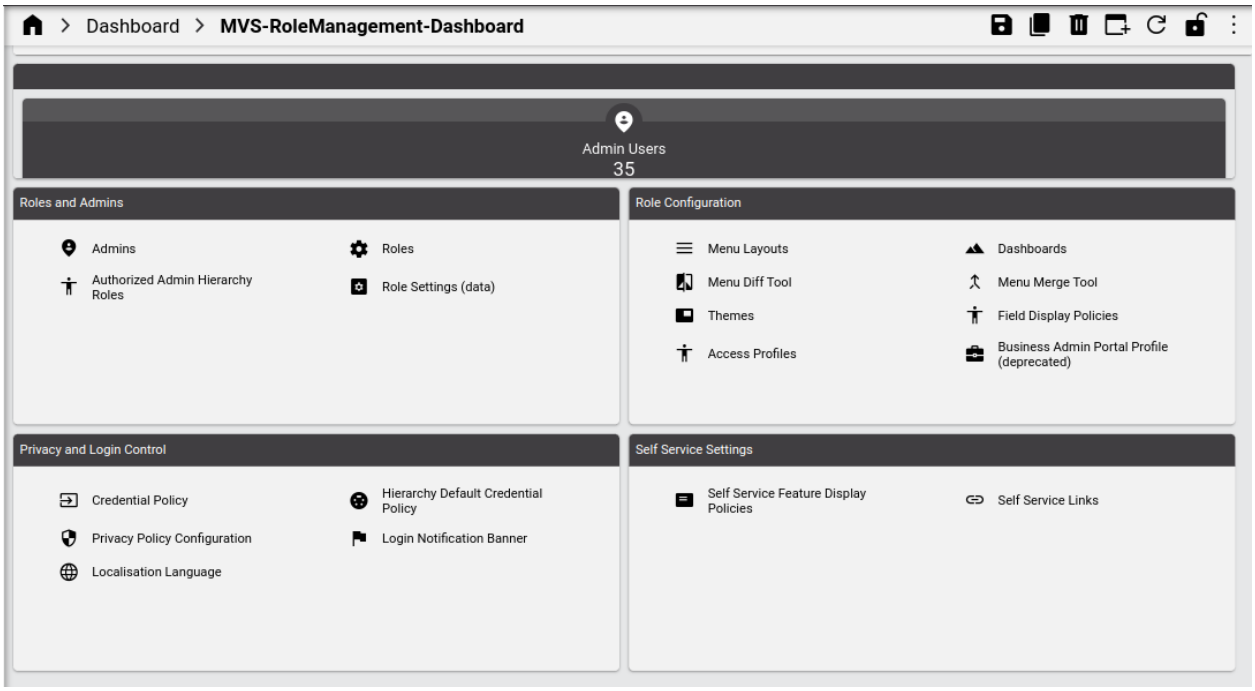
Copyright © 2025 VisionOSS Limited. All rights reserved.

- `MVS-OperationsCustomerMenu`

These menu layouts offer a number of benefits, for example:

- A compact main menu list
- Menu items directing users to dashboards consisting of items that can be selected to carry out a task - grouped into cards and all visible on one page

The comprehensive set of sample dashboards is provided and used in these menu layouts. They are identified by the dashboard name with prefix, `MVS-`, and suffix, `-Dashboard`. For example, the **Role Management** dashboard is `MVS-RoleManagement-Dashboard`.



Note:

- In release 21.4-PB3, the landing page `MVS-GroupingServices-LP` has been updated with a filter to exclude the listing of “user” Call Handlers. If this landing page is in use or previously customized, an updated customization of `MVS-GroupingServices-Dashboard` is required to enable this change in release 24.1.

This also includes home dashboards:

- `MVS-EnhancedProviderAdmin-HomeDashboard`
- `MVS-Operations-CustomerAdmin-Home-Dashboard`

These dashboards can therefore also be cloned and customized as required.

Access profiles associated with these menu layouts and dashboards can also be cloned and configured according to the customized menu layouts and dashboards. They contain the prefix:

- `MVS-EnhancedProviderAdminAP`
- `MVS-OperationsCustomerAdminAP`

The **Condition** field in menu layouts and dashboard widgets can be configured for multi vendors by using the macros as conditional values - as per enabled features in **Global Settings**:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `{{ macro.is_microsoft_enabled }}`
- `{{ macro.is_cisco_cucm_enabled }}`

Sample administrator roles are provided that combine all these elements:

- `MVS-EnhancedProviderAdministrator`
- `MVS-EnhancedCustomerAdministrator`

Add or edit a menu layout

This procedure adds new menus and modifies existing menus. You can create a new layout for your system or update the default menu layout.

1. Log in to the Admin Portal as a Provider or Reseller administrator (or higher).
2. Choose the hierarchy for the new menu layout, for example, Customer.
3. Go to **Menu Layouts**.
4. Choose an option:

Create a new menu layout, based on settings in an existing menu layout	Recommended method. Click on the menu layout you wish to copy. On the menu layout editing screen, click the toolbar **Clone** icon. A new record is created with pre-populated settings. Go to the next step to edit settings for the clone to create a new, custom menu layout.
Create a new menu layout as a new record (without existing settings)	Click the toolbar Plus icon (+) to open the **Menu Layouts/New Record** page. Go to the next step to set up the new menu layout.
Edit an existing menu layout	Click on the menu layout you wish to edit, update its settings, then save your changes. Log out, then log in again to see your changes.

Note:

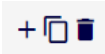
- You can click in a row to edit a value (either type in the field or select an option from a drop-down)
- Rows with nested menu items or links contain a chevron (>) instead of a Plus icon (+) so that you can see which items have child lists.
- An asterisk indicates required values.
- For further details around menu configuration, see *Menu layout settings*.

5. At **Menu Items**, configure the main menus and sub-menus, as required
   - To re-order menus, click on the hamburger icon and drag items to the required position.
   - To add, clone, or delete rows for main menus and nested sub-menus, click the **Plus** icon, **Clone** icon, or **Delete** icon in the relevant row.

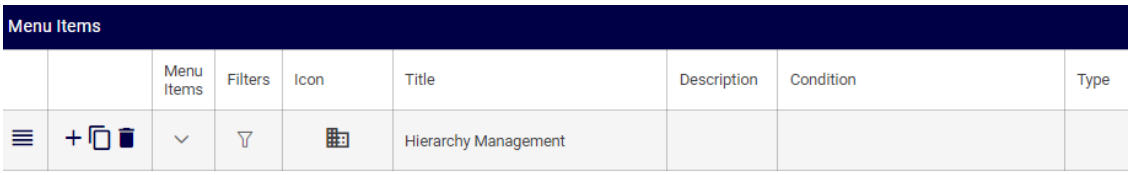
     Note: Clicking the **Delete** icon in a row triggers a system message asking you to confirm that you want to remove the row. This allows you to review the change in case you clicked the **Delete**

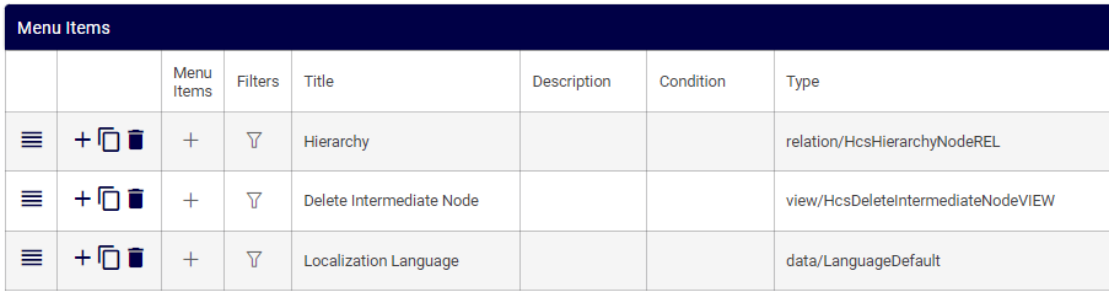
Copyright © 2025 VisionOSS Limited. All rights reserved.

icon by mistake. Clicking the toolbar **Save** icon saves all changes to the menu layout you're configuring.

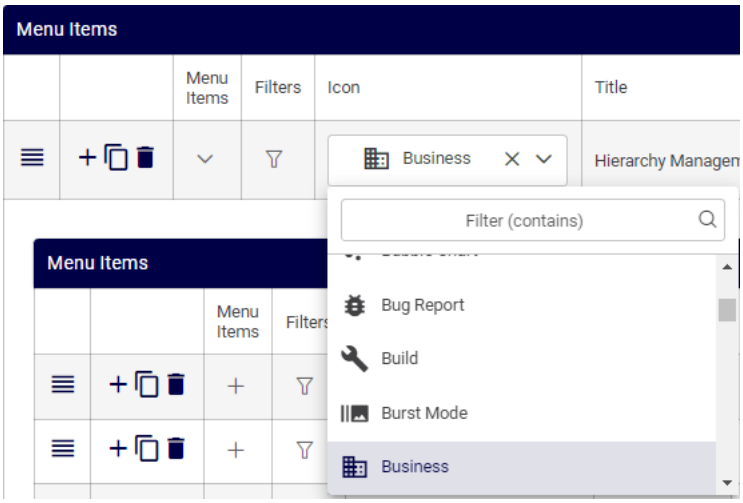


- Add, clone, or delete sub-menus (click the Plus icon in the **Menu Items** column to display nested sub-menus).





- At **Filters**, configure fixed and configurable filters.
- At **Icon**, choose a menu icon (main menus only). See: *Custom icon names reference*.



- At **Title**, add or edit the menu title, and (optionally), provide a description.
- At **Condition** (optionally), fill out a condition to define when the menu will display.
- At **Display As**, choose an option to define how the menu or sub-menu will display. Options are: Form, List, External Link, or Dashboard.

Note:

- The value for **Display As** must be **Form** when the value at **Model Type** is `view`.
- The value for **Display As** must be **Dashboard** if you're choosing a dashboard.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- At **Type**, choose the model type.

  Note: When type is `view` (`view/ModelType`), the value in the **Display As** column must be **Form**.

- At **Href**, create internal or external links.

  Note:

  – If **Display As** is set to **External Link**, the **Href** value should start with `http`.

  – If **Display As** is set to **List**, the internal **Href** value should start with `/api/`.

  – If you wish to provide a *sorted list view* of a model in a menu item, the **Href** internal href value can be entered with additional parameters to specify attribute and sort order. In this case, **Display As** should be selected as **List**, with the `direction` parameter to sort.

    For example, if **Href** is:

    ```
    /api/data/Countries/?order_by=iso_country_code;direction=desc
    ```

    the list view from the menu item of `data/Countries` will be sorted in descending order, by `iso_country_code`: `ZIM, ZAF, VNM, USA, UKR,...` and so on.

- At **Field Display Policy**, choose a field display policy, if required.
- At **Configuration Template**, choose a configuration template, if required.
- Select **Set as default Model Type** to define that when a user navigates to a form for that model from a location where any of the FDP, CFT, and title is not available, then the form will contain these elements configured as the default.

  Note: If no default is set, or multiple defaults are set for FDP and CFT selection, the selection is random. Multiple defaults will also yield an error message in the browser console if the Browser Console Log Level is set to Debug (see: *Guide to the Admin Portal user interface*) The format of the message is:

  ```
  Multiple defaults configured for ... <model-type>
  ```

  It is therefore advisable to explicitly set the default and ensure that only one default is set.

- At **Dashboard**, you can instead choose an existing dashboard to associate with the menu item.

  Note:

  – You can choose a dashboard for a main menu, sub-menu, or sub-sub-menu.

  – When setting a dashboard, the value in the **Display As** column must be **Dashboard**.

6. Click **Save**. Updated or new menu layouts are saved.
7. Assign the menu layout to the appropriate roles.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Menu layout settings

This section describes menu layout configuration options:

Note: You can view, add, and edit menu layouts in the Admin Portal via the **Menu Layouts** page. See *Add or edit a menu layout*

Field	Description
Name	Mandatory. The menu layout name.
Description	A description of the menu layout.
Menu Items	This section displays the menus and sub-menus in an editable table layout.

Menu items

The table describes configuration options the **Menu Items** rows on the Menu Layouts page:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Reorder	Click on the reorder icon (hamburger) in the relevant row to change the location of a menu.
Add, clone, or delete row	Click an icon to either add a row, clone (copy) a row, or to delete the row. Clicking the **Delete** icon in a row triggers a system message asking you to confirm that you want to remove the row. This allows you to review the change in case you clicked the **Delete** icon by mistake. Clicking the toolbar **Save** icon saves all changes to the menu layout you're configuring.
Menu Items	Click the Plus icon to expand nested menus. Click the chevron to collapse expanded menus.
Filters	Click the filter icon in the relevant row to display a dialog where you can choose fixed and configurable filters for a menu item. Fixed filters cannot be removed. The following options are available for configurable filters: • Filter By • Filter Type • Filter String
Icon	The icon to use for the menu item. Click in the cell to choose an icon. Icons display in the drop-down with a descriptive name.
Title	Click in the cell to add or edit the name (title) of a menu item.
Description	Click in the cell to add or edit the menu description.
Condition	Click in the cell to add or edit a macro that allows you to display/hide a menu and its sub-menus, based on a condition specified in the macro. If the macro evaluates to true, the menus and sub-menus display, else, when false, the menu and its sub-menus are hidden. The default is true (menus and sub-menus you add on this page display by default). See the Advanced Configuration Guide for more information about using macros.
Type	Click in the cell and choose a model type (for example, relation or view) to associate with the menu item. When type is `view` (`view/ModelType`), the value for **Display As** must be **Form**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Href	Click in the cell to specify a path as a direct reference to a model type used for the menu item. Links can be external or internal. Hrefs are generally recommended for external links. For backwards compatibility, hrefs can be used for links within the application, to link directly to a form. For example, the Add Phone page would have the following href value: *api/relation/SubscriberPhone/add* In this case, you will need to use JSON format menu import, or bulk load, to add any associated FDPs (field display policies) and CFTs (configuration templates) for the menu item. It is recommended that you do not use hrefs to reference *view/* type models.
Field Display Policy	Click in the cell to choose a FDP (field display policy) to associate with the menu.
Configuration Template	Click in the cell to choose a CFT (configuration template) to associate with the menu.
Set as default Model Type	If selected, the FDP, CFT and title is taken as default when navigating to this model from outside the menu.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Dashboard	Choose the dashbaord to display when clicking on a menu. Mandatory when the value for **Display As** is **Dashboard**. Sub-menus and sub-sub-menus can be selected as dashboards. Individual dashboards do not have their own specific context-sensitive help.
Display As	Defines how the menu item displays. Options are: List, Dashboard, Form, External Link, Tree • List (default) For two or more instances. If you choose List, and you've selected a default FDP and CFT for the model type, users with a user role associated with the menu layout view the model type based on these options. It is also possible to filter the list view. If you choose List display referenced by type or href, note that a tool (`tool/[toolname]`) can also be presented as a list, for example: `/api/tool/Transaction/?entity=data/Event&operation=execute` • Dashboard When **Display As** is dashboard, you must choose the dashboard to display when a user clicks on the menu item. • **Form** (for a single instance) If you're using href and you choose the Form display, the href value points to a model instance with the pkid, for example `data/Countries/5331a739d0278d7893e26d2e`, or ends with `/add/`. The value for **Display As** must be Form when the value for **Type** is `view`. The `view/` model types always open the *Add* form; thus, if used, the value should not have the `/add/` endpoint, for example, as in this JSON: `{ "type": "view/QuickSubscriber", "display": "form", "title": "Quick Add Subscriber" }` • External Link Href is required if the value for **Display As** is External Link. A URL specified as the href value opens as a new browser tab. You'll need to disable pop-up blocking on the users browsers to allow the external link to resolve. • Tree (if available, for two or more instances) Choosing a Tree display shows a tree view of the resource. When using href with Tree display, the href provides the tree path.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Custom icon names reference

This reference refers to the icons associated with the **Icon** name drop-downs in the interface.

For details, see: https://fonts.google.com/icons

To associate the icon of the in the drop-down, inspect the icon titles on the website, remove the title hyphens and capitalize the first letter of each word.

Related Topics

- *Fixed and configurable filters in menus*
- *Introduction to Automate dashboards*

Fixed and configurable filters in menus

Overview

Automate allows you to apply fixed filters and configurable filters on menu layouts.

- *Fixed filters*
- *Configurable filters*

For the use of fixed filters and configurable filters on **Links** widgets on dashboards, see the *Links* topic at *Introduction to Automate dashboards*.

Fixed filters

Only high-level administrators can add and modify pre-defined **Fixed Filters** to menus. For these administrators, this option also shows on the Menu Layout design input forms and presents the same interface options as configurable filters.

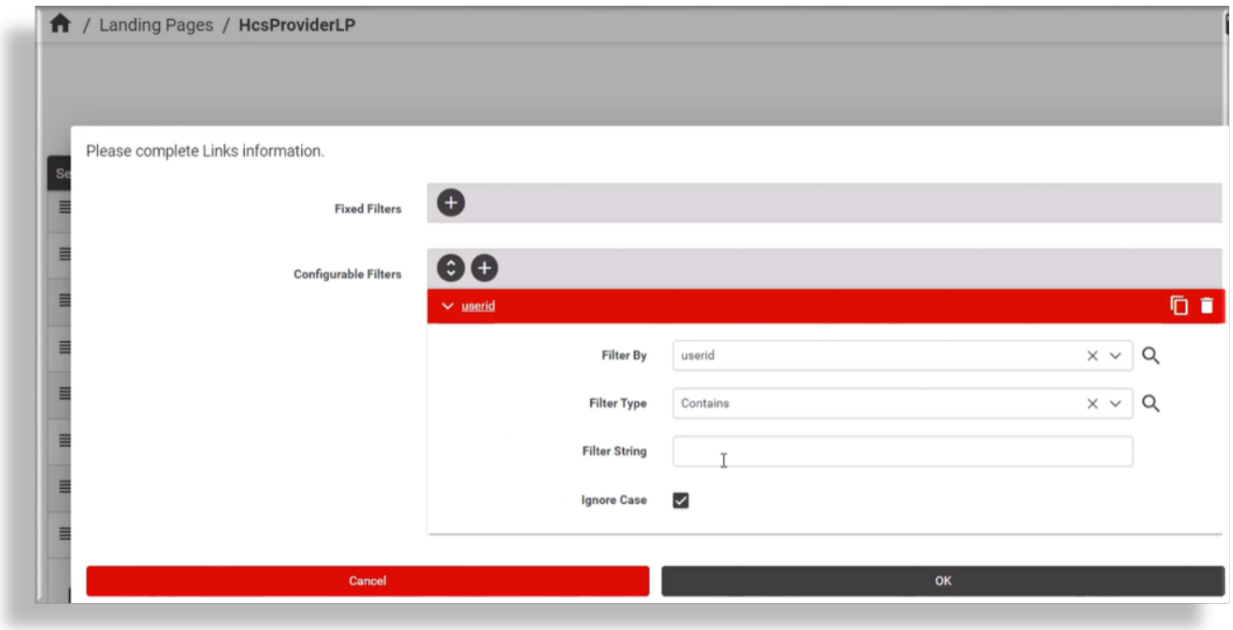
These filters are not visible to the lower level administrators and will *always* apply when the menu item link is used by them. Fixed filter results can however be filtered further by Configurable Filters.

Configurable filters

When configuring a menu layout, click the icon in the **Filters** column to open the filter configuration dialog, where you can add one or more configurable filters.

Adding more than one filter results in a logical AND of the filter application.

Copyright © 2025 VisionOSS Limited. All rights reserved.



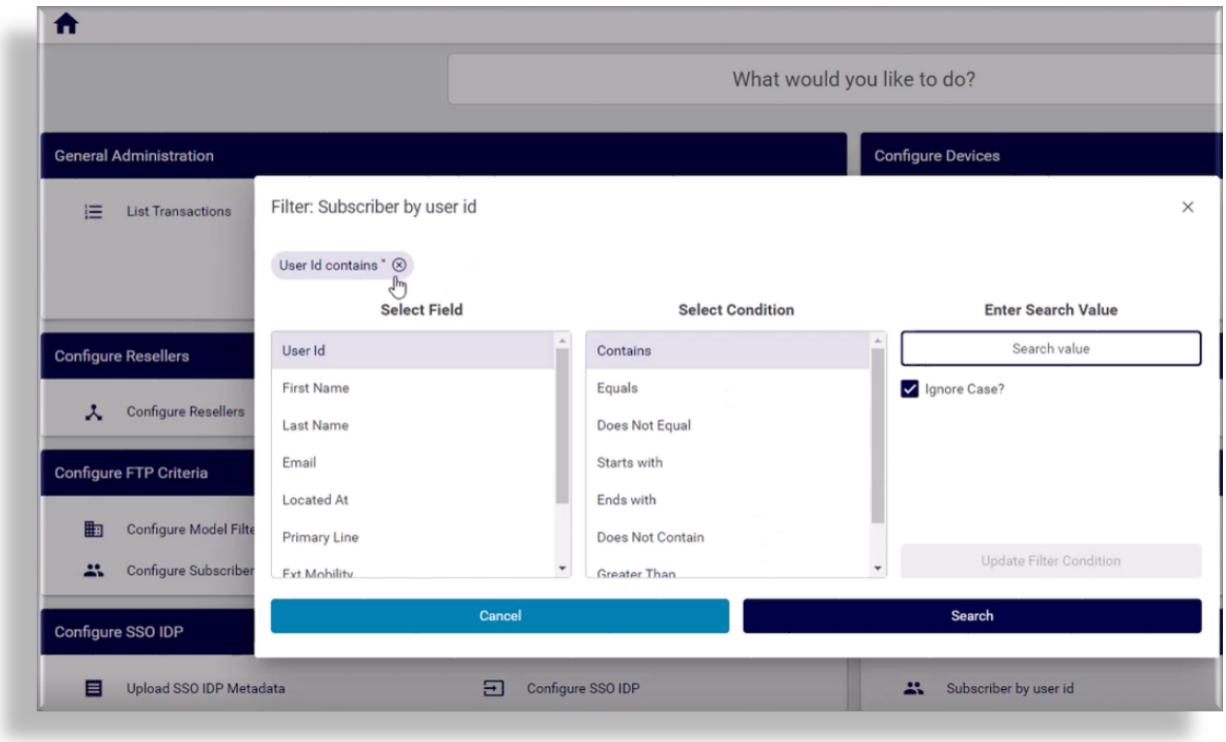
The table describes the **Configurable Filters** fields:

Filter By	Attributes of the selected Type can be selected from the drop-down list.
Filter Type	Select the matching operator to apply when the attribute is matched to the **Filter String** value: • Contains • Does Not Contain • Starts With • Ends With • Equals • Not Equal
Filter String	Select the value that the matching operator should match by.
Ignore Case	This checkbox defines whether to ignore the case of the **Filter String** value.

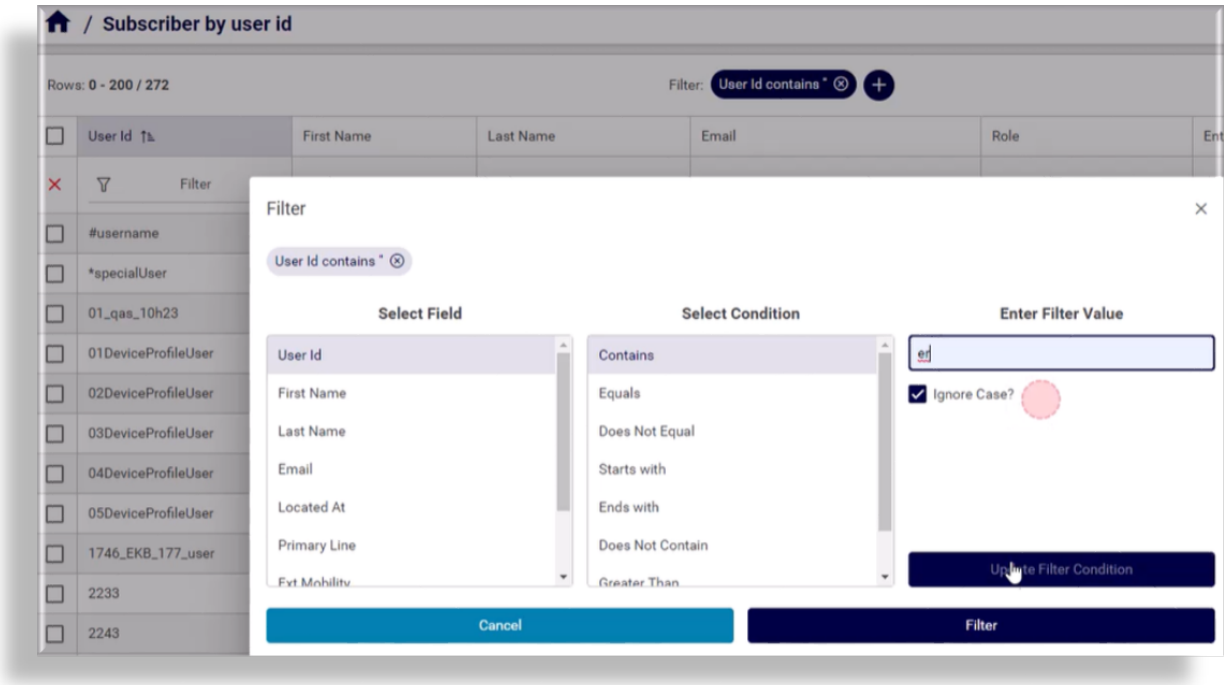
Once you've applied the configurable filters, selecting the menu item in the GUI triggers a pop up **Filter** dialog before rendering the list view, where you can apply or modify the filter before displaying the page related to the or menu.

If a **Filter String** value is entered on **Configurable Filters**, this value can also then be accepted or modified in the **Filter** dialog.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The list view of the results footer row indicates that a filter has now been applied to the list and this filter can then be further modified and removed from the list view as usual. See *Working with lists*



Copyright © 2025 VisionOSS Limited. All rights reserved.

Important: Standard list view filters on model types (for example if accessible by other menu items) can still be used as described in “Filtering Lists”, but these will be removed and replaced by any configurable filters on menu items for the corresponding model type.

5.5.3. Field Display Policies

Field display policies

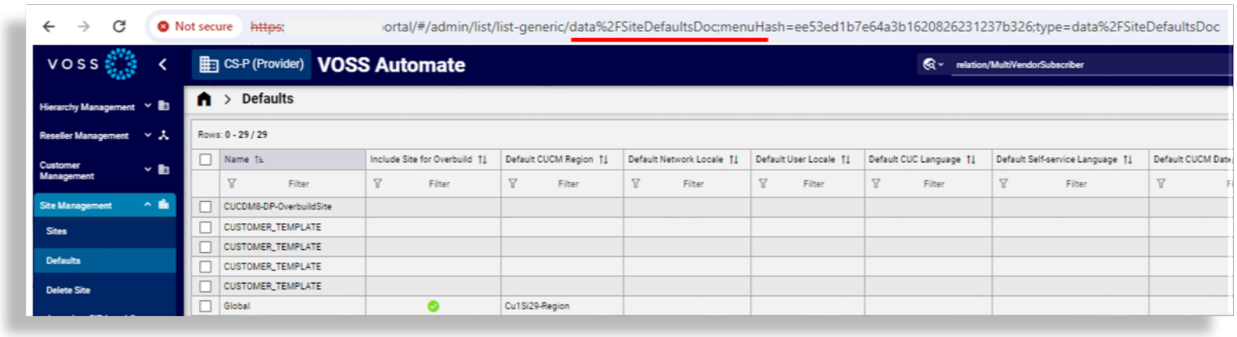
Tip: *Use the Action search to navigate Automate*

Overview

Field display policies (FDPs) define the layout and composition of fields, fieldsets, and groups on forms in the Automate Admin Portal GUI. To change these elements on the form, you can edit the FDP associated with the form, if allowed.

Note: FDPs are assigned to the model associated with a form or page in the GUI. FDPs can be added to Data models, Relations, and Views. For example, *data/SiteDefaultsDoc* is the model associated with the summary list view page and with the edit form for the site defaults.

If you want to change the layout of the form, you can edit the FDP for this model, if allowed. The layout of forms associated with some models cannot be modified via their FDP, for example, for `relation/LineRelation`, `relation/SubscriberPhone`, `tool/Transaction`, or `view/BulkAddUser`.



Via the FDP, you can define whether to group or disable fields, add online help text to a field, add a label to a field, or move a field up or down on the form.

You can apply one or more FDPs to a particular item type to present different views of the same form. You can apply a FDP for a menu layout and role so that users with this role are presented with a view of the form (defined by the FDP) for their user role when they log in. For example, a system may have users at Provider, Customer, and Site administration hierarchy levels - all of whom may access the same items, but perhaps some item fields need to be hidden for admin users at some levels. Therefore, you can create and apply a specific FDP to a menu layout designed for admin users at these levels.

Copyright © 2025 VisionOSS Limited. All rights reserved.

You can clone an existing FDP to quickly create one, then modify the clone as required, and choose this new FDP for the model on a user's menu layout. In this way, the user's view of the GUI can be modified for their level of access to the model, from the menu.

Note: The list view column header will also show the field title from the FDP if the field belongs to the list of summary attributes.

Field display policy naming convention

The name of a FDP must be unique at each hierarchy. You can however have FDPs with the same name at different hierarchies.

FDPs that have the name `default` will apply to their associated model, by default.

Display groups as tabs or panels

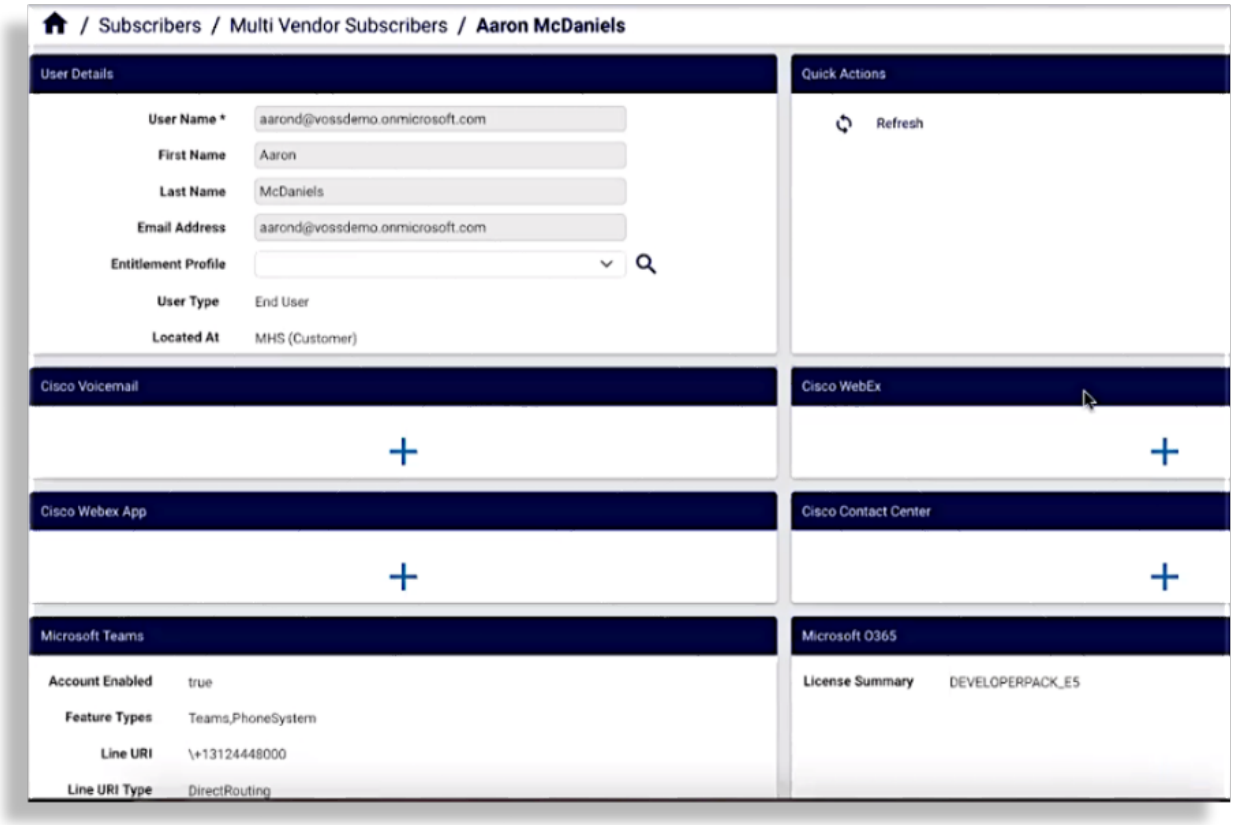
The **Field Display Policy** configuration screen provides a **Display As Groups** setting that allows you to define the default layout of some forms, as either tabs or panels.

Tabs	Each group of fields and/or fieldsets displays on a tab. The group title is the tab title.
Panels	Each group of fields and/or fieldsets displays as a panel in a 2-column list of panels on the GUI. The group name is the panel header.

Note: If no option is selected, the default is **Panels**, except for some models, which display groups as tabs by default. On some forms, depending on your user type and the model where the FDP is applied, you can click a toolbar icon in the GUI (or select from the action overflow menu) to switch between a panel or tab layout. The layout you choose is preserved when you log out and log in again.

The image shows an example of a form where groups display as *Panels*:

Copyright © 2025 VisionOSS Limited. All rights reserved.



The Automate system default is *Panels*, except for the following models, which have as their default setting, *Tabs*:

- `view/GlobalSettings`
- `data/SiteDefaultsDoc`
- `data/ucprep_UC_Profiles`
- `relation/DP_REL`
- `data/HcsDpDialPlanSchemaDAT`
- `data/HcsDpDialPlanSchemaGroupDAT`
- `tool/BulkLoad`
- `tool/DataImport`

The table lists models where the layout of elements of add and/or edit form types can't be modified via FDP. These form types also do not have the action element available on the GUI to switch the form view between tabs and panels.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Model Name	Form Type	Default
`relation/LineRelation`	edit	Panels
`relation/MultiVendorSubscriber`	edit	Panels
`relation/PexipConference`	add, edit	Panels
`relation/SubscriberDeviceProfile`	add, edit	Panels
`relation/SubscriberPhone`	edit	Panels
`tool/Macro`	add	
`tool/Transaction`	edit	
`view/AddSubscriberFromProfile`	add	
`view/BulkAddUser`	add	
`view/HcsVersionVIEW`	add	
`view/MenuDiff`	add	

Related topics

- Field display policy settings in the Advanced Configuration Guide
- Introduction to the Admin Portal User Interface in the Core Feature Guide

Add and edit field display policies

This procedure adds and edits a field display policy (FDP).

1. Log in as Provider administrator or higher.
2. Choose the relevant hierarchy.
3. Go to **Field Display Policies** to view the list of existing FDPs.
4. **Do you want to . . .**
   - **Edit an existing FDP**? Click on the relevant FDP in the list view to open the configuration form. Update the FDP as required, then save your changes.
   - **Add a new FDP**? Go to step 5.
5. To add a new FDP, from the list view, click the toolbar Plus icon (+) to open the configuration form for the new FDP you're adding.
6. Configure the FDP:
   a. Fill out a name for the new FDP, and optionally, a description.
      - If the FDP name is `default`, it is applied by default to the target model type you choose on the form.
      - FDPs at the same hierarchy must have a unique name. FDPs at different hierarchies can share the same name.

   b. Choose the target model type to associate with the FDP.

      Note: The target model type defines the fields available for use in the FDP.

Copyright © 2025 VisionOSS Limited. All rights reserved.

c. At **Display Groups As**, choose how groups should display on forms. Options are Tabs or Panels.

Note: The default is **Panels**, except for a selection of models, where the default is **Tabs**. Within a tab or a panel, you can add a combination of fields and/or fieldsets (within one or more groups).

---

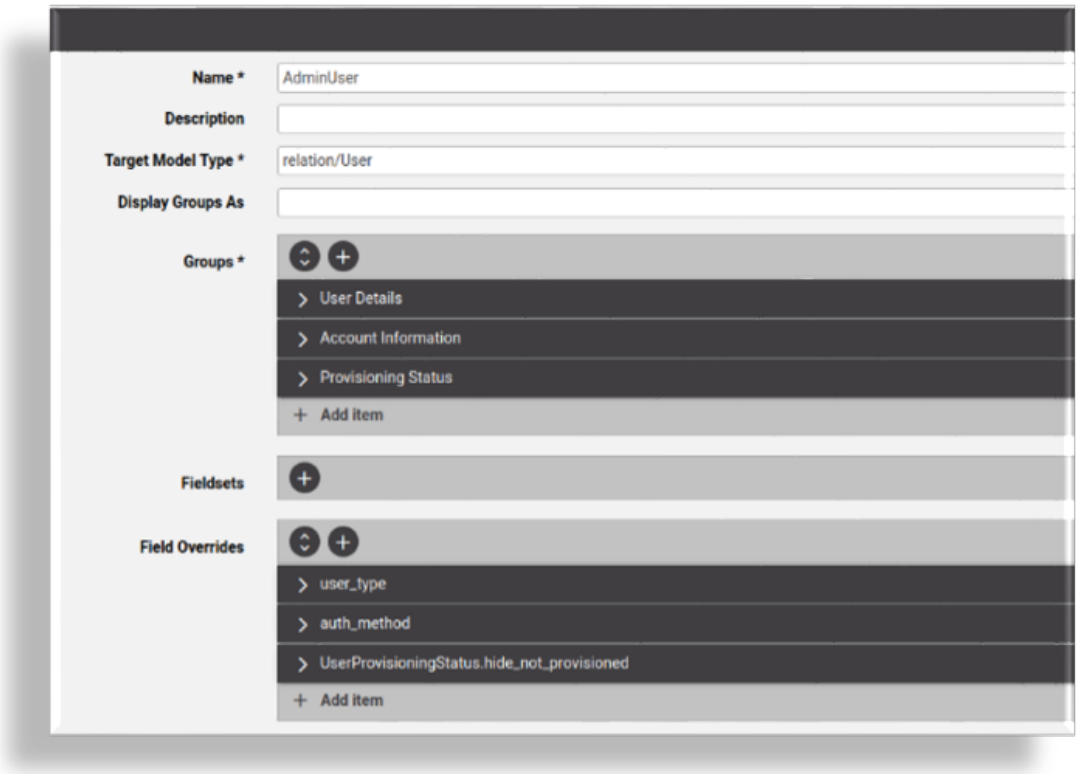
d. Add groups, one or more, required:

At **Groups**, click the Plus icon (+), then configure the group.

Note: Groups that describe a collection of attributes display together on the GUI. All fields in the FDP must belong to a group.

At the form level, groups all display either in panels or tabs, depending on the option selected in **Display Groups As**, and provided the model allows the option you choose.

You can copy or re-order (move up or down) groups, fields, and fieldsets.



The table describes the group configuration options:

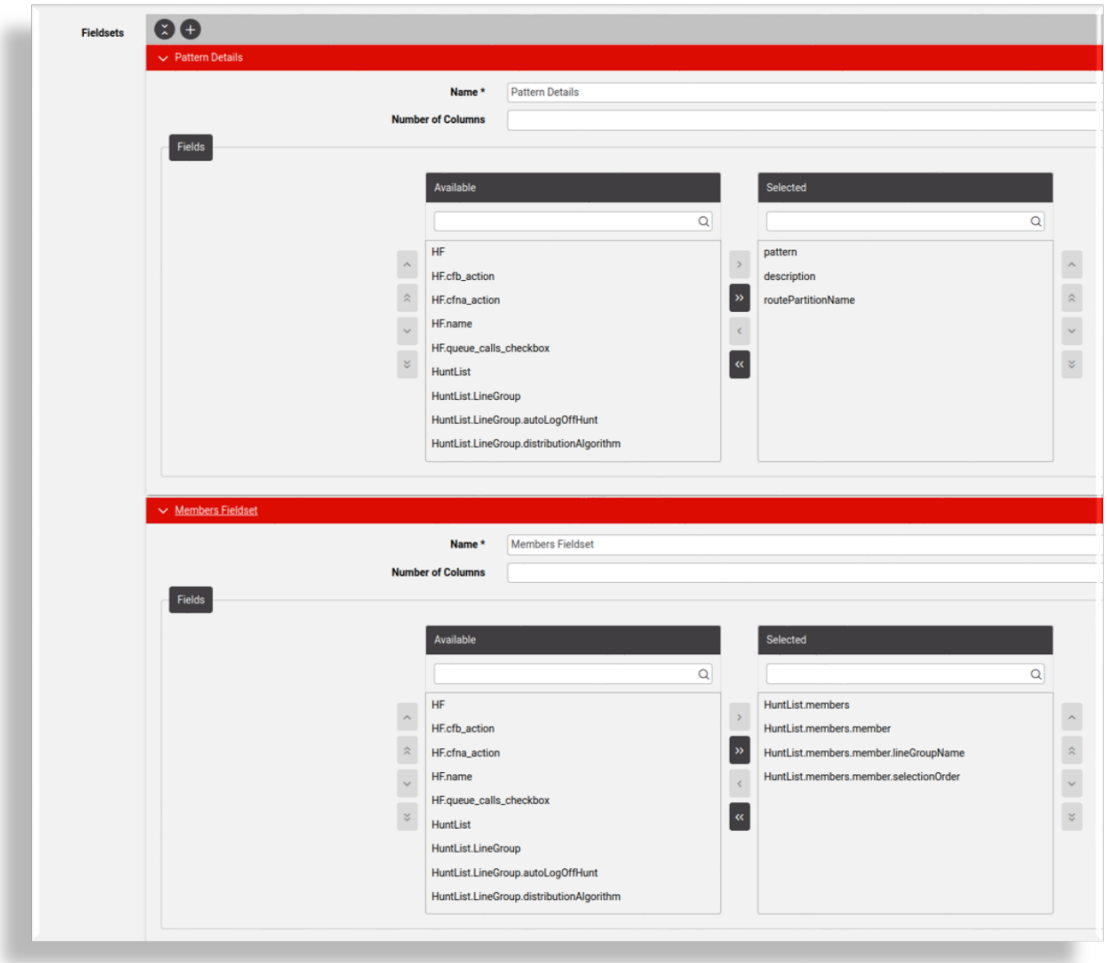
Copyright © 2025 VisionOSS Limited. All rights reserved.

Component	Description
Title	Mandatory. Fill out label text to display for the attribute on the new tab. If a group displays as a tab in the Admin Portal, the value defined for **Title** displays as the title of the tab.
Number of Columns	Fill out the number of columns for fields. The default is *1* (a single column). Fields in the **Selected** transfer box display in these columns.
Fields	Choose fields to add. Select then move fields from the **Available** field to the **Selected** field. The selected target model type defines the available fields. Use the **Move Up**/**Move Down** buttons to adjust the position of any field.

e. Add fieldsets, if required. Click the Plus icon (+) at **Fieldsets**, then configure the fieldset.

Note: Fieldset options (fields in the Available transfer box) show all field choices for the selected target model type. Fieldset names are added as choices within any group added to the FDP, and the fields display as a group in fieldsets in the panels.

The **Name** field is the name of the fieldset. First create fieldset, then add it to a group.



Copyright © 2025 VisionOSS Limited. All rights reserved.

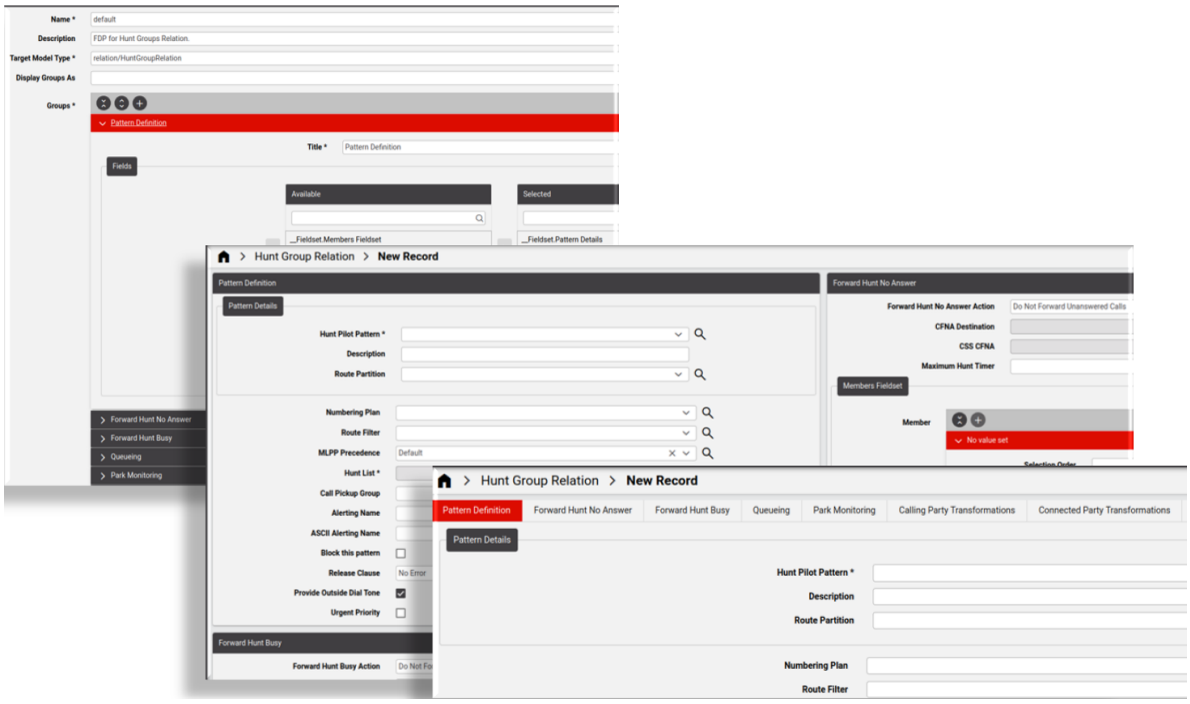
f. Add field overrides, if required. Click the Plus icon (+) at **Field Overrides**, then configure the field override.

The table describes configuration options for field overrides:

Component	Description
Field	Name of the model field to override. Options include those added to the **Selected** field for groups.
Title	New title to display for the field. If the FDP is called `default` at a hierarchy, the list view column header also displays this title if the field belongs to the list of summary attributes.
Help Text	New help text to display for the field. Leave blank to use the model attribute description.
Disabled	Sets the field as *read-only*.
Input Type	Overrides the input type of the field. Select an option to choose how the input field displays, for example, radio button, grid, multi select.

7. Click **Save**.

Once saved, the FDP can be applied by selecting it in a menu layout available to a role.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Clone a field display policy

This procedure creates a copy, or clone, of an existing field display policy (FDP) to create a new FDP, starting with the configuration of the FDP you're cloning.

1. Login as Provider administrator or higher.
2. Choose the hierarchy.
3. Go to **Field Display Policies** to view a summary list of existing field display policies (FDPs).
4. Click on the FDP you want to clone.
5. Choose **Actions** > **Clone**.
6. Update the necessary fields for the cloned FDP.
7. Click **Save**.

   You can apply the cloned FDP by choosing it in a menu layout available to a role.

Rules for creating field display policies

When creating groups and selecting the field transfer boxes of a group, a number of rules apply.

Note: Regarding notation, if the fields belong to objects or arrays, the names in the transfer boxes are shown in dot notation. Refer to the target model type on-line help field reference to distinguish object types from array types.

To understand the rules, consider a selected Target Model Type with the fields as listed below. Where the name starts with "A", the field is an array and where it starts with an "O" it is an object. The values "x", "y", "z" are also objects. The field "F" is neither object or array.

- A, A.x, A.x.b, A.x.c, A.x.d, A.y.r, A.y.s, A.y.t
- F
- O, O.v, O.z, O.z.a, O.z.b, O.w.d

Inclusion rules

The following inclusion rules apply:

- If a parent object or array field is included, the parent and all its children will be displayed in the GUI.

  Example: if O.z is selected, O.z is saved as the fields and the GUI will display O.z and also inner fields O.z.a and O.z.b.
- If a specific selection and order of child elements are required, select these child elements and order them.

  Example: if O.w.d, O.z.b, F are selected, these three fields are saved in that order in the FDP group fields and the GUI shows only the inner field O.w.d, followed by the inner field O.z.b and lastly the field F.
- Inclusion of child fields in a group without the inclusion of the parent fields will display these child fields at the root level of the form.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Example: if O.w.d, O.z.b are selected, these fields are saved as is in the FDP group fields list and only the inner fields O.w.d and O.w.b are shown in the GUI.

- Array children fields without their parent fields will be ignored by the GUI. Therefore, if the child fields of an array field are selected, the parent field should also be selected.

  Example: if A.y.s, A.y.t are selected, A and A.y should be selected.

- Array fields may not be split into different groups.
- The parents of fields cannot be in one group and its children in another.

  Example: O.z cannot be in Group 1 if O.z.a, O.z.b and O.w.d are in Group 2.

- Fields of the same object and members of the same array type cannot belong to more than one group.

  Example:

  - If A.y.s is selected for Group 1, then A.y.t cannot be selected for Group 2.
  - If O.z.a is selected for Group 1, then O.z.b cannot be selected for Group 2

- You can split the first level children of object fields into different groups.

  Example:

  - O.v can be in Group 1 while O.z is in Group 2.
  - For second level children: O.z.a can be in Group 1 and O.w.d can be in Group 2.

- To hide a field do not move it to a Selected box.

  Example: To hide O.z.b, select O.z.a, O.w.d.

Ordering fields in a field display policy

You can move fields or fieldsets in a group (up or down on the form) by clicking the **Move Up** / **Move Down** buttons at the group level or in the transfer boxes.

Ordering child and parent fields depends on the presence of siblings, other parents, and children. If a child is selected in a group and not its parent, but a sibling of that parent is selected, then the sibling's order will affect the order of the fields.

The logic of order resolution starts from parents to children, according to the rules below.

For example, we select fields in this order in Group 1:

C.z, A.x.b, A.x.c, B, A.y, A.x, C, C.w

Result:

- Parent fields on their own are considered first, hence our initial order is B, C.
- However, parent A is not selected; only the children. We determine where A was mentioned. In this case the children of parent field A were mentioned before the parent fields B or C. Hence children of A will eventually be ordered before B and C.
- Next we consider the selected first level child fields: C.z, A.y, A.x, C.w. The order becomes: A.y, A.x, B, C, C.z, C.w
- We now move down the levels: A.x.b, A.x.c.

Thus the final display order will be:

A.y, A.x, A.x.b, A.x.c, B, C.z, C.w

Copyright © 2025 VisionOSS Limited. All rights reserved.

Further examples below illustrate the presence of parents, siblings and children on the selected order.

- We add fields C.w, A, C, B, A.x, A.y.

  Result: The order is: A, A.x, A.y, C, C.w, B.

- We add fields A.x.b, A.x.c, A.y, A, B

  Result: The order is: A, A.x, A.x.b, A.x.c, A.y, B.

  Note: Note that A.x was added and that A.y is placed after A.x, since the children were ordered before A.y while A.x was never selected.

5.5.4. Themes

Introduction to themes

Tip: *Use the Action search to navigate Automate*

Overview

Themes allow you to configure the look and feel of the entire user interface, including images, logos, colors, fonts, sizing, and positioning. Themes can also be used to manage the login and interface header text, and the theme you choose can be applied to the Login page.

You can add any number of new themes, and edit existing themes. Automate ships with a default theme, which can be used as a baseline template.

Themes are associated with user roles, and are typically associated with a specific customer (company).

Related topics

- Less files and customizing themes in the Advanced Configuration Guide
- Create a theme in the Admin portal in the Core Feature Guide

Managing themes

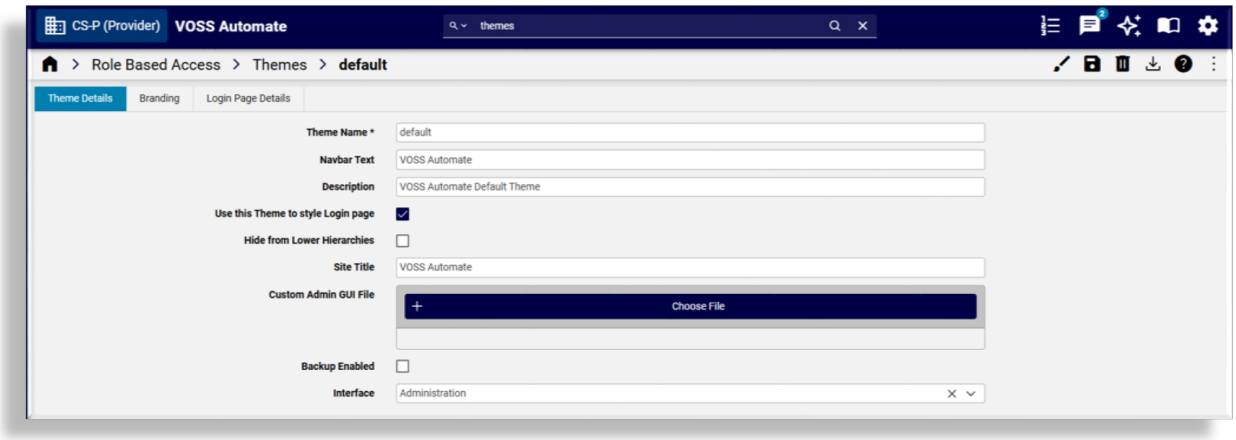
There are two ways to manage themes in the Admin Portal:

File-based themes (Less files)	If you're using a file-based theme, this takes precedence. This is a CSS file that may be added, downloaded/exported, edited, and re-imported, to apply a theme. For more information, see *Less Files and Customizing Themes* in the Advanced Configuration Guide.
Custom branding options	Configured directly within the GUI

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: File-based themes are not used for the Admin Portal.

To access theme management functionality in the Automate Admin Portal, go to the **Themes** page.



Securing themes

When importing a file-based theme to Automate at a particular hierarchy, you can choose to hide the theme from users at lower levels of the hierarchy via this setting on the Themes page: **Hide from Lower Hierarchies**.

In this case, the theme won't display in the list view for admins at lower levels of the hierarchy.

Applying a theme to the user interface

When importing or updating a file-based theme, you can choose the interface where the theme should apply, either the Admin Portal (default), or to the Self-service interface. If no interface is specified, the default applies.

In the Themes settings (via **Use this Theme to style Login page**), you can choose to apply a theme used for an interface, to also apply to the Login page across the system, for the selected interface.

Note: Currently, the system allows only a single theme to be applied to the Login page per interface. This means that a new or updated theme applied to a combination of interface and Login page for an existing theme overwrites the theme applied to the Login page style on the existing theme with the same interface setting.

The Login page theme can also be applied to the Login page when logging in. In this case, you add a suffix to the login request URL.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manage themes

Tip: *Use the Action search to navigate Automate*

Overview

You can use the **Themes** page in the Admin Portal to create or modify a theme.

You can select the following tabs on the **Themes** page in the Admin Portal:

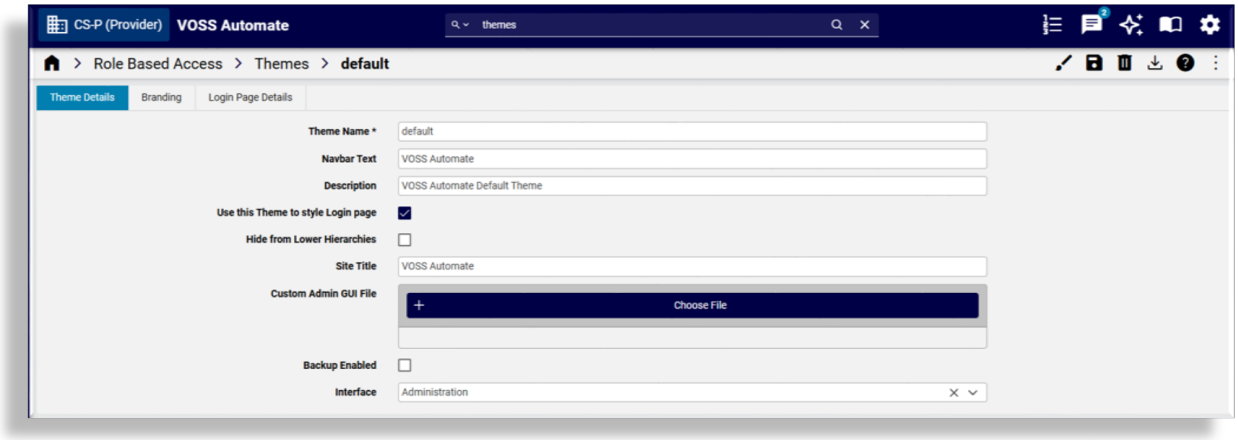
- Theme Details
- Branding
- Login Page Details

Theme settings

Theme details tab

On the **Theme Details** tab of the **Themes** page you specify theme details:

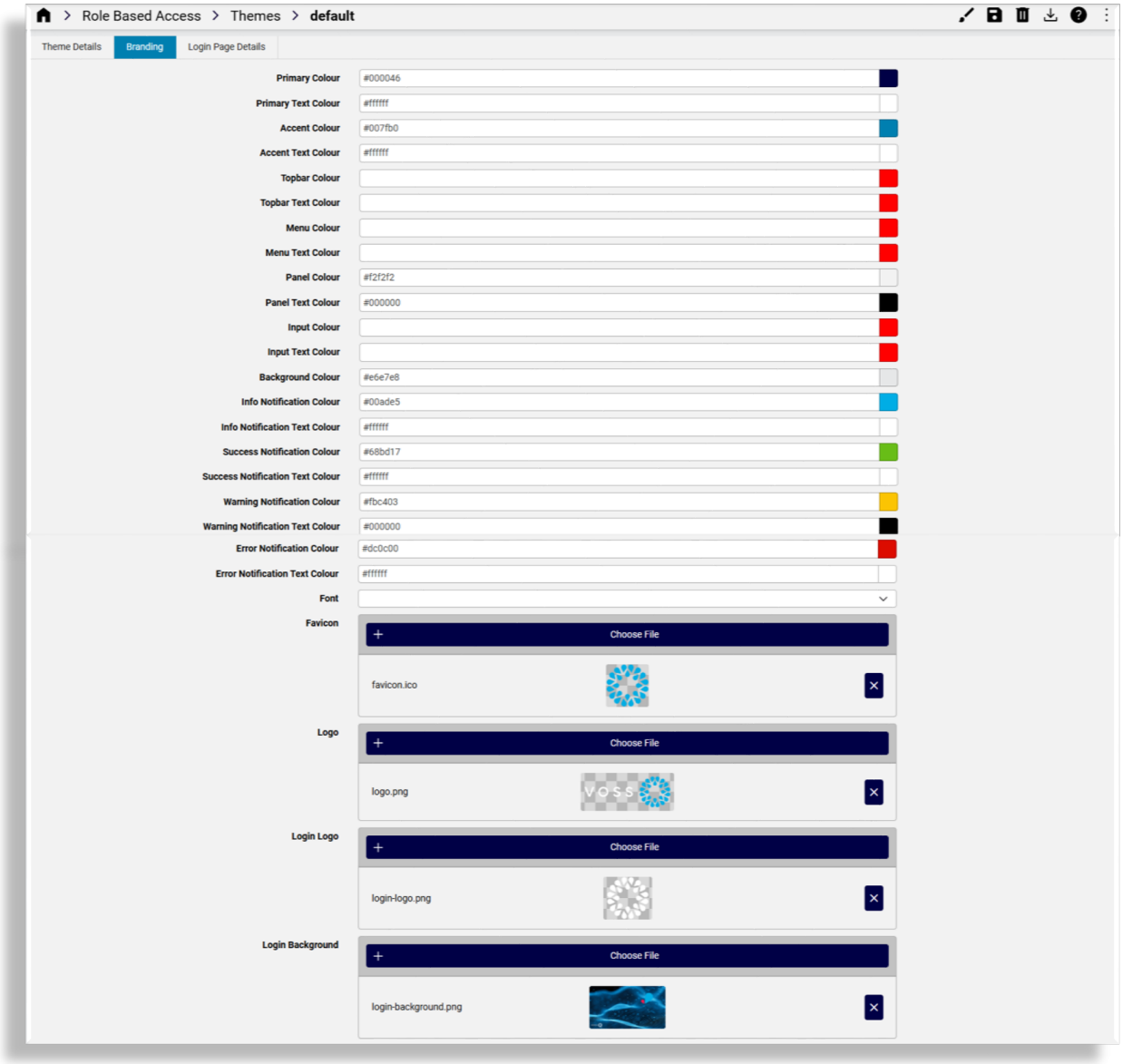
- Theme Name: Mandatory. The name of the theme. Valid characters are in the range of `a-zA-Z0-9_`.
- Navbar Text: Text to display on the navigation bar, adjacent to the organization level.
- Description
- Whether to use the theme to style the Login page.
- Whether to hide the theme from lower hierarchies.
- Site Title: The title of the site, displays on the browser tab
- Custom Admin GUI File: Upload a custom theme file, if applicable
- Whether to enable a backup of the theme (images and other custom elements)
- Interface: The interface where the theme is applied (Administration or Self-service)



Copyright © 2025 VisionOSS Limited. All rights reserved.

Branding tab

On the **Branding** tab you can customize a theme for your organization. You can change colors via the color picker or by typing in the color hex value. When no colors are chosen in this tab, the defaults apply.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Fonts

The **Font** dropdown allows for a selected font to override the global default **Roboto** font. The selected font is then applied to all text, including the login screen.

Uploading images

When uploading images for the theme:

- Note file size and *width x height* pixel dimension size restrictions. A system message displays if the image is too large.
- Only PNG files are supported for the Logo image. Other images can be PNG or JPEG.
- For image filenames, you can use the following characters and character types:

  `ALPHA / DIGIT / "-" / "." / "_" / "~"/ "#"`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Image details

- **Favicon**: The favicon for the site. Shown on the tab and when the site is bookmarked.
  - Type: PNG image or with `.ico` extension
  - Maximum dimensions: 256x256 pixels
- **Logo**: This image is used for the logo in the top left of the menu bar.
  - Type: PNG image with a transparent background
  - Maximum file size: 0.5MB
  - Maximum dimensions: 600 pixels in width and 192 pixels in height
- **Login Logo**: This image is used for the logo on the login page
  - Type: PNG image with a transparent background
  - Maximum file size: 0.5MB
  - Maximum dimensions: 600 pixels in width and 192 pixels in height
- **Login Background**: This image is used for the login screen background
  - Type: PNG or JPEG image
  - Maximum file size: 5MB
  - Maximum dimensions are 1920 pixels in width and 1080 pixels in height
- **Menu Background**: This image is used for the side menu background
  - Type: PNG or JPEG image.
  - Maximum file size: 2MB
  - Maximum dimensions: 240 pixels in width and 1040 pixels in height.

Login page details tab

The **Login Page Details** tab defines the theme for the Login page, including the title and banner text, cookie policy and privacy policy details.

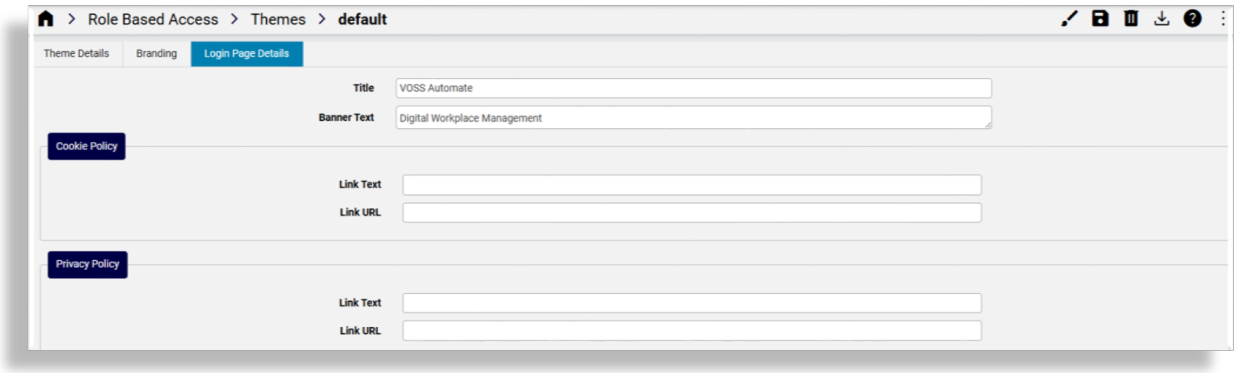
If you add banner text (limited to 2048 characters), this is used at the bottom of the Login page.

References to the cookie policy and privacy policy in the Banner Text field should be added as placeholders, which will then resolve to the **Cookie Policy** and **Privacy Policy** data entered. The placeholders are:

- `{{cookie_policy}}`
- `{{privacy_policy}}`

Note: You can add multiple lines for the banner text, including paragraphs. Banner text displays exactly as you add it to this field. Cookie and security references show as links that open in a new browser tab.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Custom themes

You can create a custom theme to change the following properties of the Admin Portal:

- Primary and accent colors
- Logo image
- Login screen background image

  If the background image also contains logos, it is recommended that these be placed on the bottom of the image.
- Background image for menu
- Browser tab title

Themes created in the Admin Portal can't be exported in full.

Preview a theme

When creating a theme, you can use the toolbar **Preview** icon (Paintbrush) to preview your theme look and feel (colors and images) before assigning it to a role and having it apply to the GUI.

Theme element color references for the Admin portal

Tip: *Use the Action search to navigate Automate*

Note:

- Color selection on the **Branding** tab of a theme *always* affects the Admin Portal.

  To edit and manage theme files:

  Refer to Less files and Theme Customization in the Advanced Configuration Guide.
- Color selection is optional. Where no colors are selected, defaults apply.
- If manual input of color Hex values is required, ensure the value is prefixed with #.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Admin portal default colors

Default color reference table:

Title	Field Name	Default Value (Hex)	Notes
Primary Color	primary_colour	#000046	This is the background color for most menus and headers, as well as the text color for links and buttons.
Primary Text Color	primary_text_colour	#ffffff	This is the text color for anything with the primary color background.
Accent Color	accent_colour	#007fb0	This color is used when attention needs to be drawn for important notifications or active buttons and text.
Accent Text Color	accent_text_colour	#ffffff	This is the text color for anything with the accent color background.
Topbar Color	topbar_colour	#000046	The color used for the top bar of the site. Will use the primary color if no value is given.
Topbar Text Color	topbar_text_colour	#ffffff	This is the text color for the top bar. Will use the primary text color if no value is given.
Menu Color	menu_colour	#000046	The color used for the menu on the left. Will use the primary color if no value is given.
Menu Text Color	menu_text_colour	#ffffff	This is the text color for the menu. Will use the primary text color if no value is given.
Panel Color	panel_colour	#f2f2f2	The color used for all the panels in the app.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Default Value (Hex)	Notes
Panel Text Color	panel_text_colour	#000000	This is the text color for normal text in the app.
Input Color	input_colour	#ffffff	The background color for input fields. Will use the panel color if no value is given.
Input Text Color	input_text_colour	#414042	The text color for input fields. Will use the panel text color if no value is given.
Background Color	background_color	#e6e7e8	The color of the background behind panels.
Info Notification Color	info_notification_colour	#00ade5	The color used for info notifications.
Info Notification Text Color	info_notification_text_colour	#ffffff	This is the text color for info notifications.
Success Notification Color	success_notification_colour	#68bd17	The color used for success notifications.
Success Notification Text Color	success_notification_text_colou	#ffffff	This is the text color for success notifications.
Warning Notification Color	warn_notification_colour	#fbc403	The color used for warning notifications.
Warning Notification Text Color	warn_notification_text_colou	#000000	This is the text color for warning notifications.
Error Notification Color	error_notification_colour	#dc0c00	The color used for error notifications.
Error Notification Text Color	error_notification_text_colour	#ffffff	This is the text color for error notifications.

On the Admin portal, consider the color selection on the **Branding** tab:

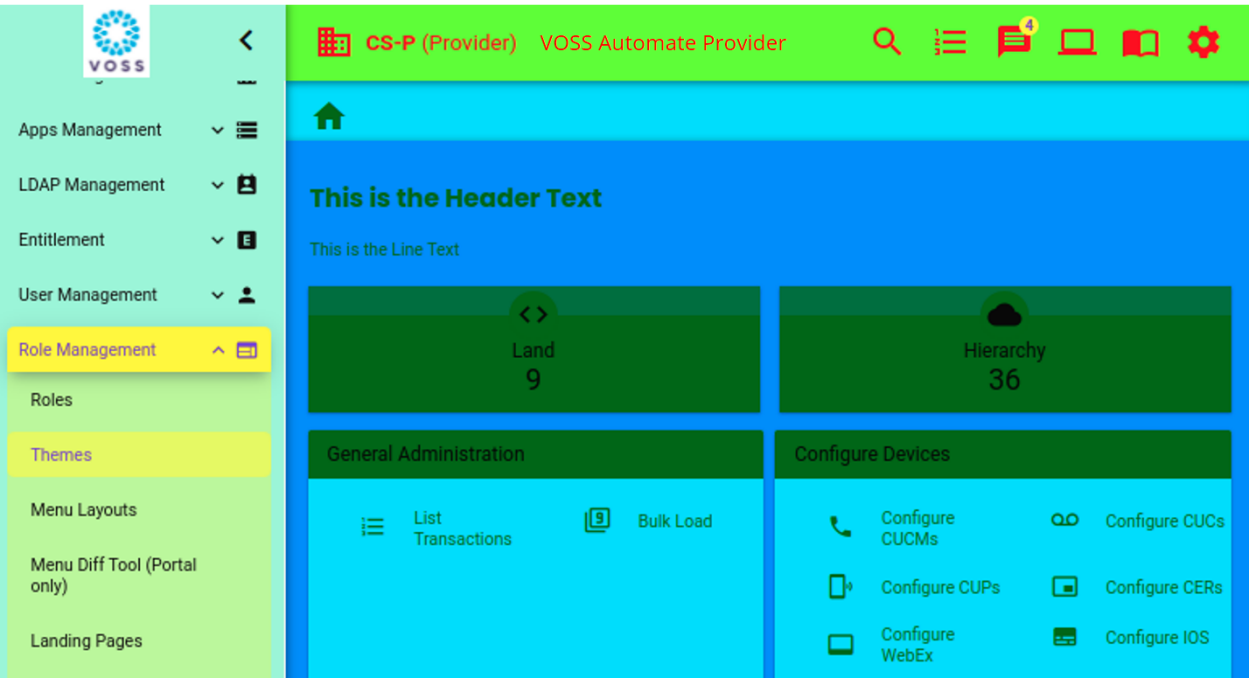
Copyright © 2025 VisionOSS Limited. All rights reserved.

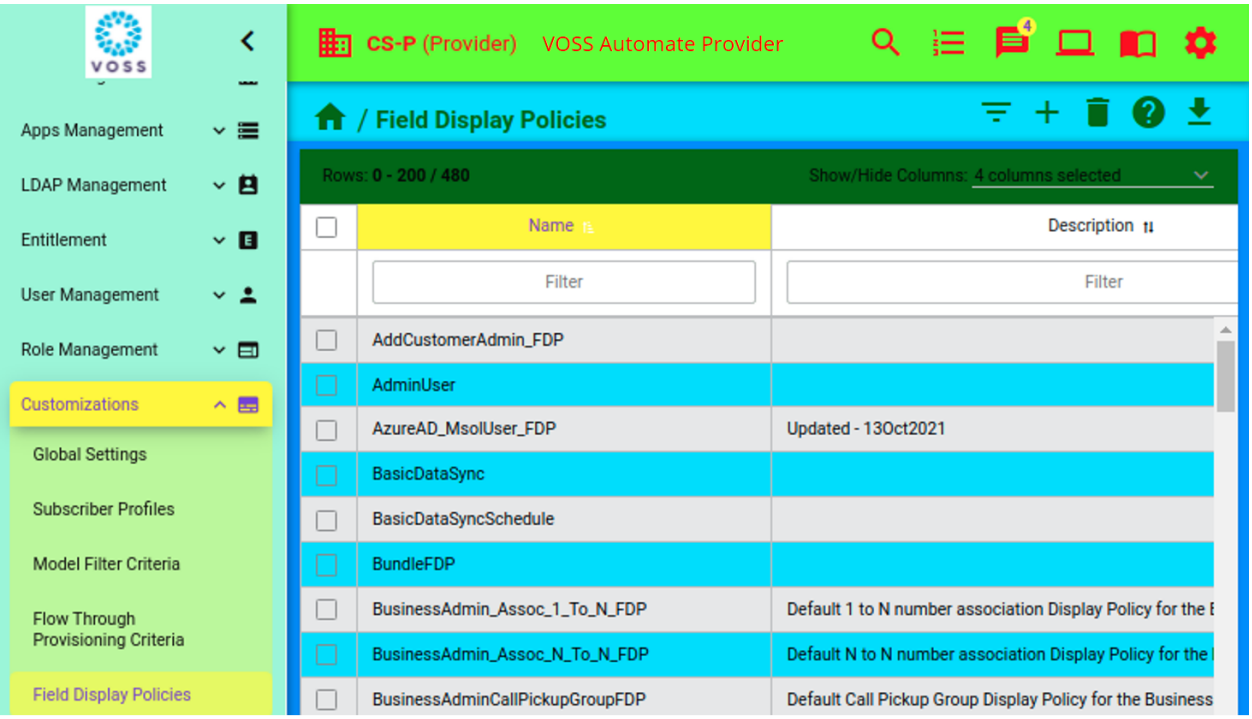
Note:

- For details on images and logos, see: *Manage themes*.
- If a color value appears blank, default values apply.
- Sub-menu and sub-sub-menu backgrounds are rendered as percentages of the Menu Color.

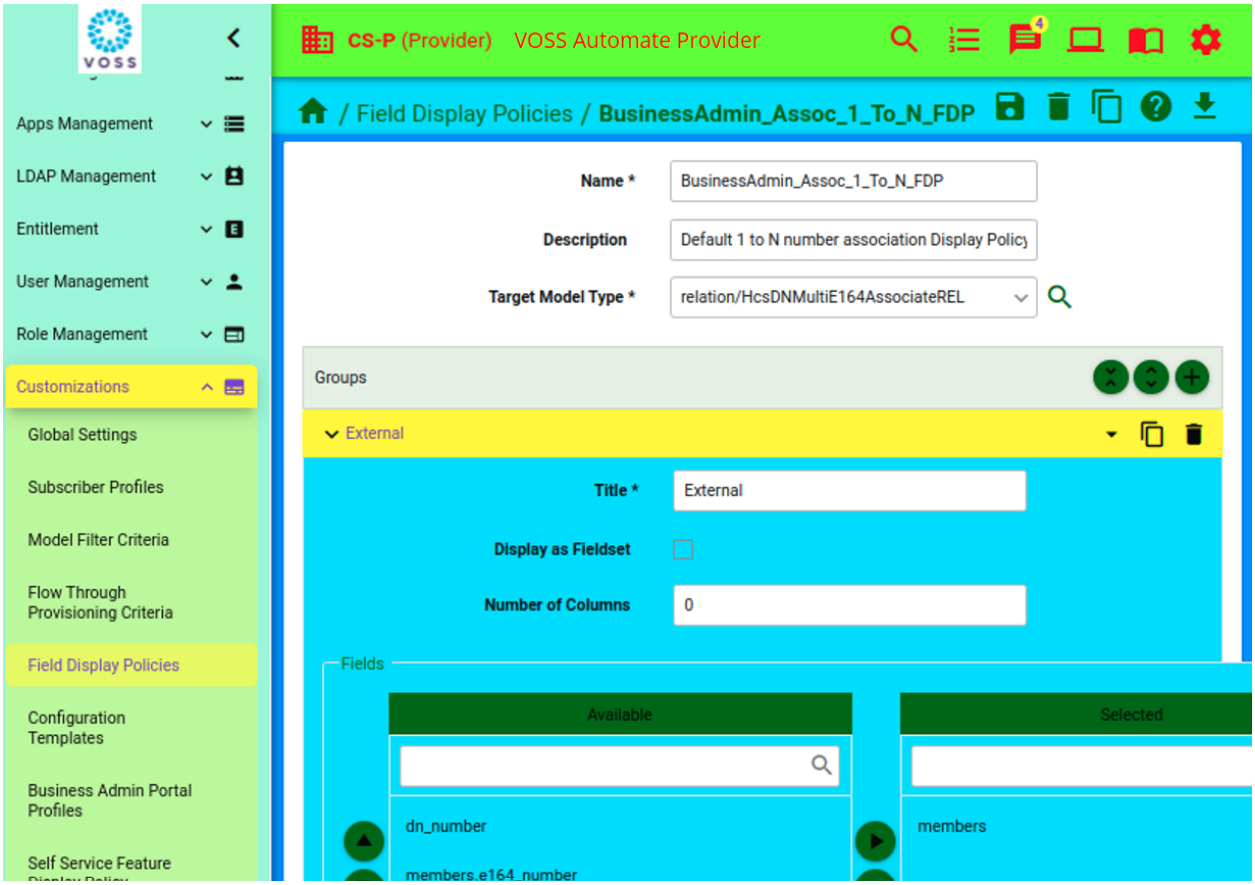
Copyright © 2025 VisionOSS Limited. All rights reserved.

Admin portal





Copyright © 2025 VisionOSS Limited. All rights reserved.



Setting the default theme

Automate provides a number of options to set the default theme upon login.

The list below indicates the priority order in which a theme will be applied:

1. URL parameter

   The Login page theme can also be applied to the login page during the log in process. To to this, add URL parameter `theme=<theme-name>` to the login request URL. This applies and overrides any theme that is set as the Login theme.

   Note: For Self-service, if the theme value is set as `login?theme=cisco_selfservice`, the theme reverts to the Self-service theme set as the default.

   For example, when two themes are available in the system, XYZ and ABC, and XYZ login page is set as default:

   - Admin Portal (legacy):

     `https://instance/login/` - Login page will show use XYZ theme

     `https://instance/login/?theme=ABC` - Login page will show use ABC theme

   - Admin Portal (introduced at v21.2):

     `https://instance/portal/#/admin` - Login page will show use XYZ theme

Copyright © 2025 VisionOSS Limited. All rights reserved.

`https://instance/portal/#/login?targetAppMode=admin&theme=ABC` - Login page will show use ABC theme

2. Subdomain of hostname

   If not 1. above:

   If the login URL is not an IP address, but a hostname, then if the *subdomain* of the hostname matches a theme name, this theme will apply.

   For example, if the hostname is `customer1.mydomain.com`, and a theme with the name `customer1` exists, then this theme will be applied.

   Hostname matching is case-insensitive. Note that if multiple themes are for example available that match case-insensitively, no match will be made and the default theme will be applied.

3. Default login theme for the interface

   If not 1 and 2 above:

   If a theme has been created for the interface and **Use this Theme to style Login page** has been enabled, then this theme will be applied to the interface.

4. Pre-defined defaults

   If not 1, 2, 3 above:

   - For the Self-service interface, the theme `voss_selfservice` will be applied.
   - For the Administration interface, the theme with name `default` will be applied.

5.5.5. Access Profiles

Introduction to access profiles

Tip: *Use the Action search to navigate Automate*

Overview

Access profiles define the model types that a user is allowed to access, and are assigned to users via the **Roles** page.

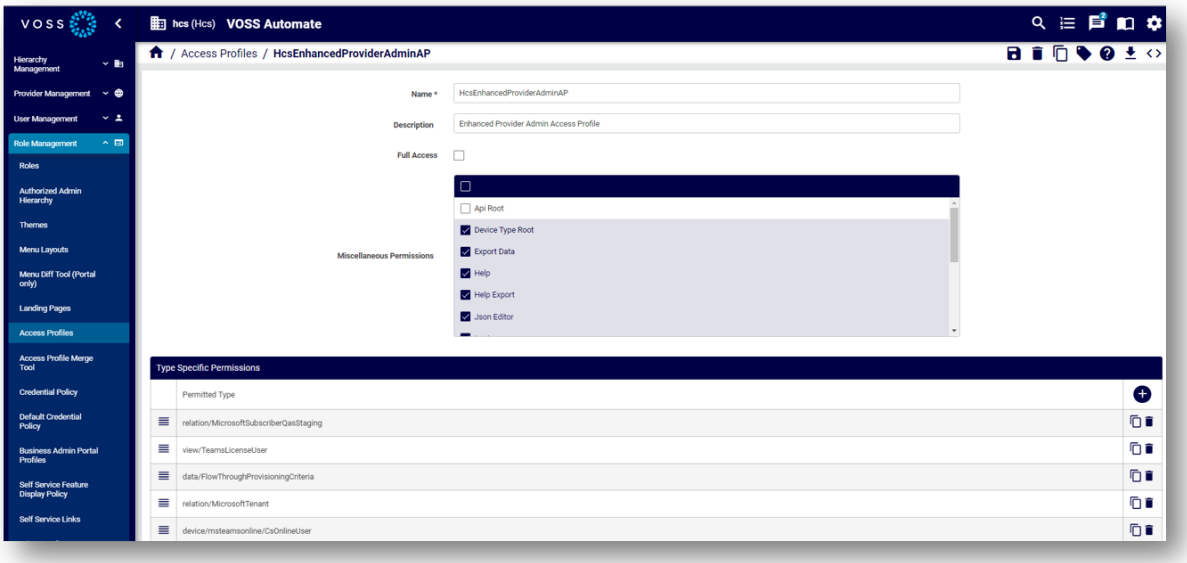
Access profiles are subject to the following requirements:

Default access profiles	These adhere to the following hierarchy of permissions: **Provider > Reseller > Customer > Site**. For instance, default Customer access profiles have less permissions than Provider access profiles. By default, the access profiles that ship with the system (except for Operator access profiles) have *read* and *export* permissions on all multi vendor subscriber quick actions and service card actions that are views, for example, `view/DeleteCucmHuntGroupAllMembers` (quick action, *Remove from all Hunt Groups*) or `view/AddExtensionMobility` (service card action, *Add Extension Mobility*).
Cloned access profiles	A cloned access profile has equal or less permissions than the access profile of the admin user who creates the clone.

Copyright © 2025 VisionOSS Limited. All rights reserved.

When a system upgrade is performed, the default access profiles are updated in accordance with the above.

Note: Existing cloned access profiles are **not** upgraded. You have to manually update them, or re-clone and modify them from the upgraded, default versions as needed.



Related topics

- Access profile permissions and operations in the Core Feature Guide
- *Search in Automate*

Manage access profiles

Admins at a higher level than Provider admins can view, add, edit, and delete access profiles via the **Access Profiles** page.

The list view shows existing access profiles added to the system.

- To add an access profile, click the Plus icon (+) from the list view, then fill out details on the configuration screen.
- To delete an access profile, select an access profile in the list view, then click the **Delete** icon.
- To edit an access profile, click on the access profile in the list to open the configuration screen.

The table describes configuration options when adding or editing an access profile:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
Name *	name	The name that is given to the access profile.
Description	description	A description for the access profile.
Full Access	full_access	Enabling this flag, grants the user full system access.
Miscellaneous Permissions	miscellaneous_permissions	The list of miscellaneous operations permitted by this access profile.
Type Specific Permissions	type_specific_permissions	Configure permissions per model type for this access profile. These permissions override any Permitted Type permissions using a wild card "*" of the same type.

Type-specific permissions

Title	Field Name	Description
Permitted Type *	type	The type that is permitted by this access profile. This field supports the use of the * wildcard. The wildcard can be restricted by a type-specific permission of the same type.
Permitted Operations	operations	The operations that are permitted by this access profile for the given type.

Related topics

- *Search in Automate*

Access profile permissions and operations

Overview

Administrators *above* Provider level, for example, `hcsadmin`, can maintain access profiles as a part of managing roles. An access profile assigned to a role provides a general set of permissions and type-specific operations that are associated with specific models.

For type-specific operations, wild cards may be used in model references, for example `data/*`.

Note: Type-specific permissions that are also configured as general permitted operations will override the general permissions.

The default access profiles show typical configurations, for example an Operator-type profile at a hierarchy would *only* require **Read** type-specific permissions, while the administrator profile at the same hierarchy would have **Create**, **Update** and **Delete** permissions for the same type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The default access profiles of the following administrators above Provider level have full general and type-specific permissions to all models:

- `hcsadmin` (Provider product deployment)
- `entadmin` (Enterprise product deployment)

Permissions

This section provides details on the following categories of permissions:

- Miscellaneous permissions
- Dashboard permissions (dashboard permission groups)
- Type-specific permissions
- Dependent permissions

Miscellaneous permissions

Many of the miscellaneous permissions are general permissions that can be overridden per model as *type-specific permissions*.

The table describes miscellaneous permissions:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Permission	Description
Api Root	Allows access to the API root endpoint.
Copilot Chat	Displays and allows the use of the **VOSS Wingman** AI assistant or copilot. This permission also requires the **Enable Copilot Chat** global setting (enabled by default) to be enabled. Refer to the *Settings and Tools* section in the Advanced Configuration Guide.
Device Type Root	Allows access to API `device` type model root endpoint, e.g. `https://<host_name>/api/device/cucm/`
Export Data	This permission is granted to users by default, regardless of their access profile. Allows export of data.
Help	Displays the On-line help button.
Help Export	Allows export of Help data.
Json Editor	Allows access to the JSON Editor for the editing of model instances. Displays a **JSON Edit** button on the GUI.
Login	Allows log in.
Meta Schema	This permission is granted to users by default, regardless of their access profile. Allows access to meta schema. For example, `https://<host_name>/api/device/cucm/AarGroup/schema/` returns schema details of the model `/device/cucm/AarGroup/`
Model Type Choices	This permission is granted to users by default, regardless of their access profile. Displays model type drop-downs (the drop-down is filtered to display only the the models allowed by the access profile). Allows access to API choices endpoint of model types, for example, `https://<host_name>/api/device/cucm/choices/` to list all instances of model type `/device/cucm/`.
Model Type Root	Allows access to API model root endpoint, for example, `https://<host_name>/api/device/`
Operations	Allows operations on models.
Tag	Allows tagging of models.
Tool Root	Allows access to API tool root endpoint; that is, `https://<host_name>/api/tool/`
Upload	Allows uploads.

Dashboard permissions (permission groups)

Dashboard permission groups define a group of Insights resource permissions required for dashboards.

Insights reporter resources (`data/ReporterResource`) required for the display of data on dashboards can be assigned individually as **Specific Permissions** in an access profile, or grouped into **Dashboard Permission Groups**, which can then be assigned. This simplifies the management of dashboard permissions. Access profiles allow for the management of these by means of transfer boxes.

If a user has access to a dashboard containing widgets that use reporter resources but the related access profile does not contain the resource, the widget data won't display and the user can't manage the widget.

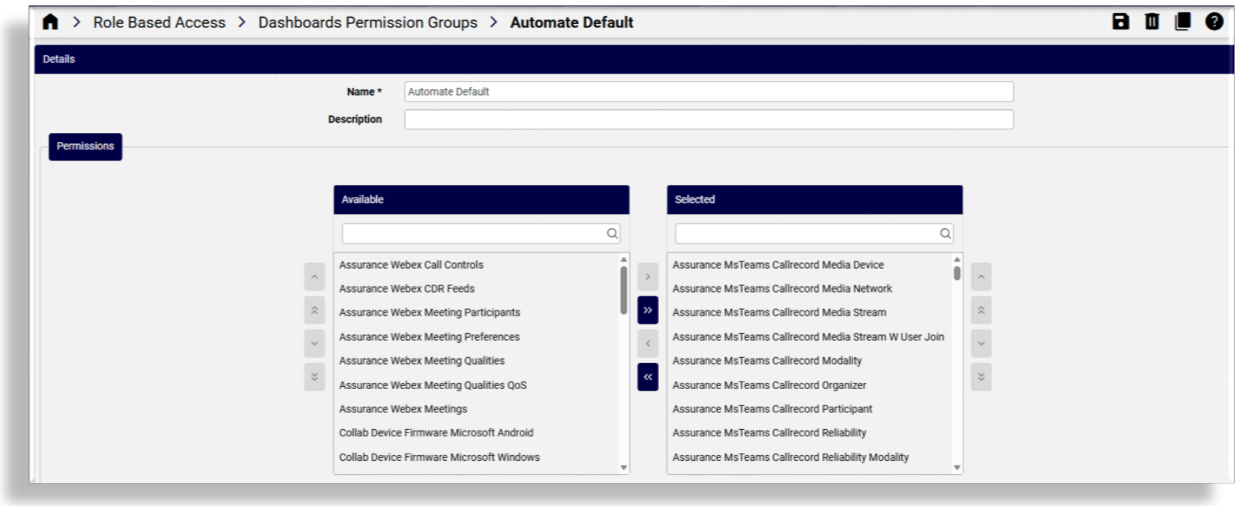
Admins with access to **Dashboard Permission Groups** can manage these groups so that they can be

Copyright © 2025 VisionOSS Limited. All rights reserved.

managed in an access profile.

Admins with access profiles inherited from the default Provider-level access profile are allowed to create and delete these permission groups. If a specific permission is not selected but is in a selected permission group, the group selection applies.

An access profile's *Dashboard permissions* is a combination of resources selected from groups and specific permissions. For details on dashboards, see *Introduction to Automate dashboards*.



Type-specific permissions

Type-specific permissions are typically available on the GUI when listing or showing the type.

Note:

- Available permissions can vary according to the selected type.
- If the **Create** type-specific permission is enabled for a model type, this also enables **Clone** of a model instance.

The table describes some of the type-specific permissions:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Permission	Description
`data/DashboardFieldGrouping:read`	Required for dashboards to work. This permission is granted to users by default, regardless of their access profile.
`view/HcsVersionVIEW`	Allows you to view *About* information.
`data/UserSavedSearch:read`	Allows the user to view saved searches.
`data/Alert:read`	Allows the user to receive alert notifications.
`data/MenuLayout:read`	This permission is granted to users by default, regardless of their access profile.
`data/Dashboard:read`	This permission is granted to users by default, regardless of their access profile.
`data/Dashboard:export_dashboard_d`	Allows the user to have the Export Dashboard Data custom action. Note that this permission is different from the export permission that allows for the schema export of the model, since it applies to the data contained in an instance.
`data/HierarchyNode:read`	This permission is granted to users by default, regardless of their access profile.
`data/SelfServiceTranslation:read`	This permission is granted to users by default, regardless of their access profile.

The table describes typical operations allowed by type-specific permissions:

Operation	Description
Create, Delete, Read, Update	Management operations on models.
Configuration Template, Field Display Policy	Create these for the model.
Export, Export Bulkload Template	Allow export formats of the model.
Bulk Update	From a GUI list view, more than one item can be selected and updated.
Purge	Allows purge for device models, for system level administrators above Provider level. From a list or instance view, removes the local database instance but retains it on the device. This operation is only relevant where the UC server is still online and available in the Automate system.
Migration	For designers. A migration template can be obtained.
Tag, Tag Version	For designers. A model instance can be tagged and a version provided.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dependent permissions

Dependent permissions are permissions that apply to some API endpoints and may be granted by virtue of having another permission in the access profile.

The following dependent permissions apply:

- Permission to `/api/handle_oauth_webex/`

  Granted by the permission to the **Update** operation on `relation/SparkCustomer`

Related topics

- Introduction to access profiles in the Core Feature Guide

5.5.6. Menu Diff Tool

Menu diff tool

System level (hcsadmin, entadmin) and provider administrators have access to the Menu Diff tool on the menu to allow for a side-by-side comparison and management of two selected menu layouts:

- **Source Menu**: a drop-down list of menu layouts from hierarchies at the administrator's hierarchy *and higher*.
- **Target Menu**: a drop-down list of menu layouts from hierarchies at the administrator's hierarchy *and lower*.

The side-by-side forms with the two selected menus can be expanded using the **Expand**/**Collapse** button.

Menu differences are highlighted as follows:

- The same menu item in both menus but on a different menu path is highlighted.
- A menu item in one menu but not in the other menu is highlighted.

To update the target menu, drag and drop menu items from the source menu to a position in the target menu.

- Where a menu item is now in both menus, it is not highlighted anymore.

Note:

- All menu properties (e.g. Field Display Policy, model reference, and so on) are copied.
- If the menu item than is copied contains sub-menus, these are included.

Click **Save** to save changes in the target menu.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

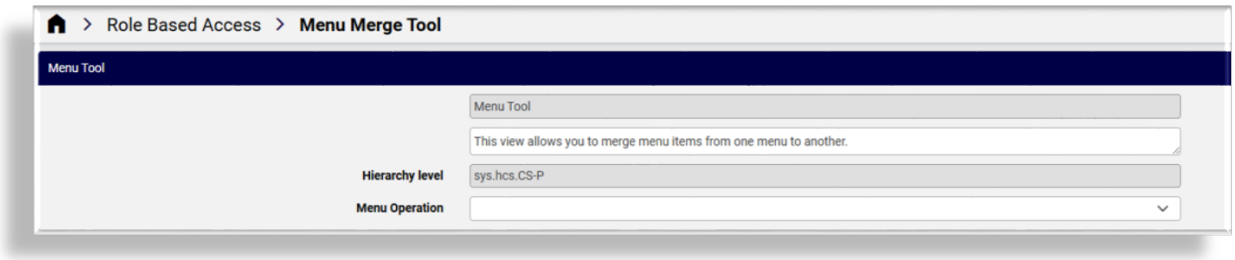
- Menu Merge Tool in the Core Feature Guide

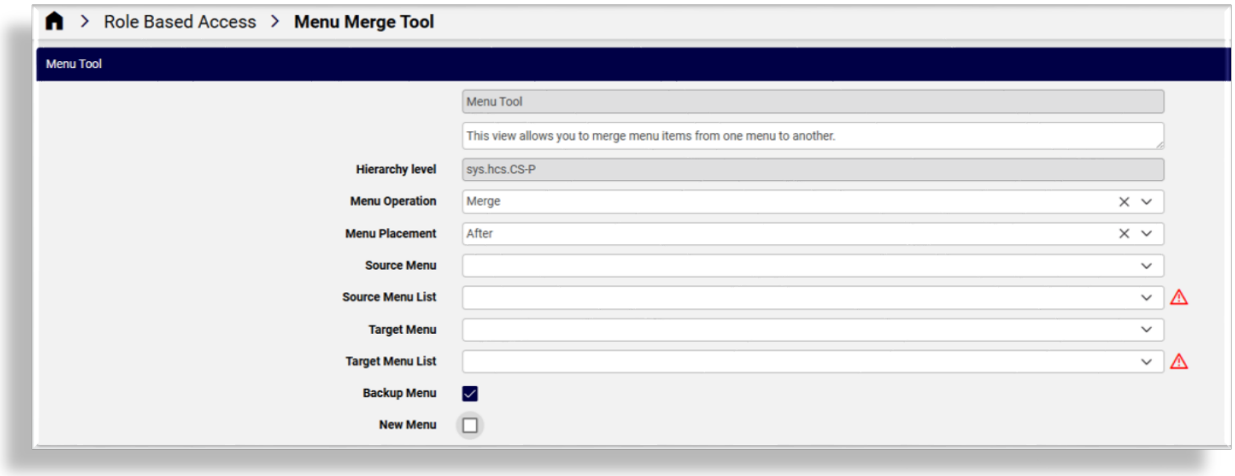
5.5.7. Menu Merge Tool

Tool to manage menus

Menu Merge tool

The Menu Merge Tool allows to you merge menu items from one menu to another.





5.6. Privacy and Login Control

5.6.1. Credential Policy

Credential policies

Overview

Credential policies are sets of rules that define user sign-in behavior at various levels of the hierarchy. For example, to facilitate user account security, VOSS Automate authenticates user sign-in credentials before

Copyright © 2025 VisionOSS Limited. All rights reserved.

allowing access to the system. Additionally, administrators can configure settings for events such as failed sign-in attempts and lockout duration.

Credential policies can be applied at any hierarchy level. A credential policy applied at a particular hierarchy defines allowed user sign-in behavior at that hierarchy.

Related Topics

- *Introduction to hierarchies*
- *Authorized Admin Hierarchy Roles*

Default credential policy

While credential policies are not mandatory at specific hierarchy levels, a default credential policy is defined at the sys.hcs level.

Administrators at lower levels can copy and edit the default policy, if required, or they can save the default credential policy at their own hierarchy level so that it can be applied to users at that level.

Inherited credential policies

If an administrator at a specific level of the hierarchy has not created a credential policy at their hierarchy level, the credential policy is inherited from the closest level above.

If a Provider administrator has defined a credential policy, but a Customer administrator has not defined a credential policy, the customer hierarchy automatically inherits the credential policy from the Provider level.

Custom credential policies

A different credential policy can be defined for each user.

For each administrator user where IP address throttling (sign-in Limiting per Source) is required, a credential policy should be manually created and assigned. This credential policy must have an IP address, and username and email throttling enabled.

Related Topics

- *Customized credential policy*

Credential policies, SSO authenticated users, and LDAP-synced users

Credential policies are not applicable for SSO authenticated users. For LDAP synced users, only the session timeouts are applicable.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Assign a credential policy to a user

Tip: *Use the Action search to navigate Automate*

This procedure assigns a credential policy.

Typically, a user inherits a credential policy from the nearest hierarchy node, at or above their location, wherever a default credential policy is defined. However, you can explicitly assign a credential policy to a user.

1. Log in as provider, reseller, or customer administrator.
2. Go to the **Users** page.
3. Click the user that you want to assign a credential policy to.
4. On the **Account Information** tab, from the **Credential Policy** drop-down, choose a credential policy to assign.

   The menu contains all the credential policies available at or above the user's node in the hierarchy.
6. Click **Save**.

Note: If a user is signed in when the credential policy is changed, changes are not applied until the user signs out and signs in again.

Assign a credential policy to an administrator

Tip: *Use the Action search to navigate Automate*

This procedure assigns a credential policy to an administrator.

Typically, an administrator inherits a credential policy from the nearest hierarchy node at or above their location, wherever a default credential policy is defined. However, you can explicitly assign a credential policy to an administrator.

1. Log in as provider, reseller, or customer administrator.
2. Go to the **Admins** page.
3. Click the administrator that you want to assign a credential policy to.
4. On the **Account Information** tab, from the **Credential Policy** drop-down, choose a credential policy to assign.

   The menu contains all the credential policies available at or above the administrator's node in the hierarchy.
6. Click **Save**.

Note: If an administrator is already logged on when the credential policy is changed, changes do not take effect until the administrator logs out and logs on again.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Customized credential policy

Tip: *Use the Action search to navigate Automate*

Overview

A default credential policy called `HcsCredentialPolicy` ships with Automate. However, you can deploy a customized credential policy at a provider, reseller, or customer hierarchy node.

When you set a customized credential policy as the default credential policy at a hierarchy node, all users and admins at or below that hierarchy node are subject to the customized credential policy, except for any users or admins that are explicitly assigned a different credential policy.

Related topics

- *Credential policies*

Credential policy inheritance

Unless explicitly assigned a credential policy, users and admins are subject to the default credential policy set at a hierarchy node at or above their location. The default credential policy for the hierarchy node closest to the user or admin location is used. If no customized credential policies are deployed, all users and admins are subject to the HcsCredentialPolicy credential policy, which is the default credential policy at the sys.hcs level.

Deploy a customized credential policy

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where you want to deploy a customized credential policy.
3. Go to the **Credential Policy** page.
4. Either clone the HcsCredentialPolicy credential policy, or add a new credential policy:
   - To clone the HcsCredentialPolicy policy, click **HcsCredentialPolicy**, then click **Action > Clone**.
   - To add a new credential policy, click **Add**. The credential policy settings default to the settings for HcsCredentialPolicy.
5. Provide a name for the credential policy.
6. Modify the credential policy settings as needed.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Idle Session Timeout	The number of minutes a user session can be idle before being automatically logged off. The minimum setting is 1 minute and the maximum is 525600 minutes (365 days). The default is 20 minutes.
Absolute Session Timeout	The number of consecutive minutes a user can be logged in, regardless of session activity, before being automatically logged off. A value of 0 disables absolute session timeout. The maximum is 525600 minutes (365 days). The default is 1440 minutes (24 hours).
Password Expires	The number of months that can elapse between password resets. The default is 6 months.
User Must Change Password on First Login	Select this check box to force users to change their password on initial login. Default = clear.
Lock Duration	The number of minutes a lock will be held when user is locked out. The default is 30 minutes.
Disable Failed Login Limiting per User	Select this check box to not limit the number of times a user can fail to log in before the account is locked. Default = clear
Failed Login Count per User	Selecting this check box will result in user account being disabled if failed login attempt reaches 'Failed Login Count per User' within 'Reset Failed Login Count per User (minutes)'. This field is clear by default.
Reset Failed Login Count per User	After this number of minutes from the last login attempt, the failed login count is reset to 0. The default is 5 minutes.
Disable Failed Login Limiting per Source	Clear this check box to limit the number of times any user from the same IP address can fail to log in before the account is locked. Note: On Provider HCFM and Provider Decoupled deployments, the default is to disable the limit. (checked) On Enterprise deployments, the default is to enable the limit. (unchecked) Do not enable source login rate limiting for a credential policy that will apply to Self Service users. A separate credential policy is recommended for administrators and users that do not use Self Service if source login rate limiting is required.
Failed Login Count per Source	If source login rate limiting is enabled, enter the number of times any user from the same IP address can fail to log in before the IP address is blocked. The default is 10 times.
Reset Failed Login Count per Source	If source login rate limiting is enabled, this value is the number of minutes from the last login attempt from the IP address after which the failed login count is reset to 0. The default is 10 minutes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Number of Questions Asked During Self Service Password Reset	Enter the number of security questions users or admins must answer when resetting their own password with the **Forgot Password** link. The default is 3.
Password Reset Question Pool	Contains a list of possible security questions that users or admins must answer when resetting their own password with the **Forgot Password** link.
Password Reuse Time Limit	The number of days from the date the password was created that the password cannot be reused. The valid range is 0-365 days. The default is 15 days. Setting it to 0 disables the reuse time limit.
Minimum Password Length	The minimum length of a password in characters. The minimum allowed value is 8. The default is 8. When a password is entered that does not meet the length as specified here, an error message will display to indicate the minimum length entered here.
Enable Password Complexity Validation	Select this check box to enable the rule on how complex a password must be. The complexity rule requires a password to contain at least one of each of the following: • Uppercase letter • Lowercase letter • Digit • Special character (see below)
Inactive Days Before Disabling User Account	The number of days users or admins can go between logging in without having their account disabled. Setting it to 0 disables the inactive time limit. The default is 0.
Session Login Limit Per User	The number of concurrent login sessions a user may have. Setting it to 0 disables the session login limit. The default is 0. If the session limit value is set to 1 or more and the user exceeds the session limit when starting a new session, the oldest login session will be disconnected.
Number of Different Password Character	The minimum number of character changes (inserts, removals, or replacements) required between the old and new passwords.
Minimum Password Age	The number of days within which a user cannot change their password. A zero (0) value means that password age validation is disabled. The minimum value is 1 day and the maximum is 365 days.

Acceptable special characters are:

```
` ~ ! @ # $ % ^ & * ( ) - _ = + [ { ] } | \\ : ; ' " , < . > / ?
```

Note: It is recommended that you make a credential policy only more restrictive than HcsCredentialPolicy in order to not have a policy that is too insecure.

7. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: If a user is already logged in when the credential policy is changed, changes do not take effect until the user logs out and logs in again.

8. Go to **Default Credential Policy**.
9. Provide a name for the Default Credential Policy at this hierarchy node.
10. From the **Credential Policy** drop-down, choose the credential policy you just cloned or added.
11. Click **Save**.

    Every user and administrator at or below the hierarchy node is now subject to the default credential policy, unless the user or administrator was explicitly assigned a different credential policy.

Note: Timeout limits will initiate the display of timeout limit notifications in the Admin Portal - see: *Timeout limit notifications*.

5.6.2. Hierarchy Default Credential Policy

5.6.3. Privacy Policy Configuration

Privacy policy menu items

VOSS Automate supports management of privacy policy notices on the user interface. This allows compliance with General Data Protection Regulation (GDPR) requirements.

By default, high level system administrators above the Provider level hierarchy can manage privacy policy references that are available on user menus. These administrators can provide the required access to the `data/PrivacyPolicy` data model and add menus to lower level administrators if required.

Privacy policy references can be set up for each hierarchy. If one is not added to a specific hierarchy, the one at the next higher hierarchy applies.

When a privacy policy applies to a user hierarchy:

- On the Admin Portal, a privacy policy menu item is added to the bottom of the user's menu. The title of the menu item is the name of the created policy.
- On the Self-service GUI (if available), a side button bar menu item is added. The title of the menu item is **Privacy Policy**.

When selecting the menu item, the link URL of the policy opens on a new browser tab.

Note:

- For the Admin Portal, the Privacy Policy menu item is not visible from a menu layout and cannot be managed from **Menu layouts**.
- Login page privacy policy links are managed from **Themes**.

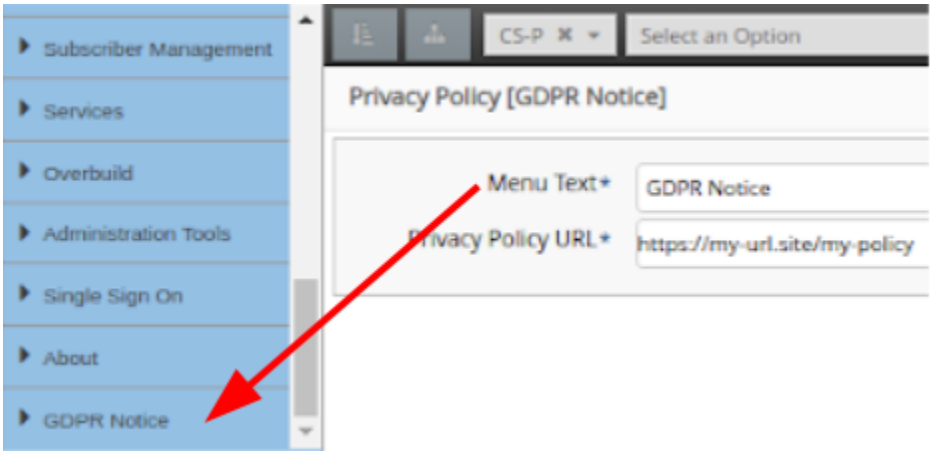
Copyright © 2025 VisionOSS Limited. All rights reserved.

Manage privacy policy menu items

Tip: *Use the Action search to navigate Automate*

1. Log in as an administrator with the required privacy policy management permissions and menu access.
2. Go to the page, for example by default, **Privacy Policy Configuration**. The list view shows privacy policy names and links at various hierarchies in the system. Privacy policies can then be added, modified and deleted.
3. To add a privacy policy, navigate to the hierarchy at which the privacy policy should be added and click **Add**.
4. Add a Name, Privacy Policy URL and click **Save**. Note that this name becomes the menu item name.

On the Admin Portal, a privacy policy menu item is added to the bottom of the user's menu - for users at the specified hierarchy or lower and without a privacy policy on their own hierarchy. On the Self-service GUI, a side button bar menu item is added.



Support for privacy and security notices

Automate allows for the configuration of appropriate login security warnings as well as links to cookie and privacy policies for best practice and compliance with regulatory requirements such as General Data Protection Regulation (GDPR).

Support is available on the login screen as well as menus of both the administrator interface and the Self-service application.

- Pop-up login banner

  A pop-up banner can be configured for the purpose of security notices or user agreements on the login page after users enter their credentials and when they click the **Login** button on either the administrator interface or Self-service application. Clicking either the **Agree** or **Cancel** buttons remove this pop-up banner.

  For details on configuration, refer to *Login notification banner*.

- Privacy and Cookie Policy notices

  When drafting cookie policy notices, Automate provides reference content - see: *Automate cookie policy*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Login screens: As a part of Theme management, Privacy and Cookie Policy notices can be added on the login interface of both the administrator and Self-service login screens.

  For configuration details, see:

  Login Banner in the Core Feature Guide

  The style of the banner can also be customized. Refer to "Theme Banner Customization" in the "Advanced Configuration Guide".

- Menu items: High level system administrators above the Provider level hierarchy can manage privacy policy references that are available on administrator and Self-service user menus.

  For details, refer to *Privacy policy menu items* and *Manage privacy policy menu items*.

Automate cookie policy

When formulating a cookie policy, customers should include details on the use of cookies by Automate. The following text provides details on the use of cookies in Automate that can be included in the policy:

```
VOSS Automate uses cookies for the following purposes:

Personalisation - we use cookies to store information about your most recent settings,
preferences and to personalize our website for you.

The cookies used for this purpose are:

hierarchyTreeSaveStateCookie
resourceTreeSaveSelectedCookie
resourceTreeSaveStateCookie
ace.settings
sso_login_url

Security - we use cookies as an element of the security measures used to protect
user accounts, including preventing fraudulent use of login credentials, and to
protect our website and services generally.

The cookies used for this purpose are:

* Administrator login:

  csrftoken
  sessionid

* Self-service login:

  csrftoken
  sessionid
  session
  rbacInfo
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

5.6.4. Login Notification Banner

Login notification banner

A banner, typically a security notice or user agreement, can be configured at a hierarchy level to show on the Administrator and Self-service login page before login.

High level administrators who have access to the `data/LoginBanner` model can configure the banner. A banner can be created so that:

- Only one instance is allowed per hierarchy

If an administrator or Self-service user logs in and belongs to a hierarchy for which there is no defined login banner, the first banner higher up on the hierarchy is displayed. If no banners are configured, then the user logs in without a banner.

The banner text is displayed in the format that it is entered into the input box upon configuration.

When the banner is configured, users will see the banner displayed on the login page after they enter their credentials and when they click the **Login** button. An **Agree** and **Cancel** button is shown beneath the banner. Users then need to click the **Agree** button to complete the login. If they click **Cancel**, they are returned to the login page.

Note: This banner is independent of the text on the login screen that may contain a privacy policy reference. The privacy policy text and reference on the login page is configured as a part of the Login Page Details when managing a theme.

5.6.5. Single Sign On (SSO)

Single Sign On (SSO) Overview

VOSS Automate supports Single Sign-on (SSO) through the SAML v2 standard for SSO. The system acts as a service provider in the SAML authentication architecture and supports service provider initiated (SP-initiated) authentication of users against a SAMLv2 Identity Provider (IdP).

Authentication settings on an IdP server include:

- Authentication Scope
- User sync Type**

For details, see *Configure Self-service SSO SP settings*.

Users accessing VOSS Automate using SSO authentication are required to access the system using a URL that is specific to the IdP setup in VOSS Automate. This ensures that the SAML interaction is with the correct IdP, since VOSS Automate supports multiple IdPs to be set up in the system.

Note: SSO for end-user Self-service is supported when using a shared VOSS web proxy for Admin and Self-service, when using the Admin URL in the SSO setup. Once authenticated in the IdP via that URL, the user is dropped into the end-user Self-service interface (if they are an end user) and access via their role. SSO is not supported when using a dedicated Self-service proxy.

When accessing the URL, the user is presented with the login challenge via the Identity Provider (outside of VOSS) if they do not already have a session active on the IdP. Once authenticated with the IdP, the assertion

Copyright © 2025 VisionOSS Limited. All rights reserved.

from the IdP is sent to VOSS Automate from the IdP and the user is given access and presented with the appropriate interface in VOSS Automate (Admin or Self-service). If users already have an authentication session with the IdP, they do not see the IdP login page and will be directed straight to VOSS Automate.

Note:

- Credential policy features, such as password rules or session length, are all managed by the IdP outside of VOSS Automate.
- SSO support is for authentication only and does not apply the user's permissions within VOSS Automate.
- No logout is supported when using SSO. VOSS Automate will not initiate the termination.

To read through an example for configuring VOSS Automate and Microsoft Entra for SSO, see the following reference document:

VOSS Automate Technote - Single Sign On (SSO) with Microsoft Entra PDF (available on the VOSS Automate Documentation Portal)

Configure Self-service SSO SP settings

hcs-admin

Tip: *Use the Action search to navigate Automate*

This procedure configures Self-service Single Sign-On (SSO) for Automate.

Note:

- The configuration applies to customers and customer administrators associated with the identify provider (IdP).
- Administrators are configured for SSO use via the **Users** page.
- Administrators can also be configured with multiple user roles, that is, have a user type "End User + Admin" (see: *Add admin user*).

  While the role of such an administrator user is "selfservice", the user's association with an Authorized Hierarchy model instance redirects such an administrator to the *same* interface as a single role administrator when using the SSO URLs for login. See *Integrating with an SSO Identity Provider*.

  Administrators with multiple user roles who wish to access the *Self-service* interface need to explicitly switch to the Self-service portal URL upon login:

```
https://<Hostname>/selfservice/#/
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Prerequisites:

- Create a self-signed or third-party-signed system certificate.
- The Automate server and the IdP server must be configured so that their clocks are synchronized.

  You can define the number of seconds of permitted clock drift between Automate and the IdP. The number of seconds for tolerance is customizable, and this value must be set in accordance with the deployment's security policy. By default, Automate uses a value of 0 for clock drift; that is, assume clocks are exactly in sync.
- You must be a high-level administrators logging in above the *Provider* admin level to perform this procedure.

To configure self-service Single Sign-On (SSO) for Automate:

1. Log in to Automate as *hcsadmin*.
2. Go to **SSO SP Settings**.
3. Click the Plus icon (+) to add a new record.

   Note: Configure only one instance of SSO SP Settings.

4. On the **Base** tab/panel:
   - (Mandatory). At **System Certificate**, select the signed third-party system certificate to use.

     Note: Choosing an unsigned third-party-signed certificate will result in an error. For details around renewing an expired certificate. See *Renew single sign-on certificate for Automate* in the Core Feature Guide.

   - At **Validity (Hours)**, to allow the SSO SP setting to expire, enter a number of hours. This is the validity period (in hours) that the metadata is valid for.
5. On the **SAML SP Settings** tab/panel:
   - (Mandatory). At **FQDN of the Server**, fill out the server FQDN.

     Note: The FQDN that will be embedded in the SP metadata for this IdP for URLs that refer back to the Service Provider. The FQDN of the server is stored in the SP metadata that is uploaded to the IdP. The SSO login URL then contains the fully qualified domain name (FQDN):

     `https://<FQDN of the Server>/sso/<login_URI>/login`

     If you have configured a custom hostname for SSO user login, enter it here. Upon login, the IdP will redirect you to this FQDN.

   - Select options relevant to your security environment and requirements:
     - **Sign Authn Requests**

       Defines whether outgoing authentication messages will be signed. If yes, the specified private key will be used. By default, this is False (unchecked). If one of your identity providers has *WantAuthnRequestsSigned* set in its metadata, then select this checkbox (set to True).

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Want Assertions Signed**

  Defines whether assertions should be signed. Only select Want Reponse Signed if you're sure that all IdPs sign responses.

Note: If a secure connection is required with the secure attribute set on the cookies, the URL values for bindings of end points must be specified with `https`.

The **Assertion Consumer Service** fields define how SAML requests and responses map on to standard messaging and communications protocols.

---

6. Save your changes.

Note: Saved SSO settings are published by the Automate service provider and are available from metadata URL, for example: http://mydomain/sso/metadata/. SSO service provider configuration requests to this URL automatically trigger an xml file download of the specified SSO service provider configuration.

---

7. View the location of the Automate SP metadata that you will upload to the IdP:
   - Go to **SSO SP Metadata**.
   - Point your browser to the URL shown here.
   - Save a copy of the SP metadata.
8. Upload SP metadata to the IdP.

   Refer to your IdP documentation for details on configuring SSO on your IdP.

   The IdP must release the UID and map it to an appropriate attribute. For example, an IdP that authenticates with Active Directory can map the UID SAML attribute to sAMAccountName in the Active Directory server.
9. Download IdP metadata from the IdP server.

   Refer to your IdP documentation for details on downloading IdP metadata.

   If an expired SSO certificate is being renewed and the IdP metadata has *not* changed, then the download, configure, and upload of the IdP metadata is not required.

SAML Elements in Assertions

The following list provides details for designers on the correct handling of Security Assertion Markup Language (SAML) elements in assertions:

1. When using the `SubjectConfirmation` element in a SAML assertion, the `NotOnOrAfter` condition shall be used.
2. When using the `Conditions` element in a SAML assertion, both the `NotBefore` and `NotOnOrAfter` elements or the `OneTimeUse` element shall be used.
3. If a `OneTimeUse` element is used in an assertion, there shall only be one used in the `Conditions` element portion of an assertion.

The VOSS Automate system will inspect SAML messages and raise error messages if the elements do not follow the rules for SAML assertions specified above.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The list below shows the respective error numbers and messages as they will show in the logs, as well as example error SAML snippets:

1. NOTONORAFTER_SUBJECTCONFIRMATION_ERROR (14010)

   "SubjectConfirmation is used but there is no NotOnOrAfter attribute"

```
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData/>
</saml2:SubjectConfirmation>
```

2. a) CONDITION_NOT_BOTH (14012)

   "NotBefore and NotOnOrAfter should be present when using either in Condition"

```
<saml2:Conditions NotOnOrAfter="2015-11-20T12:32:23.645Z">
    <saml2:AudienceRestriction>
        <saml2:Audience>http://functional.fedrampfail.plain/sso/metadata/</
↪saml2:Audience>
    </saml2:AudienceRestriction>
</saml2:Conditions>
```

2. b) CONDITION_ONETIMEUSE (14013)

   "OneTimeUse element should be present when neither NotBefore nor NotOnOrAfter attributes in Condition"

```
<saml2:Conditions>
    <saml2:AudienceRestriction>
        <saml2:Audience>http://functional.fedrampfail.plain/sso/metadata/</
↪saml2:Audience>
    </saml2:AudienceRestriction>
</saml2:Conditions>
```

3. CONDITION_MULTIPLE_ONETIMEUSE (14014)

   "Only one OneTimeUse element should be present in Condition"

```
<saml2:Conditions>
    <saml2:AudienceRestriction>
        <saml2:Audience>http://functional.fedrampfail.plain/sso/metadata/</
↪saml2:Audience>
    </saml2:AudienceRestriction>
    <saml2:OneTimeUse/>
    <saml2:OneTimeUse/>
</saml2:Conditions>
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

5.6.6. Configure SSO IDP

Configure SSO IdP

Tip: *Use the Action search to navigate Automate*

This procedure configures integration with a SSO identity provider (IdP).

1. Log in as Provider, Reseller, or Customer administrator (depending on your IdP configuration level).
2. Go to **Upload SSO IDP Metadata** and upload the IdP metadata file. See *Upload SSO IdP metadata*.
3. Go to **Configure SSO IDP**, then click the Plus (+) icon to add the SSO identity provider configuration.

   Note: Only one instance of an SSO identity provider can be configured for a hierarchy node.

   While an IdP may exist at more than one hierarchy in Automate, a user will only be permitted to log in if the user exists at or below the hierarchy of a single IdP.

4. Complete at least the mandatory settings:
   - **Entity ID**: Mandatory. Entity ID of the IDP. This field must exactly match the entity ID in the IdP metadata file.
   - **Login URI**: Mandatory. Login URI for the IDP. This is the URI that will be embedded in SSO Login URL. It can contain only alphanumeric characters and forward slashes.
   - **Service Provider Domain Name**: The FQDN that will be embedded in the SP metadata for this IdP for URLs that refer back to the service provider.

     If a customer is using a *custom domain*, the value for service provider domain name is filled out at the hierarchy level and the login and metadata URLs used will be tied to the IdP as follows:

     ```
     SSO Login URL:  ``https://<Service Provider Domain Name>/sso/<Login URI>/login``
     Admin Portal:   ``https://<Service Provider Domain Name>/admin/sso/<Login URI>/
     ↪login``
     ```

     The metadata is obtained from: `https://<Service Provider Domain Name>/sso/<Login URI>/metadata`

     If the service provider domain name *is* specified, the metadata XML file from Automate then contains `Service.Provider.Domain.Name` in the assertion consumer service URL as shown in the example below:

     ```
     <md:AssertionConsumerService
         Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
         Location="https://Service.Provider.Domain.Name/sso/acs/"
         index="1"/>
     ```

     This metadata needs to be uploaded to the IdP (not the generic metadata obtained from SSO Service Provider Configuration).

     Important: If you have previously uploaded metadata to the IDP and you subsequently complete this **Service Provider Domain Name** field, you need to remove the previous record from the IdP

Copyright © 2025 VisionOSS Limited. All rights reserved.

and re-upload the metadata so that it contains this field.

If the service provider domain name is *not* specified for a given IdP, the following URLs formats are used for SSO login:

```
SSO login URL:          ``https://<FQDN of the Service Provider>/sso/<login_URI>/
↪login``
Admin Portal:           ``https://<FQDN of the Service Provider>/admin/sso/
↪<Login URI>/login``
```

The IdP redirects to this FQDN on login.

- **Local Metadata File**: Mandatory. Choose the IdP metadata file. This file must be unique across the system.
- **Note**: A reminder to upload the IdP metadata file.
- **SSO Enabled**: Select the checkbox to enable SSO for users synced in or created at the current hierarchy level. Clear this checkbox to disable SSO for the users associated with the defined IDP.
- **SSO Login URL**: Read-only. Displays the SSO Login URL to use. Users with `selfservice` role and no Authorized Admin Hierarchy will be redirected to Self-service.
- **Admin SSO Login URL**: Read-only. Displays the Admin Portal SSO Login URL to use.
- **Business Admin SSO Login URL**: Read-only. Displays the new Business Admin Login URL to use. From release 21.4, this will *always* redirect to the new Admin Portal.
- **User lookup field**: Mandatory. Select the field to bind the VOSS and SSO user - typically, `username`.
- **UID Attribute Name**: An optional attribute name string value configured on the IdP to be used as UID for authentication. If present, this value is evaluated first by Automate as the UID and used as an alternative user identifier when the default UID record is not present. If this value is not present, the default UID record is used to identify the user.
  - If a custom attribute is used as the UID from the identity provider (IdP), then use this attribute as the UID attribute name. Automate evaluates the value in **UID Attribute Name** first as the UID to identify the user and is for example used as an alternative user identifier when the default UID record is not present.
  - If this value is *not* present, the default UID record is used to identify the user. For example, if the UID attribute is not mapped on the IdP, and an attribute, `ElectronicMail`, is mapped to `mail` on the (IdP), the **User lookup field** on the SSO IdP should be the value from the `email` field in Automate, and the value for **UID Attribute Name** should be `ElectronicMail` (the attribute returned by the IdP).

The full URL of a claim in the assertion may be used as the UID attribute name together with the mapped field on User.

The SAML response may include claims attributes configured on the IdP as follows:

```
'http:\/\/schemas.microsoft.com\/identity\/claims\/objectidentifier': ['e333df87-
↪4321-4889-852e-45c291234a2b'],
'http:\/\/schemas.microsoft.com\/identity\/claims\/displayname': ['Users_
↪Display_Name'],
...
'http:\/\/schemas.xmlsoap.org\/ws\/2005\/05\/identity\/claims\/name': [
↪'User@some_domain.com']
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

If 'User@some_domain.com' maps to username in Automate, the SSO may be configured as follows:

  - User lookup field = username
  - UID Attribute Name = http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

- **Authentication Scope**: Hierarchical scope this server applies to.
  - Full tree authentication (default): All nodes at and below this node in its tree can authenticate against this server.
  - Local authentication: Only users at this node can authenticate against this server.
- **User Sync Type**: Type of users that can authenticate against this server.
  - Synced users only: Only users synced in from LDAP can authenticate against this server.
  - All users

5. Click **Save** to save the SSO IdP configuration and enable SSO if selected.
6. Go to **Admins** and filter on **Auth Method** equals `SSO` to display enabled SSO users.

Related topics

- See **SAML SP Settings FQDN** in *Configure Self-service SSO SP settings*
- For further details on authentication scope, see also *User login options by auth method and server auth scope*
- *SSO scenarios for user roles*
- *Upload SSO IdP metadata*

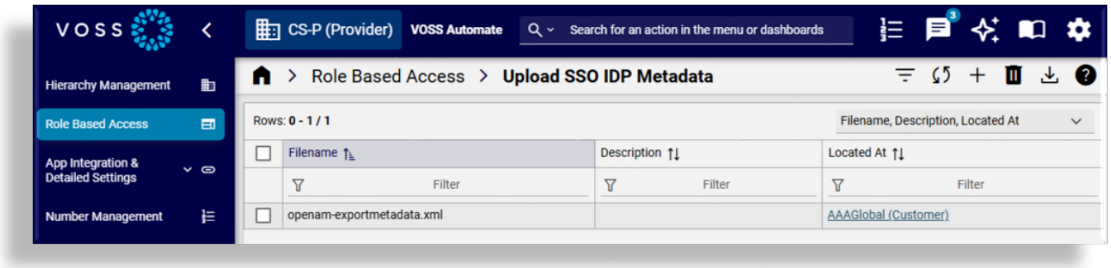
Update the metadata file on a SSO IdP entry

Tip: *Use the Action search to navigate Automate*

This procedure changes the metadata file on a SSO IdP (Identity Provider) entry.

Note: You'll need to update the metadata file if your SSO configuration changes.

1. Upload the updated SSO IdP metadata file:
   a. In the Admin portal, go to **Role Based Access**, then click **Upload SSO IDP Metadata** to open the list view for your SSO IdP metadata files.



Copyright © 2025 VisionOSS Limited. All rights reserved.

b. Click the Plus icon (+) to add a new record.

c. Click **Choose File** to upload the file from your local computer or a network location, and optionally, add a description.

Note: The metadata file must be unique across the system and must match the requirements for your SSO setup, including correct entity ID, UID attribute name, and other parameters.

---

d. Click **Save** to upload the file.

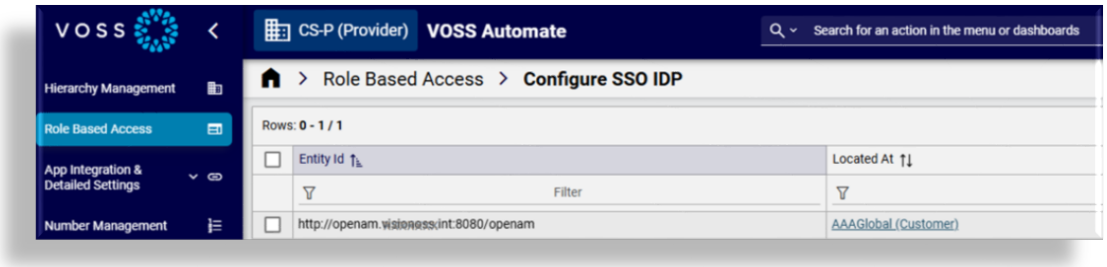
2. Change the metadata file on the IdP entry:

a. In the Admin portal, choose the relevant hierarchy.

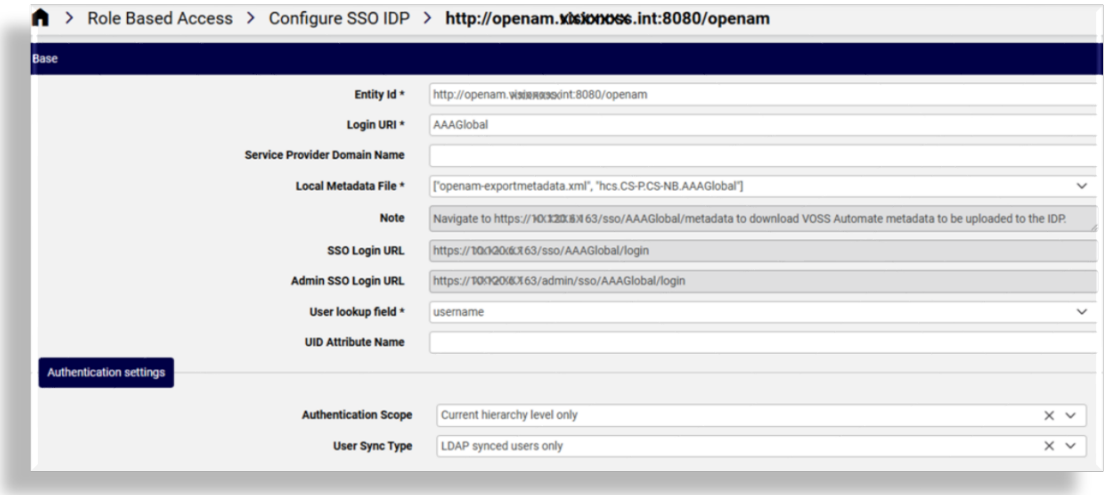
Note: Only one instance of an SSO IdP can be configured for a hierarchy node. While an IdP may exist at more than one hierarchy in Automate, a user will only be permitted to log in if the user exists at or below the hierarchy of a single IdP.

---

b. Go to **Configure SSO IDP** to open the configuration settings for the IdP entry where you're changing the metadata file.



c. Click on the IdP entry to open its configuration settings.



d. At **Local Metadata File**, select the updated metadata file from the drop-down.

e. Pay attention to the **Note** field, which displays an instruction for downloading the Automate metadata so that you can upload it to the IdP.

f. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Re-upload the Automate metadata to the IdP, if required:
   a. Remove previous metadata records from the IdP.
   b. Download the Automate metadata at the location specified in the **Note** field on the IdP configuration settings page, then upload it to the IdP.

   Note: If the Service Provider (SP) metadata has been updated (for example, due to a domain name or certificate change), download the updated SP metadata from the Automate system and upload it to the IdP to ensure that the IdP and SP configurations remain synchronized.

4. Verify the configuration:

   Test the SSO login URLs to ensure that the updated metadata file works as expected. The URLs typically include:

   - SSO Login URL: https://<FQDN of the Service Provider>/sso/<Login URI>/login
   - Admin Portal Login URL: https://<FQDN of the Service Provider>/admin/sso/<Login URI>/login

Related topics

- *Configure SSO IdP*

5.6.7. Upload SSO IDP Metadata

File management

Tip: *Use the Action search to navigate Automate*

Overview

The `data/File` model is associated with files and file management, for example, to upload SSO IdP metadata files.

For more information on models and Help, see *Conventions Used in this Guide* in the Core Feature Guide.

Automate allows you to add new files to the system, and if you have permissions for Move and Clone operations on your access profile, to clone (copy) files, and to move cloned files up or down in the hierarchy, for example, to move a cloned file from customer to site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Upload SSO IdP metadata*
- *Upload a certificate to use for app registration*

Upload SSO IdP metadata

Tip: *Use the Action search to navigate Automate*

This procedure uploads a SSO IdP metadata file so that you can add or change the metadata file on a SSO IdP entry. For example, you will need to replace the SSO IdP metadata file when your SSO configuration changes.

Note: The `data/File` model is associated with files and file management so you will use this model to upload SSO IdP metadata.

1. Go to **Upload SSO IdP Metadata**.
2. At **Filename**, click the Plus icon (+) to select the file to upload from a network location or your local computer.

   Note: The file must be unique across the system. The metadata file must match the requirements for your SSO setup, including correct entity ID, UID attribute name, and other parameters.

3. Optionally, add a description for the file.
4. Click the **Save** icon to upload the file.

Next steps

1. Re-upload metadata to the IdP, if required:

   If you're replacing a SSO IdP metadata file, update SSO IdP to change the metadata file to the new file. See *Configure SSO IdP*

   If the Service Provider (SP) metadata has been updated (for example, due to a domain name or certificate change), download the updated SP metadata from the Automate system and upload it to your IdP. This ensures that the IdP and SP configurations remain synchronized.

2. Remove previous metadata records (if applicable):

   If you've previously uploaded metadata to the IdP and have now added or changed the **Service Provider Domain Name** field or related configuration, you will need to remove the old record from the IdP. Then, re-upload the new metadata file containing the new information.

3. Verify the configuration:

   After uploading the new metadata file, ensure that all relevant configurations, such as URLs and attributes in the metadata file, align with the requirements of your IdP.

   Test the SSO login URLs to ensure that the updated metadata works as expected. The URLs typically include:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- SSO Login URL: https://<FQDN of the Service Provider>/sso/<Login URI>/login
- Admin Portal Login URL: https://<FQDN of the Service Provider>/admin/sso/<Login URI>/login

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. App Integration and Detailed Settings

6.1. Microsoft App Integration and Detailed Settings

6.1.1. Microsoft Overview

Introduction to Microsoft UC integration

Overview

This section introduces Microsoft Unified Communications (UC) integration with Automate.

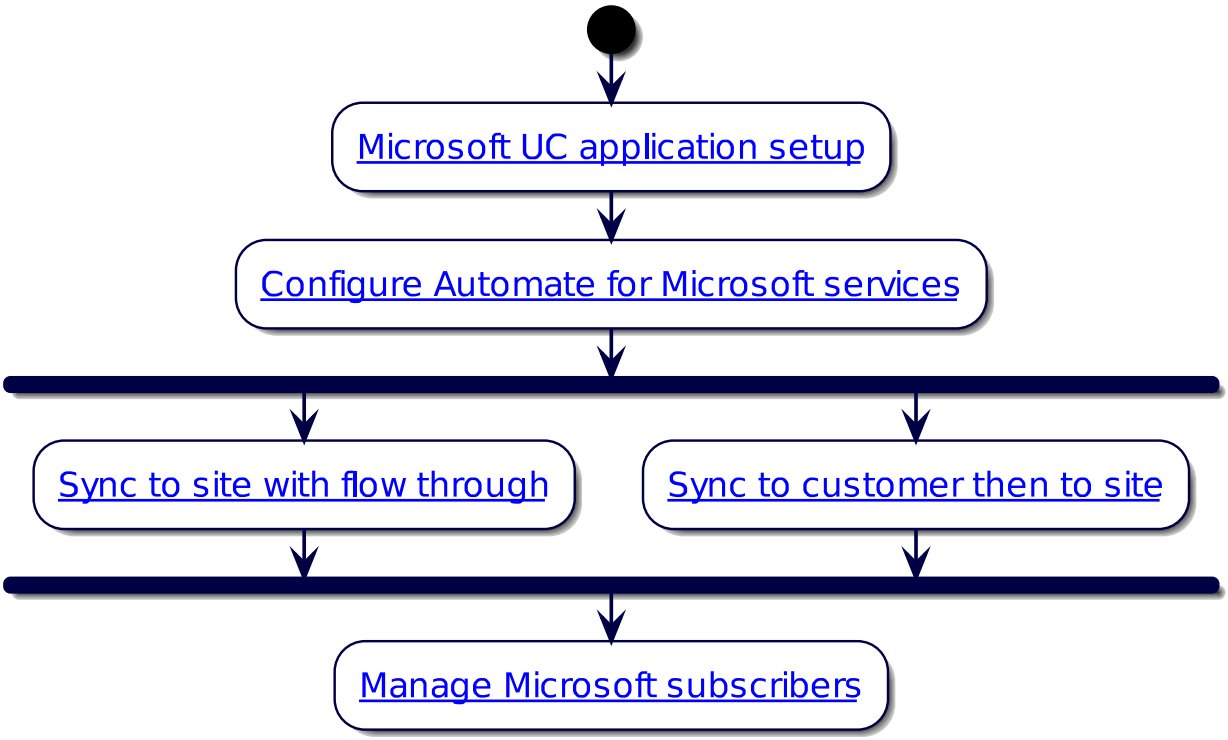
Automate provides an interface for managing Microsoft users and services, either as a stand-alone, Microsoft-only implementation, or as part of a multi vendor implementation.

Automate can be used to manage multiple applications within Microsoft's UC stack, including:

- Microsoft Entra ID
- Microsoft Teams
- Exchange Online
- On-premise Active Directory
- Skype for Business Server
- Exchange Server

The flowchart provides a high level workflow for the Microsoft solution in Automate.

Microsoft Overview Flowchart



Related topics

- *Microsoft Quick Start Guide for Automate*
- *Microsoft UC Application Setup*
- *Microsoft tenant setup*
- *Microsoft Licenses*
- *Introduction to Microsoft Teams dial plan management*
- *Configure Microsoft tenant dialplan*
- *Introduction to Microsoft Teams policies* in the Core Feature Guide
- *Overbuild for Microsoft*
- *Model filter criteria*
- *Flow through provisioning (FTP)*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Devices for Microsoft UC application setup

The following devices must be configured for Microsoft UC application setup (authentication, authorization, and PowerShell proxy):

- *Microsoft Graph API*
- *Windows PowerShell and PowerShell proxy servers*
- *Microsoft Teams*
- *Microsoft Exchange Online*

Microsoft Graph API

Automate communicates with Microsoft Entra using Microsoft Graph API. Registering Automate as an application object in Microsoft Entra provides authentication and authorization for Automate.

Microsoft Graph API offers:

- Simplicity
- No requirement for an intervening proxy
- Lower latency
- Secure authentication options
- Granular permissions management

As the Microsoft Graph API matures, Automate can easily be updated to leverage new Graph functionality - new templates can be added, and existing ones can be updated. Template updates can be deployed with no downtime or service impact.

Windows PowerShell and PowerShell proxy servers

Automate communicates with the Microsoft Teams Portal and Microsoft Exchange Online via PowerShell Proxy, allowing enforcement of authentication and authorization in two places:

- On the PowerShell proxy
- In the Microsoft 365 tenant

At least one Windows computer is needed as a PowerShell proxy server.

Automate manages Microsoft Teams and Microsoft Exchange Online via PowerShell proxy servers, which execute remote PowerShell cmdlets.

The table describes how PowerShell proxies may be used to manage on-premise or cloud-based applications:

On-premise apps	Join the PowerShell proxy server to the domain under management. If using Automate to manage multiple on-premises customer domains, add at least one domain-joined PowerShell proxy for each domain.
Cloud-based apps	Use a PowerShell proxy server to manage multiple Microsoft 365 tenants. A PowerShell proxy that manages only cloud-based applications can optionally be configured as a workgroup server.

Copyright © 2025 VisionOSS Limited. All rights reserved.

For Microsoft apps management, Automate uses Windows PowerShell to create separate PowerShell sessions via the PowerShell proxy servers for each application managed for a specific customer tenant or domain.

All PowerShell sessions for a customer can be hosted by the same PowerShell proxy server, or you can configure a separate server for each session. Optionally, these PowerShell proxy servers may be dedicated exclusively for this purpose.

The PowerShell proxy setup script that ships with Automate installs or updates PowerShell to the required version. Refer to *Run PowerShell proxy server setup script*

Microsoft Teams

Automate uses the PowerShell proxy server and the Microsoft Teams PowerShell module to manage settings for end users, services, device policies, and telephony in Microsoft Teams.

PowerShell scripts authenticate to Microsoft Teams through an *application registration*.

Basic authentication and credentials linked to a service account in the tenant are used to provision resource accounts in Microsoft Teams.

You must assign at minimum the following role to the service account used for managing Microsoft Teams:

Role	Description
Teams Administrator	Provides full access to all Microsoft Teams, manages service requests, and monitors service health. Use cases: • List MS Teams users • Retrieve Teams user identity, attributes, and assigned policies • Update MS Teams user attributes and assigned policies • Enable / disable Enterprise Voice for MS Teams users • Create, read, update and delete MS Teams policies • Create, read, update, and delete MS Teams Enterprise Voice configuration, including Voice Routing Policies, PSTN Usages, Voice Routes, PSTN Gateways, and Tenant Dialplans • Create, read, update, and delete MS Teams Call Queues and Teams Auto Attendants • Create, read, update, and delete MS Teams endpoints, including Teams Phones, Common Area Phones, Collaboration Bars, and Teams Rooms

Copyright © 2025 VisionOSS Limited. All rights reserved.

Microsoft Exchange Online

Automates uses the PowerShell proxy server and Microsoft's Exchange Online PowerShell module to manage user mailboxes, shared mailboxes, room mailboxes, and distribution groups in Microsoft Exchange Online.

Automate employs *app-only authentication* for Microsoft Exchange Online, requiring a certificate and private key installed on the PowerShell proxy.

For *app-only authentication*, you will need to create an X.509 certificate with a private key, then install the certificate and private key on the PowerShell proxy server. Automate can create this certificate for the Microsoft tenant setup, upload it to the PowerShell proxy server, install it, and update the thumbprint in the tenant data. The public key is exported from Automate and imported into Microsoft Entra.

The certificate can also be imported from the customer into Automate.

During the registration of the Automate application object with Microsoft Entra, upload the certificate (public key only), assign Exchange Online API permissions, and an appropriate RBAC role to the application:

- Automate requires the following Microsoft Entra permission: `Exchange.ManageAsApp`

  This permission allows a registered application to access Exchange Online resources.

- Automate requires the following role-based access control (RBAC) role: `Exchange Administrator`

  Users with this role have global permissions within Microsoft Exchange Online and can create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.

Note: For custom administrator user roles, ensure the associated access profile (access profile type `device/msexchangeonline/*`) allows for all operations on all Microsoft Exchange models.

Related topics

- *Access profile permissions and operations*
- App-only authentication | Microsoft Docs.

PowerShell proxy deployment topologies

PowerShell proxy server domain membership

PowerShell proxy servers may be joined to a Microsoft Entra domain.

Domain membership is required if you're using Automate to manage or extract data from any on-premises component, such as Skype for Business Server, on-premises Microsoft Entra, or on-premises Exchange Server.

Domain membership is optional in all other scenarios.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Redundancy and load-balancing

Deploying two or more PowerShell proxy servers provides redundancy. PowerShell proxy servers can be scaled and made highly available by interposing a load balancer between Automate and the PowerShell proxy servers.

Load balancer requirements

The load balancer:

- Must forward incoming HTTP and HTTPS requests on TCP ports 5985 and 5986
- Must forward incoming SSH/SCP requests on TCP port 22
- Must be configured in “IP Affinity” mode so that all incoming requests from a specific IP address are preferentially routed to the same PowerShell proxy. This is done to maintain the integrity of HTTP sessions that can consist of multiple HTTP requests.

When deploying Automate as a multi-node cluster and the load balancer is configured in “IP Affinity” mode, each unified node will have all its requests routed to the same PowerShell proxy.

A properly configured load balancer will distribute the overall load from all the unified nodes across the deployed PowerShell proxy servers. When a PowerShell proxy goes out of service the load balancer will route incoming traffic to the surviving servers, bypassing the failed one.

Setting up load balancing for a multi-proxy deployment setup

If leveraging redundant PowerShell proxies behind a load balancer, updates of the app registration authentication certificate or future modules pushed by Automate to the PowerShell proxies, requires additional steps:

1. In the Microsoft tenant configuration, set the PowerShell proxy address directly to the first PowerShell proxy and select the updated certificate.
2. Save the configuration.
3. Confirm the update and connection works via the first proxy with a test connection via the transaction log.
4. Return to the tenant configuration, set the second proxy address, and save the configuration.
5. Confirm the update and connection works via the second proxy with a test connection via the transaction log.
6. Repeat with any additional proxies.
7. Once all proxies are confirmed as updated and functional, return the PowerShell proxy address to the load balancer’s FQDN, and save the configuration.
8. Test the connection.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Outbound Internet Proxy

Some organizations require all traffic outbound to the public Internet (including traffic to Microsoft 365 tenants) to traverse an outbound Internet proxy server for audit logging and, optionally, authentication.

Microsoft Entra

Automate uses the Microsoft Graph API at https://graph.microsoft.com over TCP port 443 to interact with Microsoft Entra.

Microsoft's application registration process provides authentication and authorization services for Automate.

You can configure the permissions granted to the Automate application based on the management use cases for which Automate has been designated. For example, you can grant permission to Automate to manage end user license assignments, or you can withhold that permission (in which case Automate will only be able to view existing license assignments, limiting the Automate workflows available to you).

Microsoft UC Application Setup

Microsoft

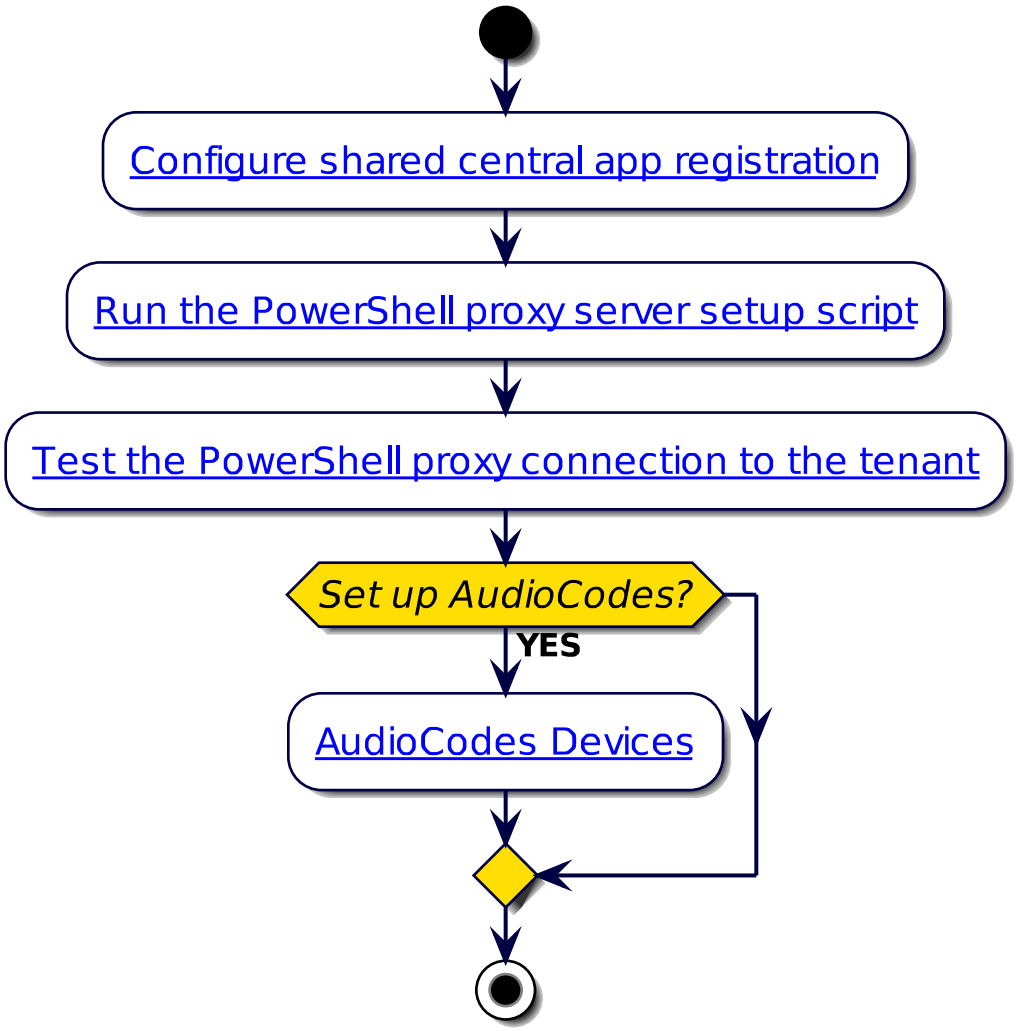
Overview

To manage and provision Microsoft applications, Automate must be able to authenticate with Microsoft Entra, one or more PowerShell proxy servers, Microsoft Teams, and Microsoft Exchange Online.

This step sets up the authentication between MS 365, MS Teams, and Automate, and sets up the PowerShell proxy server.

Some of the details generated during this setup (for example, the client/application ID) is used in VOSS Automate to configure the Microsoft tenant connection parameters.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: For details around the URLs, ports, and protocols that Automate uses to connect to the PowerShell proxy and the Microsoft 365 tenant, and which the PowerShell proxy uses to connect to the tenant, see:

"Network Communications External to the Cluster" in the VOSS Automate Installation Guide or Platform Guide.

Related Topics

- *Microsoft Quick Start Guide for Automate*
- *Shared central app registration*
- *Run PowerShell proxy server setup script*
- *Test the PowerShell proxy connection to the tenant*
- *AudioCodes Devices*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Run PowerShell proxy server setup script

Overview

Automate ships with a PowerShell Proxy setup script to automate the setup of the Windows PowerShell proxy server for for Microsoft Teams and (optionally) Microsoft Exchange Online.

Note: The PowerShell proxy setup script automatically installs or upgrades the required modules of Microsoft Teams and Exchange modules, and performs other setup steps, such as installing OpenSSH on the PowerShell Proxy. You can run the script on a new PowerShell proxy server, or use an existing one. A single PowerShell server can be used by multiple tenants, with or without Microsoft Exchange.

Pre-requisites

- Download the script and associated files from the client portal: https://voss.portalshape.com

  Note: Release and file versions displayed here may differ, depending on your target release. The script uses the associated files during install.

  Go to: **Downloads > VOSS Automate > [your target release] > Windows Powershell Proxy**.

  The directory contains a `.ps1` file and additional required files (such as .NET framework and PowerShell modules).

  Download all the available files and extract `.zip` files.
- Ensure you have the supported Microsoft Server operating system version for use as a Windows Proxy. Refer to the Microsoft Windows Server version for your target release in the Compatibility Matrix.
- You must have local Administrator privileges on the PowerShell proxy server.

Execute the script

This procedure runs the `.ps1` script.

1. Transfer the downloaded `.ps1` script and files to the Microsoft PowerShell proxy server.
2. On the Windows server, run the script as an Administrator.
3. **Are you using a currently active service user account, or do you need to create one**?
   - **Using a currently active service user account**. Press **Enter** to proceed.
   - **Creating a new service user account**. Fill out the name you want to use for the service user account that will be created, then press **Enter** to proceed.

   Note: If you don't provide a service user account name, the script uses the currently active user account.

4. Fill out a password for the service user account to be assigned. If you're using the current service user account, fill out the password for that user.
5. Press **Enter**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. **Are you using an outbound internet proxy**?
   - **Yes**. Fill out the proxy server IP/FQDN and port in the following format: `xxx.xxx.xxx.xxx:yyyy` (for example, `192.168.1.1:3128`)
   - **No**. Leave the field blank.
7. Press **Enter**.

   The script executes, performing the following steps:

   Note: This script uses local files to install all required PowerShell modules so that an internet connection won't be required to execute it. The files must be downloaded from the VOSS client portal and placed in the same folder as the script before executing.

   - Checks that the local admin service account is present
   - Configures the outbound internet proxy
   - Configures WinRM (Windows Remote Management service)
   - Installs/updates .NET framework
   - Installs/updates PowerShell modules
   - Checks that OpenSSH server is enabled and running
   - Checks that the privileged scheduled task is present
   - Checks that debug tools are present
   - Installs PowerShell

   Sample output (your output may differ):

```
The service account must be in the "Log on as a batch job" local security policy in␣
↪order to be
allowed to run the scheduled task. Administrator is not allowed to log on as a␣
↪batch job. Adding to the
policy. Administrator has been added to the log on as a batch job policy.
Creating VOSS folder and initializing script for scheduled tasks to run.

[...]

Creating new task RunPowershellScriptWithElevatedPermissions to run as Administrator.
↪..
Privileged scheduled task RunPowershellScriptWithElevatedPermissions created and␣
↪configured.
Creating new task RunPowershellScriptWithElevatedPermissionsPS7 to run as␣
↪Administrator...
Privileged scheduled task RunPowershellScriptWithElevatedPermissionsPS7 created and␣
↪configured.
Do you want to install or update the .NET framework? (y/n) y
Input: y
Installing/updating .NET framework...
.NET Framework 4.8 is already installed.
Do you want to install or update the Teams Powershell module? (y/n) y
Input: y
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
Installing/updating Teams Powershell module...
Successfully installed version 7.0.0 of the MicrosoftTeams Powershell module.

[...]

Do you want to configure security protocols? (y/n) y
Input: y
Configuring security protocols...
TLS 1.3 has been enabled.
TLS 1.2 has been enabled.
TLS 1.2 for .NET 4.x has been enabled.
TLS 1.2 for .NET 3.5 has been enabled.
TLS 1.0 has been disabled.
TLS 1.1 has been disabled.
You must restart the Windows Server for the changes to take effect.

[...]
```

8. Restart the Windows server for the changes to take effect.
9. After the server has restarted, run the script again to configure MS Exchange.

   On the second run:

   - Choose Exchange
   - Fill out a different user name as service account

   Note: No further input should be required. However, check the prompts carefully to verify.

Related topics

See Microsoft Quick Start Step 1 in the Core Feature Guide.

Configure Automate for Microsoft services

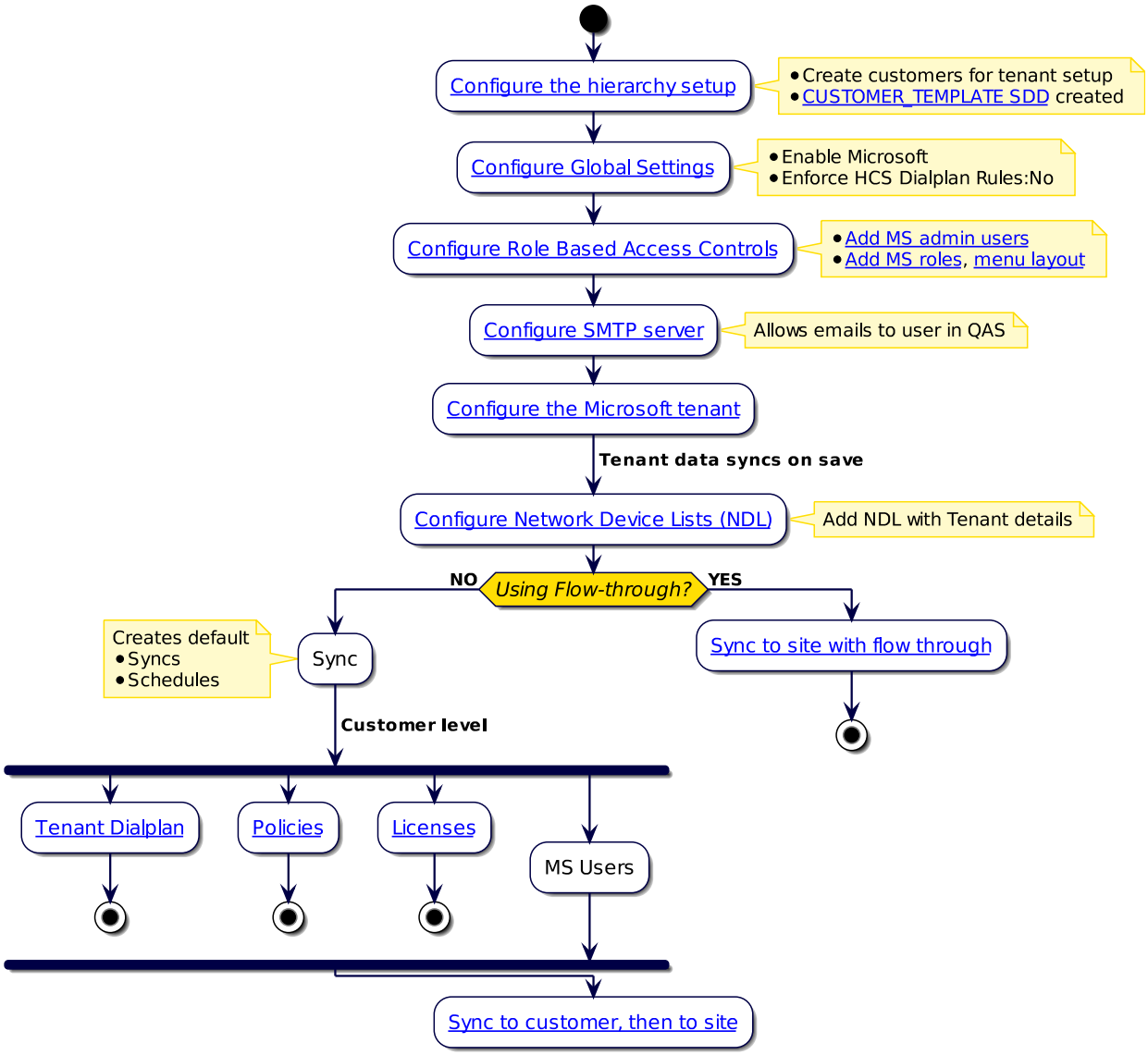
Overview

When using Automate with Microsoft (as a single or multiple vendor deployment scenario), you'll need to configure several settings in Automate before importing Microsoft users, licenses, policies, and dialplans.

Note: For details on the generic flow through provisioning feature (which includes Microsoft, LDAP, or CUCM users), see *Flow through provisioning (FTP)*

The flowchart sets out the initial configuration of Automate for Microsoft services.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- Microsoft overview in the Core Feature Guide
- Sync to site with flow through provisioning in the Core Feature Guide
- *Sync to customer, then to site*
- *Flow through provisioning (FTP)*
- *Onboard user (Microsoft)*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate configuration and sync workflow steps

This procedure describes the high-level workflow for configuring Automate for Microsoft services and for syncing in users, licenses, policies, and dialplans.

Prerequisites

- *Step 1: Microsoft UC Application Setup*
- Consider whether you want to *Prevent duplicate numbers*

1. Log in to the Admin portal as provider admin.
2. Configure the hierarchy to add customers for the tenant setup.
3. In the Global Settings, enable Microsoft, and disable *Enable HCS Dialplan Rules*.
   - In **Global Settings**, **Enabled Services** tab, enable Microsoft.
   - If you have a Microsoft-only environment, on the **Number Inventory** tab, set the following to *No* (False): **Enforce HCS Dialplan Rules**

   Note: HSC dialplan is relevant only when using Cisco (in a single vendor or multi vendor installation).

4. Configure role-based access controls to apply to users on import (add Microsoft admin users, roles, and menu layouts).
   - Add an admin user. See *Add admin user*.
   - Configure menu layouts, See *Add or edit a menu layout*.
   - Add user roles, and choose menu layouts for the roles. See *Role Management*.

   Note: Automate allows an admin user to set up pre-defined role-based configuration, which will be applied to users on import. This allows users to be auto-provisioned on import, with the correct services, lines, policies, and licenses.

   When preparing for import, you'll need to create the admin users, service profiles, user roles, and role-based menu layouts (to hide or display functionality for different categories of users). For example, you can assign a Microsoft-only user role (`MicrosoftOnlyRole`) in a Microsoft-only scenario.

5. Configure the SMTP server to allow emails to users (if required). See *Add a SMTP Server*.
6. Configure the Microsoft tenant, one for each customer. See *Microsoft tenant setup*

   Note: The tenant configuration defines how Automate connects to the Microsoft Cloud to allow syncing of data between Automate and Microsoft Azure, Microsoft 365, Microsoft Teams, and Microsoft Exchange. Saving the tenant creates the default syncs and schedules.

7. Configure network device lists (NDLs). You'll add Microsoft tenant details to the NDLs. NDLs are required for creating sites. See *Network device lists (NDLs)*
8. Sync in Microsoft users.
   - Go to the tenant configuration screen, then, choose a sync option:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Click **Action > Sync All** to run a full pull sync (syncs in the tenant dialplan, policies, licenses, and Microsoft users to the customer level).
- Click **Action > Sync New Users** to sync in new or updated users *only* (add new users, or update existing users).

  For **Sync New Users**:

  New users are synced in for the following models:

  * `device/msgraph/MsolUser`
  * `device/msteamsonline/CsOnlineUser`
  * `device/msteamsonline/ApplicationInstance`

  Existing users are updated (add, modify, delete) for the following models:

  * `device/msgraph/MsolUser`
  * `device/msteamsonline/CsOnlineUser`

Note:

- If you're using flow through provisioning for Microsoft users, additional steps are required before running the initial sync. See *Sync to site with flow through provisioning*

  You will need to enable the *Sync New Users* sync method initially (if you've upgraded to 21.3-PB1). To do this, save the tenant instance on this screen first so that the necessary data sync instances are created. These data syncs can be identified by the name format: `SyncMSTeamsOnlineUsers__<tenant>`, with **Update** and **Remove** operations disabled by default.
- Automate issues a warning when it detects an `in` condition for `UserPrincipalName` used alongside other `CsOnlineUser` filters during sync and filtering. In Microsoft tenants with auto-filter enabled, the expected records may not be returned if your MsolUser cache is not up to date. See "Microsoft syncs" in the Best Practices Guide.

Next steps

- *Step 3: Sync Microsoft Users to Sites*

Related topics

- *Microsoft tenant setup*
- Microsoft syncs in the Best Practices Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Shared central app registration

Introduction

This topic describes how to set up shared central application (app) registration authentication for Microsoft Graph, Microsoft Teams PowerShell, and Microsoft Exchange PowerShell, for a new Microsoft tenant. This task includes assigning permissions and roles.

Your authentication methods and permissions come from the central app registration. Roles must assigned to the app registration manually.

When adding a new tenant and you wish to use Microsoft Exchange, you must either generate a certificate or import an existing certificate and have Automate manage it. Automate pushes the certificate to the PowerShell proxy.

- To generate a certificate in Automate, see *Generate a certificate for application registration*
- To use an existing certificate, see *Upload a certificate to use for app registration*

Note: Microsoft requires that you use app registration for authentication. If you wish to use basic authentication with service account credentials, please contact VOSS support for assistance. Until Microsoft implements changes to their resource account infrastructure, basic auth is required to create, update, and delete resource accounts. List (import/sync) of resource accounts is supported with app registration authentication in Automate 24.1.

About shared central app registration

In shared central app registration, either VOSS (for hosted and general customers) or a Service Provider Partner (in a reseller environment), builds and maintains the app registration in their Microsoft Entra ID tenant, and performs organizational and application validation with Microsoft.

Users from multiple tenants/Entra ID organizations are allowed to leverage the application.

VOSS or the Service Provider Partner (SPP) provides the customer with an admin grant link, for example, `https://login.microsoftonline.com/common/adminconsent?client_id={client-id}`.

The customer clicks on the link and agrees, using their Global Admin user. Then they need to assign the Teams and Exchange Administrator roles to the application, like any other user in Entra ID.

VOSS or the SPP maintains the certificate and/or secrets securely, and ensures that they're added to VOSS when renewal is required.

Once updated, PowerShell proxies automatically receive the updated certificates from Automate. These settings are maintained at a global or reseller level in Automate, with customer/tenant-level overrides, if required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure shared central app registration

This procedure configures Central App Auth and assigns the Teams Administrator role and the Exchange Administrator role (if you're using MS Exchange) to the app.

1. Authorize the app in the relevant Microsoft tenant to add Central App to your tenant (VOSS hosted app):

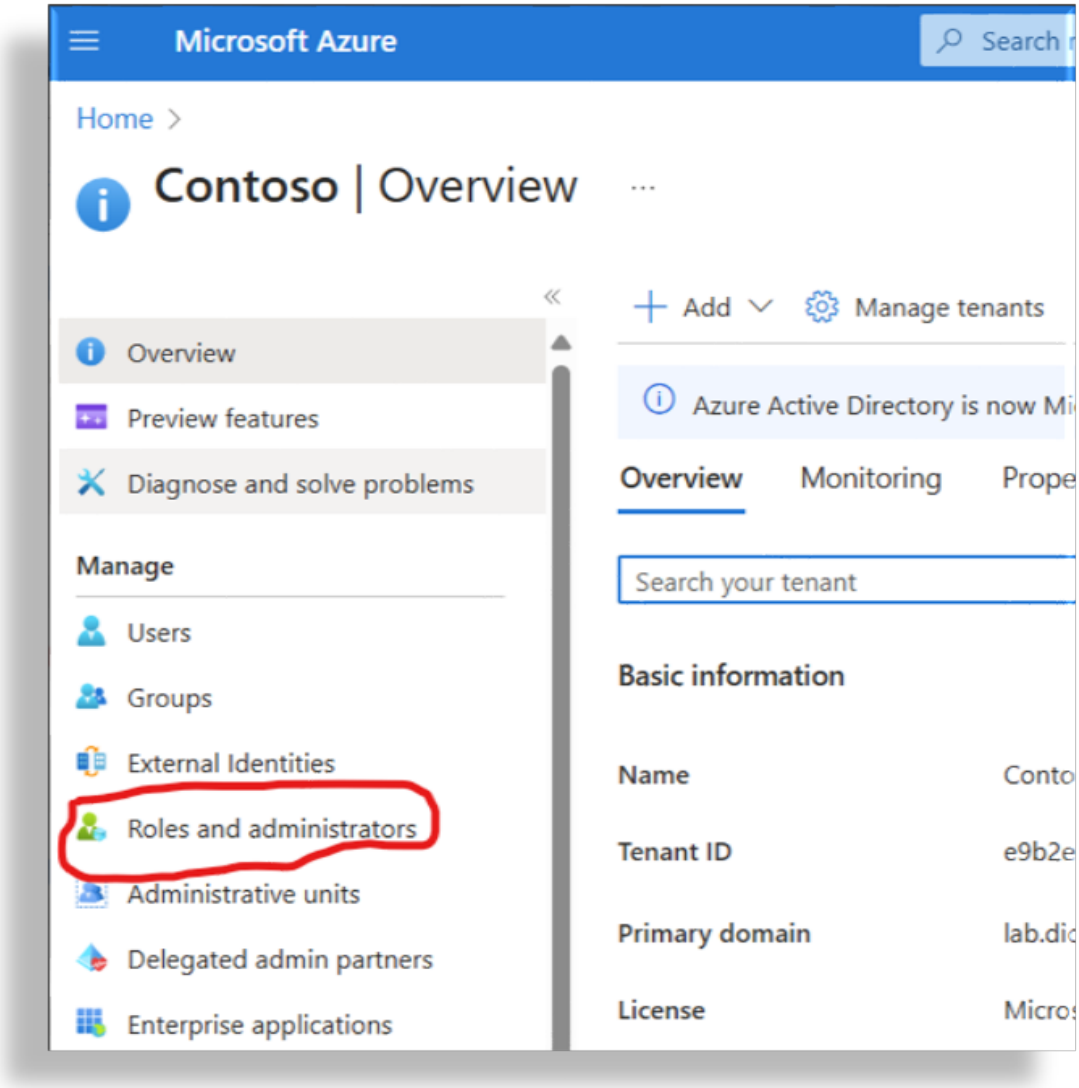
   `https://login.microsoftonline.com/common/adminconsent?client_id=bbaa714a-a571-4d13-a6e1-4758621b746`

2. Assign the *Teams Administrator* role and the *Exchange Administrator* role to the app:

   a. Go to the **Entra ID** section of the Microsoft Azure Portal:

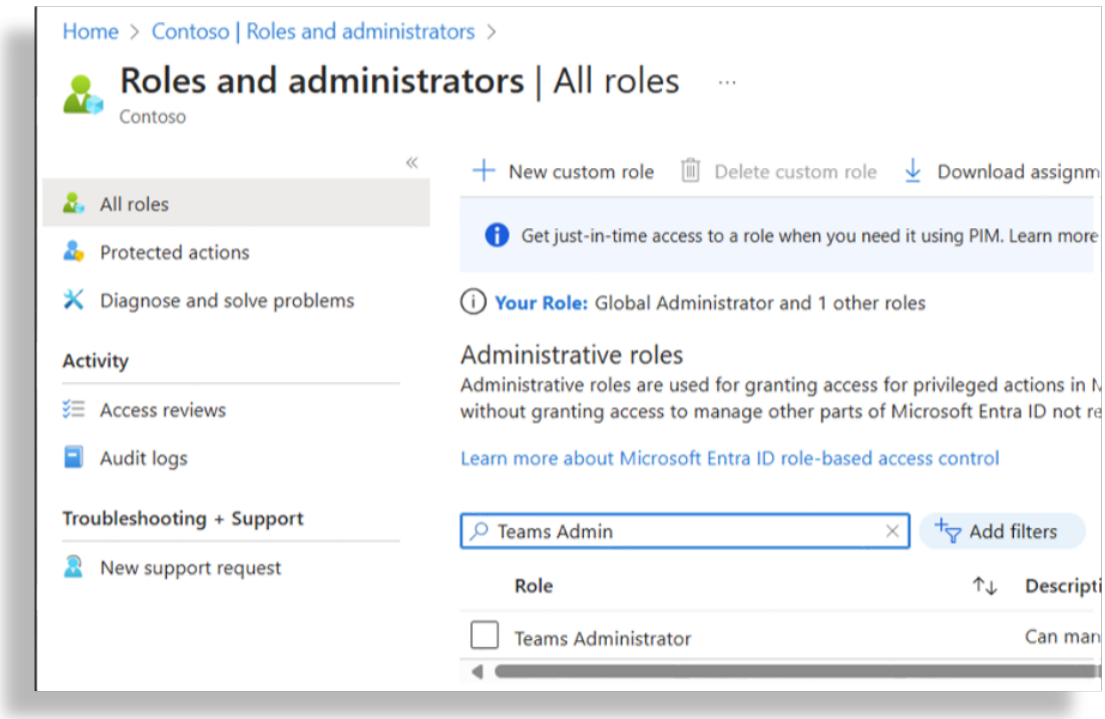
   `https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview`

   b. Navigate to **Roles & Administrators**.

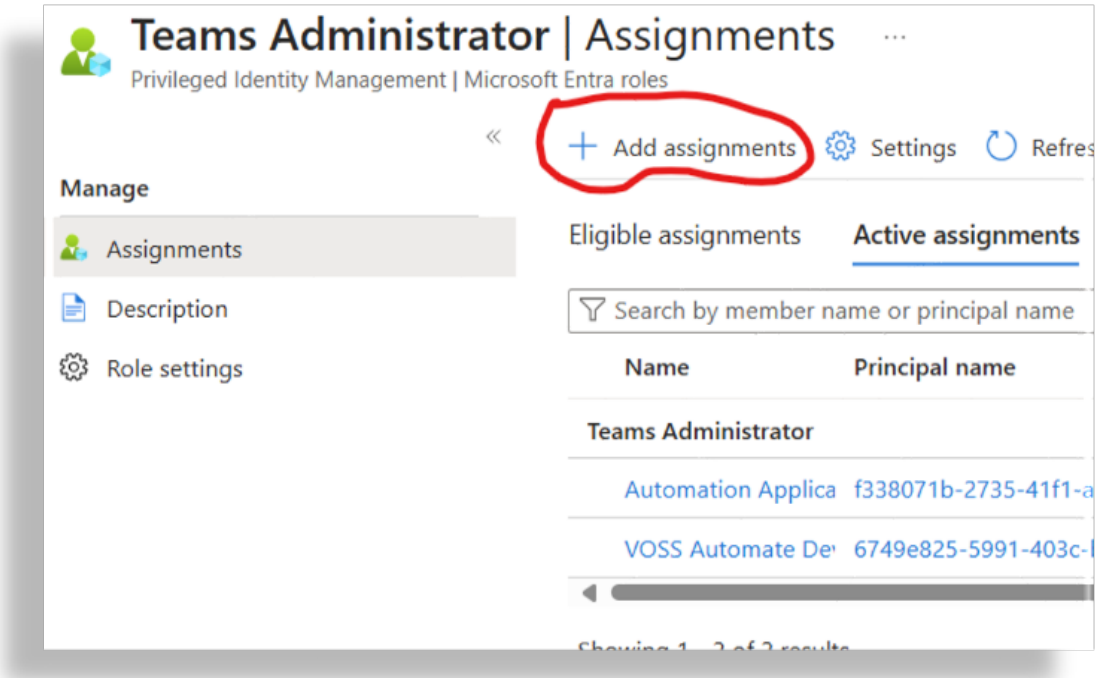


   c. Search for *Teams Administrator*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

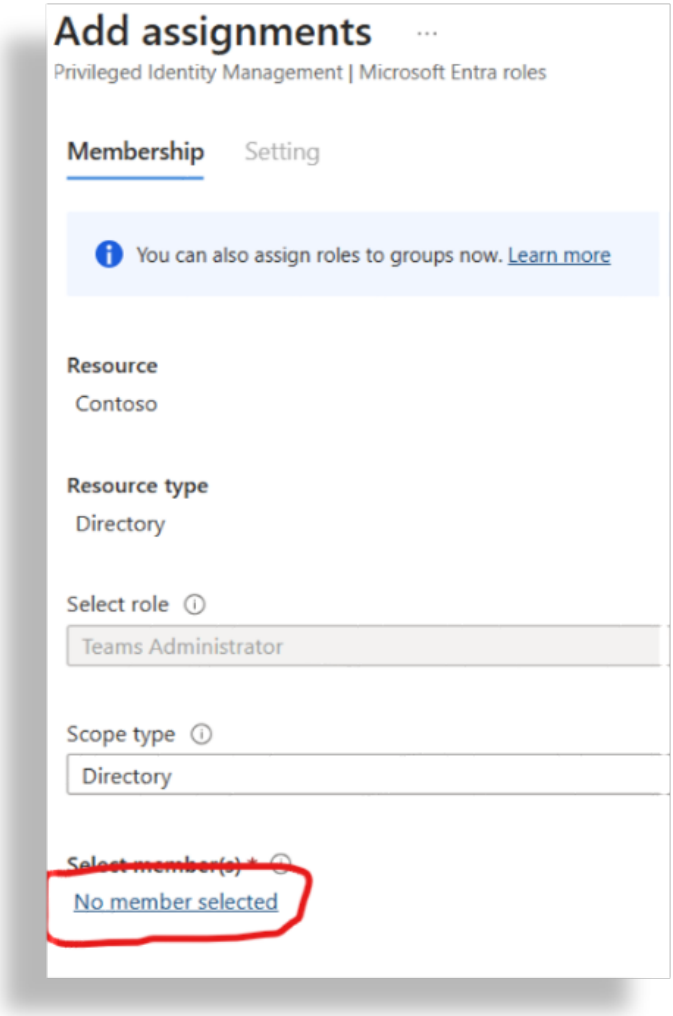


d. Open **Teams Administrator**, then click **Add Assignments**.

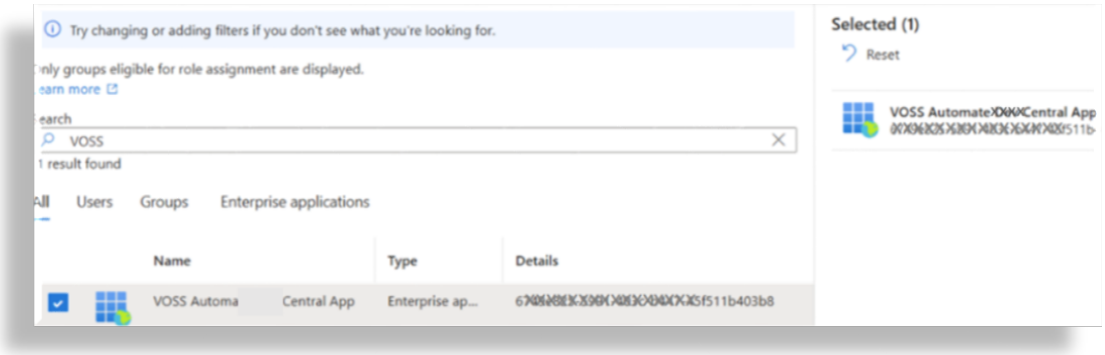


e. Select **No member selected**.

Copyright © 2025 VisionOSS Limited. All rights reserved.



f. Search for *VOSS*, then select the checkbox for **VOSS Automate App**.

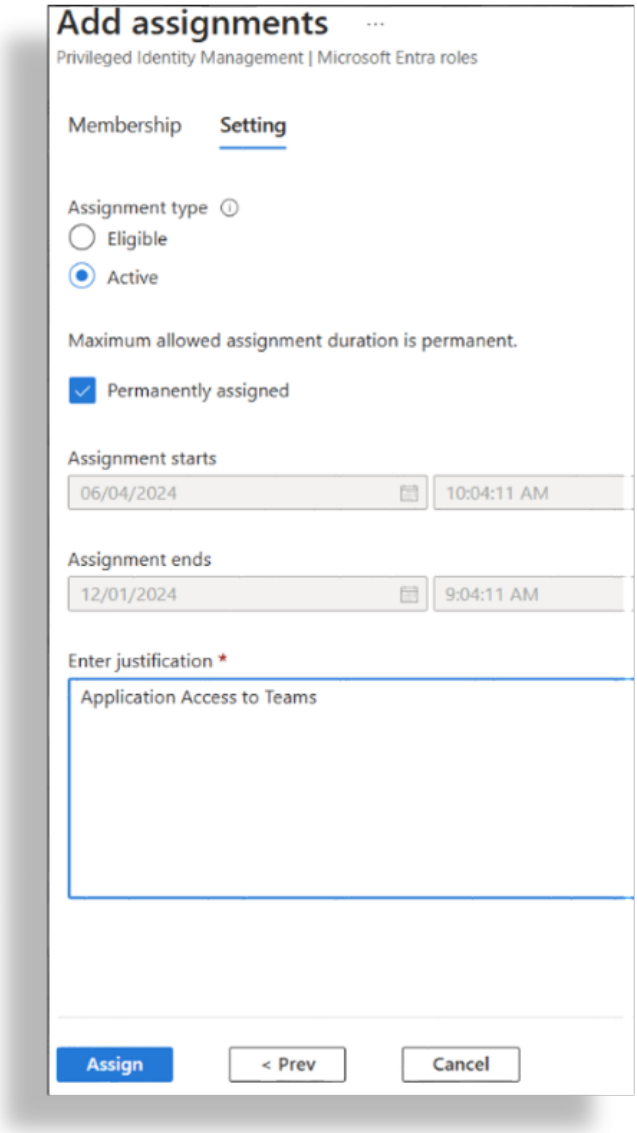


g. Click **Next**.

h. At **Enter justification**, fill out a reason for the assignment in the text field.

Note: You can add any description in this field.

Copyright © 2025 VisionOSS Limited. All rights reserved.



i. Click **Assign**.

   The new assignment may take a few minutes to complete before it appears in the assignment list (**Teams Administrator | Assignments**).

j. Repeat step 2 from the **Teams Administrator | Assignments** page, but this time, on **Teams Administrator | Assignments**, search for the **Exchange Administrator** role.

3. Install the certificate on the Automate server.

Note: If you're using VOSS (hosted) Central App, the "Default Central App Authentication" certificate is already installed.

You can replace this certificate with a new PFX file that replaces an expired certificate/key pair when the certificate expires. When upgrading, the "Default Central App Authentication" certificate is automatically updated.

---

4. Configure the Automate Microsoft tenant to use the "customer" Tenant ID you approved for earlier,

Copyright © 2025 VisionOSS Limited. All rights reserved.

along with the App ID (Client ID) and certificate as necessary.

For example, for VOSS Central App customers:

- App Name: VOSS Automate Central App
- Client Id: bbaa714a-a571-4d13-a6e1-4758621b7460
- App Created Date Time: 6/4/2024 3:24:31 PM
- CertificateThumbprint : 2BF36F11BE9317C9217BE6847BEDXXXXXXXXXXX

Upload a certificate to use for app registration

Microsoft

Tip: *Use the Action search to navigate Automate*

This procedure uploads a *.PFX* file into Automate so that it can be used for application registration.

Note: Certificates are required for authentication. Although you can generate a certificate in Automate and upload that certificate to Microsoft Entra. In some cases, customers prefer to use their own certificate. Once the certificate is uploaded to Automate, Automate can manage it on itself and on the PowerShell proxy.

1. In the Automate Admin Portal, choose the relevant customer hierarchy, then go to **File Management**.
2. Click the Plus icon (+) to add a new record.

3. Click **Choose File**, then browse to the location where you have the file stored on your computer or network.

   Note: The file you're adding **must** be a *.PFX* file that is signed and has the required encryption.

5. Optionally, add a description, then click **Save**.
6. Choose the relevant customer, then go to **Certificate Management**, and click the Plus icon (+) to add a new record.
7. Add the new certificate, using the *.PFX* file you added:
   - Add a name and a description.
   - At **PFX File**, in the drop-down, select the *.PFX* file you uploaded.
   - Add the PFX file password.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: This is the password that is generated when converting the certificate into *.PFX* format outside of Automate.

- Save your changes.

Automate creates the certificate file and deletes the *.PFX* file from Automate. The certificate will now be available to use in the tenant for application registration. See *Configure Microsoft Tenant Connection Parameters* in the Core Feature Guide.

There is no need to upload this certificate into Microsoft Entra because this certificate already exists there. If your certificate does not yet exist in Microsoft Entra, you'll need to export the public key via the **Certificate Management** page, then upload the certificate into Automate in order to use it in the tenant connection parameters.

Related topics

- *Cisco UCM Music on Hold (MOH) file management*
- *Upload SSO IdP metadata*
- *Upload a certificate to use for app registration*
- *File management*

Test the PowerShell proxy connection to the tenant

Test the connection from PowerShell to Microsoft Teams

This procedure tests the connection to Microsoft Teams from a non-privileged PowerShell session.

1. From a PowerShell session, configure a test session for an outbound Internet proxy (if your PowerShell Proxy server is behind an outbound Internet proxy that requires authentication):

```
$w = New-Object System.Net.WebClient

$w.Proxy.Credentials = (Get-Credential) (when prompted, enter your
outbound proxy credentials)
```

Note: The credentials you enter above persist only for the duration of this PowerShell session, and are deleted when you exit the PowerShell session.

See the caveat regarding proxy authentication, at: *PowerShell proxy deployment topologies*

2. Verify the version you're using, (e.g. 6.1.0):

```
Get-Module -ListAvailable -Name MicrosoftTeams
```

3. Issue the following command to test the connection to Microsoft Teams and to perform a test query, and when prompted, you'll need to enter your MS Teams service account credentials:

```
Connect-MicrosoftTeams -Credential (Get-Credential)
Get-CsOnlineUser -ResultSize 1 | Select DisplayName
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Perform step 1 first if your PowerShell Proxy is behind an outbound Internet proxy that requires authentication.

4. Verify that you have successfully connected to the tenant and retrieved one random user.

Related topics

- *Microsoft Quick Start Guide for Automate*

(Optional - Exchange Online only) Test the connection from PowerShell to Microsoft Exchange

1. Use the following command to test the connection:

```
Connect-ExchangeOnline -CertificateThumbPrint <certificate_thumbprint> -AppID
↪<client_id> -Organization $online_admin_domain
```

Note: You will use your `certificate_thumbprint`, `client_id` and `online_admin_domain`, as in the following example:

```
Connect-ExchangeOnline -CertificateThumbPrint␣
↪A2DEF024C59B4969A30A8892F832F418DF09F6 -AppID 5ff3dc33-c8db-48ba-b86e-
↪642d84d42ae0 -Organization VossSolutionsO365.onmicrosoft.com
```

2. Use the following command, then confirm that you can see a user mailbox:

```
Get-EXOMailbox -ResultSize 1
```

Related topics

- *Microsoft Quick Start Guide for Automate*

Sync in Azure users

Overview

Users are synced in from Azure once you've set up the Microsoft UC applications (including PowerShell). Next, you'll need to configure the Microsoft tenant connection parameters.

When using Microsoft to manage UC provisioning, you will need a number of different portals in a tenant:

- Azure
- Microsoft 355 Admin Center
- A portal on the Microsoft Teams side for telephony (once users are licensed through Microsoft Office 365)
- Optionally, you can also add MS Exchange to the tenant

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate combines these functions into a single management interface, allowing service providers to import data from multiple Microsoft tenants and to manage these customers (or tenants) from a single portal and login.

The diagram describes the initial configuration required to integrate Microsoft with VOSS Automate:

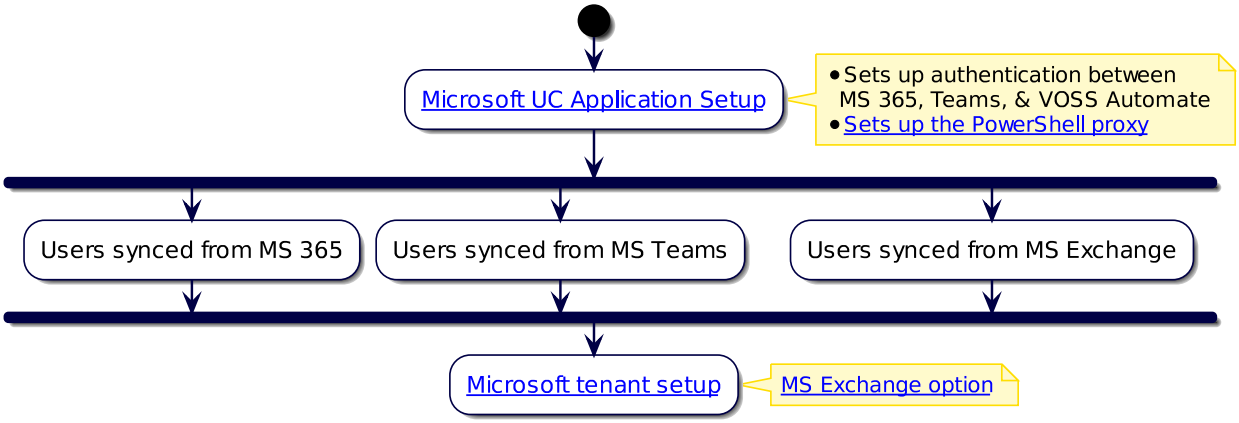
- You'll need to install and configure one or more Microsoft Windows PowerShell Proxy servers. This allows Automate to access Azure via the PowerShell. For details, see *Run PowerShell proxy server setup script*
- Once you've installed the Microsoft Windows PowerShell service, you'll use the IP address and credentials of the proxy server to configure the Microsoft tenant.

Next steps

Configure Automate for Microsoft Services in the Core Feature Guide

Workflow

The flowchart sets out the workflow to sync in Azure users.



Sync Microsoft users to sites

Overview

When setting up Automate for Microsoft, the final step involves syncing in Microsoft users.

Note: Syncing Microsoft users to sites is the final step for integrating Automate with Microsoft. For the other steps, see *Microsoft Quick Start Guide for Automate*.

You can choose to either directly sync in the tenant dialplan, policies, licenses and Microsoft users to the customer, or configure sync with flow through provisioning before syncing in Microsoft data and users:

Note: If you're syncing in users with a number that already exists at a site, by default, the system creates a duplicate of the number. To prevent duplicate numbers in the number inventory, enable the following global settings: *Prevent duplicate numbers*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *Sync to customer, then to site*
- *Sync to site with flow through provisioning*

The table compares the two sync types for Microsoft data and users.

Sync to customer, then to site	Sync to site, with flow through provisioning
Sync users to customer level, and then to sites schedules. **Step 1**: Run a full pull sync to create default syncs and schedules, and move all of the following to the customer level: • Tenant dialplan • Policies • Licenses • Microsoft users **Step 2**: Configuration for moving users to sites: • Configure model filter criteria (for overbuild) • Enable overbuild in the site defaults • Configure Quick Add Groups • Configure user profile • If using Microsoft Enterprise Voice, configure internal number inventory for sites **Step 3**: Two options for moving users to sites: • Run overbuild to move two or more users (batch) • Else, run Quick User to move a single user to a site	Configure Automate to sync in Microsoft users as fully provisioned, directly to the sites. **Step 1**: Configure the following: • Model filter criteria • Site defaults • Quick Add Groups • User profile • Configure the Microsoft tenant • Flow through provisioning criteria • Global settings (enable flow through) **Step 2**: Run a sync to create default syncs and schedules. • The sync creates default syncs and schedules, and syncs in the following to the customer: – Tenant dialplan – Policies – Licenses • Syncs in Microsoft users as fully provisioned users, to the sites.

Note: See *Onboard user (Microsoft)* for details around setting up Automate for managing licenses via a configuration template and Quick Add Groups or User from Profile or field display policies (FDPs).

Sync to customer, then to site

This section provides a worfklow overview for moving Microsoft users to the sites once the Microsoft tenant has been added and a full pull sync has been performed. The sync imports the tenant dialplan, policies, licenses, and Microsoft users to the customer level. Now users must be provisioned and moved to the appropriate sites.

Note: Use these steps if you chose not to sync users directly to sites (in a sync with flow through after setting up the NDLs).

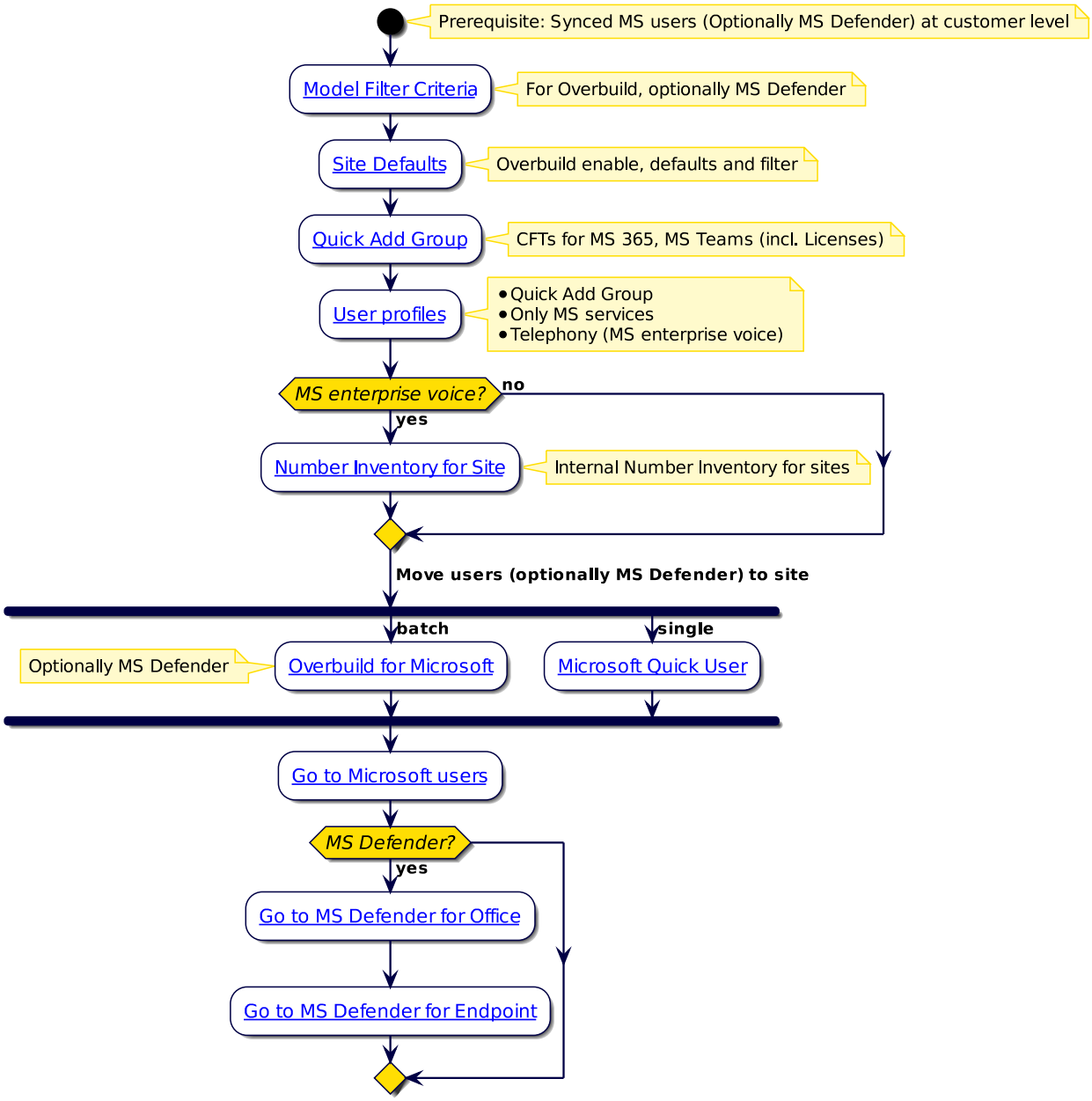
Copyright © 2025 VisionOSS Limited. All rights reserved.

Prerequisites:

- *Configure Automate for Microsoft services*

Workflow to sync to customer then to site

The flowchart sets out the steps to move Microsoft users to the sites after an initial sync to move users to the customer level:



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Introduction to Microsoft UC integration*
- *Sync to site with flow through provisioning*

Sync to site with flow through provisioning

When using sync with flow through provisioning for Microsoft users, you'll need to configure several settings in Automate (including flow through provisioning criteria) before the initial sync from the Microsoft Cloud. This allows Automate to apply the correct configuration, licenses, policies, and services to imported users, and to move users to sites.

Once you run the sync, the tenant dialplans, policies, and licenses are imported to the customer level, while users are imported, provisioned, licensed, and moved to the correct sites.

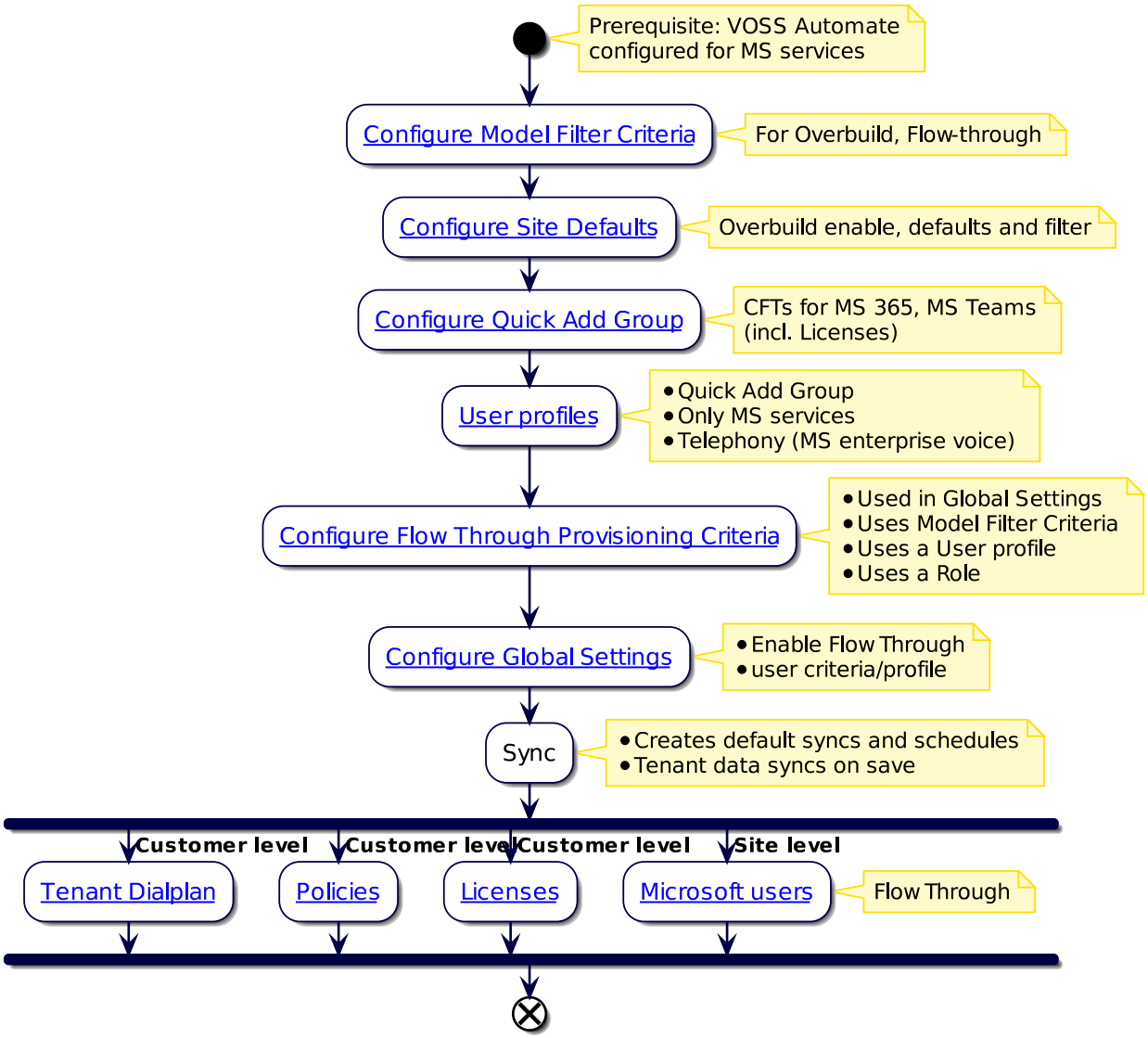
Prerequisites:

- Microsoft UC Application Setup in the Core Feature Guide
- Configure Automate for Microsoft Services in the Core Feature Guide

Workflow to sync to site with flow through provisioning

The flowchart sets out the sync with flow through of Microsoft user and services:

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related Topics

- Microsoft Quick Start in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide

Create MS Teams service account on Microsoft cloud

This procedure creates the Microsoft Teams admin user service account for Automate in the Microsoft 365 Admin Center, and assigns the *Teams Administrator* role.

Note: The PowerShell proxy server uses the Microsoft Teams service account to manage Microsoft Teams resource accounts.

Copyright © 2025 VisionOSS Limited. All rights reserved.

To create the MS Teams user service account

1. Use your MS account admin user to log in to the Microsoft 365 Admin Center.
2. Go to **Users > Active users**, then click **Add a user**.
3. Fill out user details:
   - Specify first name, last name, display name, and username (e.g. "voss-svc").
   - Choose a domain. You can choose any domain in the drop-down, including the default "*.onmicrosoft.com" domain.
   - Create a password for the account.
   - Clear the checkbox that requires the user to change their password when they first sign in.

   Note:
   - Make a note of the user name, domain name, and password you create. You'll need these details when setting up the connection parameters in Automate. See *Microsoft tenant setup*
   - There is no need to assign a license.

   - Assign the user with the **Teams Administrator** role.

     Note: Starting in Q3 2024, Teams administrators must have user management permissions in Microsoft 365 to create resource accounts. If you wish to continue using Automate to create resource accounts, the Service Account should be assigned "User Administrator", "Global Administrator", or custom roles that include the "User Management" permission".

     For further details around Microsoft's changes with regard to resource accounts, see VOSS Automate 24.1 - Microsoft Customers, Upgrade Planning for App Registration

4. Save your changes to create the user.

General Tenant Functions

Microsoft tenant setup

Tip: *Use the Action search to navigate Automate*

Overview

Microsoft

provider

When Microsoft services and users are deployed in your system, a Microsoft tenant must be set up for each Microsoft customer in the system. The Microsoft tenant workflows create default schedules, data syncs, and test connections, based on the solution capabilities enabled for the tenant.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Solutions and the Microsoft tenant

Solutions are licensed system components delivering specific functionality and features. As at release 25.3, for new and upgrading customers, the following solutions are available in the system and enabled by default in the Global Settings:

- UC Automation
- Email

Deployment of the following solution capabilities is reserved for future development:

- UC Monitoring
- UC Analytics
- Security
- License Management
- Meetings Rooms

Inquire with your VOSS service representative for further details about the deployment and use of the *reserved for development* solutions.

Permissions required in the app registration for the Microsoft tenant, by solution:

- UC Automation: Certificate
- Email: Certificate
- UC Monitoring: Secret
- UC Analytics: Secret
- Security: Certificate
- License Management: Certificate
- Meetings Rooms: Certificate

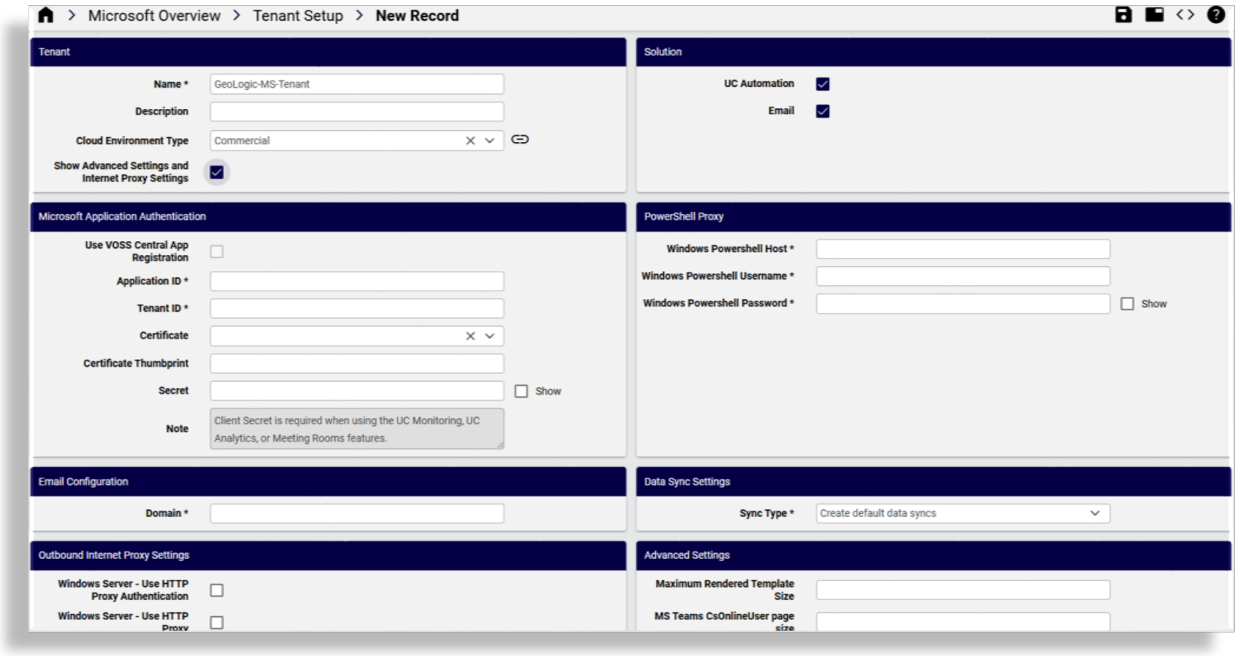
Add a Microsoft tenant

This procedure adds and configures a Microsoft tenant at the customer level with one or more solution capabilities, including configuration of a single, customer configurable app registration containing all permissions associated with the selected solutions.

These steps also configure connections:

- Between Automate and the PowerShell Proxy
- Between the PowerShell Proxy and the Microsoft tenant
- The Graph API connection between Automate and the Microsoft tenant

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: References in this section to “PowerShell Proxy” refer to the MS Windows host running PowerShell commands. References to just “Proxy” refer to the HTTP proxy server that the the Windows PowerShell host uses to access the tenant in the cloud.

Prerequisites:

- Solution capabilities required on the customer tenant must be enabled in the Global Settings.
- The FQDN or IP address of a single-node PowerShell Proxy, or the FQDN corresponding to your load balancer’s virtual IP address.

  See *Run PowerShell proxy server setup script* in the Core Feature Guide
- Credentials for the local service account you created on the PowerShell Proxy
- Proxy authentication credentials (if the outbound Internet Proxy requires authentication). Note that Authenticated proxy is not supported.
- The client ID and tenant ID
- Either the client secret or certificate. See *Solutions and the Microsoft tenant*. A secret or certificate created when registering Automate as an application object with Microsoft Entra ID. For greater security, certificate is preferred.

  If an Arbitrator is configured on Automate, secret is required.

  See *Arbitrators* in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

To add and configure the Microsoft Tenant

1. Log in to the Admin Portal as a Provider administrator.

   Note: By default, the Provider administrator role is the only role that has the ability to create Tenant connections.

2. Go to the **Tenant Setup** page.
3. Click the Plus icon (+), then choose the hierarchy, typically, Customer.
4. Optionally, add a description. The tenant name auto-populates the **Name** field. You can update it if required.
5. At **Cloud Environment Type**, select the cloud environment type to authenticate to. For details, see *Microsoft tenant cloud environment type*.
6. At **Solution**, select solution capabilities to enable for this tenant.

   Note: As at 25.3, the following solutions are available: *UC Automation*, *Email*

   Solutions must be enabled for your system in the Global Settings. See *Solutions and the Microsoft tenant*. Displayed fields on the form are filtered by selected solutions. For example:

   - **UC Automation enabled**? Displays **PowerShell Proxy** settings.
   - **Email enabled**? Displays **PowerShell Proxy** and **Email Configuration** settings.
   - **UC Automation and Email enabled**? Displays **PowerShell Proxy** and **Email Configuration** settings. **Use VOSS Central App Registration** cannot be used (Relevant only when only a single solution is enabled).

   It is NOT possible to disable/remove a solution on the tenant once you've saved the tenant.

7. Configure settings based on enabled solutions:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Settings	Instructions
Microsoft Application Authentication	If you have only one solution enabled and want to use **VOSS Central App Registration**, select the checkbox, Then fill out the **Tenant ID**. The workflow applies the Application ID based on the selected solution. If you have more than one solution enabled you'll need to create your own app registration: • **Application ID** is auto-populated. • Fill out **Tenant ID** • UC Automation and Email solutions require a certificate. Select your certificate. The certificate is pushed to Windows during the *Test Connection* step after saving the tenant. • **Certificate Thumbprint** is auto-populated once you select the certificate. • **Secret** is required if you have an Arbitrator configured on Automate.
PowerShell Proxy	*UC Automation* and *Email* solutions Configure PowerShell server authentication details: • **Windows PowerShell Host**: Fill out the FQDN or IP address of a single-node PowerShell proxy, or the FQDN corresponding to your load balancer's virtual IP address. • **Windows PowerShell Username** and **Windows PowerShell Password**: Fill out the credentials for the local service account you created on the PowerShell Proxy.
Data Sync Settings	*UC Automation* and *Email* solutions Choose the sync to perform. Three options: • **Create default data syncs**: Creates default data syncs that ship with the product (these syncs are common to all solutions): – SyncMS365 – SyncMS365Users – PurgeMS365 • **Create default data syncs with custom MS365 MIF**: Creates a new model instance filter (MIF) for a specific model. Choose a filter or create a custom filter to run the default syncs with filtered data. • **Use Datasync Builder**: Uses the custom data sync template to create the data syncs based on selected solutions. You can either use a data sync profile or choose one or more templates to use with the Datasync Builder. Choosing individual templates will allow you to set the first execution date and time for any data sync template that requires schedules. Scheduling defined on the tenant in this way applies only to the tenant and is not added to a template or profile.
Email Configuration	*Email* solution • **Domain**: Provide the Microsoft Exchange admin domain used to authenticate.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note:

- In Shared Central App Registration, VOSS builds and maintains the app registration in their Microsoft Entra ID tenant and performs organizational and application validation with Microsoft.
- Tenant ID and Application ID are recorded in the app registration and identify the tenant in the Microsoft cloud.
- For the certificate:
  - You can generate a certificate in Automate and upload it to MS Entra ID, or;
  - If you already have a signed certificate from another source in your organization and it's already uploaded to MS Entra ID, you can upload that certificate into Automate and have Automate manage it on itself and on the PowerShell proxy.

8. Optionally, select **Show Advanced Settings and Internet Proxy Settings** to configure additional settings on the tenant, where relevant:

   Outbound Internet Proxy Settings:

   a. **Do you have an outbound internet proxy deployed between the PowerShell proxy and the public internet**?

      - **Yes**. Select **Windows Server - Use HTTP Proxy**.

        If the outbound Internet proxy requires authentication, select **Windows Server - Use HTTP Proxy Authentication**, and fill out a username and password.

        You will have already provisioned the outbound internet proxy's IP address (or FQDN) and port number when you set up the PowerShell proxy. See *Run PowerShell proxy server setup script*, and note the caveat regarding proxy authentication described at:

        PowerShell proxy deployment topologies in the Core Feature Guide

        If you wish to disable the use of a currently configured outbound internet proxy:

        - Uncheck **Window Server - Use HTTP Proxy** and save the Microsoft tenant configuration.
        - Re-run the PowerShell proxy server setup script and respond `y` to the outbound internet proxy question, followed by entering `none` as the value for the proxy as in the example below:

```
Do you want to configure the outbound internet proxy? (y/n) y
Input: y
Configuring outbound internet proxy...
Enter the outbound internet proxy address and port.
Use the format <proxy_address>:<proxy_port>.
Enter "none" to remove the proxy. Press Enter to use "10.121.2.231:3128".
↪ none
Input: none
Proxy settings removed and proxy disabled for user Administrator.

Current WinHTTP proxy settings:

    Direct access (no proxy server).

System-wide WinHTTP proxy settings removed.
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **No**. Clear the following fields: **Windows Server - Use HTTP Proxy**, **Windows Server - Use HTTP Proxy Authentication**, **Windows Server - Proxy Server Username**, **Windows Server - Proxy Server Password**

  Authenticated proxy is supported.

b. At **MS 365 HTTP proxy** / **MS 365 HTTPS proxy**, set the outbound internet proxy server if required for traffic outbound to the public internet.

The proxy setup defines the route for the MS Graph API communications that the system uses for communication with the MS 365 Cloud tenant.

- For HTTP proxy traffic, fill out a MS 365 HTTP proxy value with the following format: `http(s)://[user:password]@host:port/`.

  Special characters in either the user or password must be URL encoded. Verify the required format with the proxy administrator.

- For HTTPS proxy traffic, fill out a MS 365 HTTPS proxy value with the following format: `http(s)://[user:password]@host:port/`

  Special characters in either the user or password must be URL encoded. Verify the required format with the proxy administrator.

Note:

- **MS 365 HTTP proxy** and **MS 365 HTTPS proxy** values will almost certainly be identical unless your proxy administrator has clearly told you that HTTP and HTTPS traffic are being proxied through different servers. It is not required that the **MS 365 HTTP proxy** address begin with `http://` or that the **MS 365 HTTPS proxy** address begin with `https://`. It is perfectly acceptable to proxy HTTP traffic to an `https://` address or HTTPS traffic to an `http://` address.
- In both cases the host can be a FQDN if resolvable via DNS or the IP address of the internet proxy.

Advanced Settings

The table describes fields in the **Advanced Settings** pane:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Maximum Rendered Template Size	The maximum allowed size of any rendered template for all models for all managed drivers. Size in bytes, so 900000000 is 900MB. Only set this value if the amount of data returned when using the default value is causing an error. Default is 900MB.
MS Teams CsOnlineUser page size	Defines page size for the `msteamsonline/CsOnlineUser` device model. Only set this value if the amount of data returned when using the default value is causing an error.
MS Teams Number page size	Defines the maximum number of records to retrieve at a time from APIs related to the `msteamsonline/Number` device model. Starting January 2025, Microsoft has set the page size limit for phone number retrieval to a maximum of 1000 numbers per query. Requests exceeding this limit will result in an error. See the Automate 24.2-PB1 release notes for the upgrade notes for EKB-22837, for details.
MS 365 MsolUser page size	Defines the maximum number of records to retrieve at a time from the API related to `device/msgraph/MSOLUser`. For optimal performance, leave this field blank to use the default value, *999*.
MS 365 Group page size	Defines the maximum number of records to retrieve at a time from APIs related to `device/msgraph/Group`. For optimal performance, leave this field blank to use the default value, *999*.
Auto filter Teams users	Defines whether to add a default, automatic filter to all CsOnlineUser syncs to only return records matching MsolUsers in the cache. Default is False. When enabled (True), no other sync filters can be used for CsOnlineUser syncs. Using additional filters will trigger a system error in this case. **Important:** Automate issues a warning when it detects an `in` condition for `UserPrincipalName` used alongside other `CsOnlineUser` filters during sync and filtering. In Microsoft tenants with auto-filter enabled, the expected records may not be returned if your MsolUser cache is not up to date.

Note: For details on the auto filter for Teams users, see Microsoft syncs in the Best Practices Guide

9. Save the tenant configuration.

Note: Saving the tenant with the certificate deploys the certificate to the PowerShell proxy and installs it. You can then import the certificate on the tenant App registration in Microsoft Entra for authentication of all apps (MS Exchange, Teams, and Graph).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Next steps

- *Test the tenant connection*
- High level administrators with access to the `data/MultivendorUsernameMappingMacros` model instances should verify that no changes are needed in user name mapping macros prior to sync.

Important: For release 21.5-PB5, Multivendor environments using the `data/MultivendorUsernameMappingMacros` model at a hierarchy *below* `sys` level require an additional update. High level administrators with access to this model should ensure instances include:

```
"username_macro_ms_365": [
   "{{ input.UserPrincipalName }}",
   "(( fn.is_none_or_empty input.username == fn.true ))<NOT_FOUND>(( data.User.
↪username | username:input.username != '' ))<{{ data.User.username | username:input.
↪username }}><NOT_FOUND>",
   "(( fn.is_none_or_empty input.username == fn.true ))<NOT_FOUND>(( data.User.
↪username | username_ms_365:input.username != '' ))<{{ data.User.username |␣
↪username_ms_365:input.username }}><NOT_FOUND>",
   "(( fn.is_none_or_empty input.UserPrincipalName == fn.true ))<NOT_FOUND>(( data.
↪User.username | email:input.UserPrincipalName != '' ))<{{ data.User.username |␣
↪email:input.UserPrincipalName}}><NOT_FOUND>",
   "(( fn.is_none_or_empty input.UserPrincipalName == fn.true ))<NOT_FOUND>(( data.
↪User.username | username_ms_365:input.UserPrincipalName != '' ))<{{ data.User.
↪username | username_ms_365:input.UserPrincipalName }}><NOT_FOUND>",
   "(( fn.is_none_or_empty previous.UserPrincipalName == fn.true ))<NOT_FOUND>((␣
↪data.User.username | username_ms_365:previous.UserPrincipalName != '' ))<{{ data.
↪User.username | username_ms_365:previous.UserPrincipalName }}><NOT_FOUND>",
   "(( fn.is_none_or_empty input.UserPrincipalName == fn.true ))<NOT_FOUND>(( data.
↪User.username | username_ms_teams:input.UserPrincipalName != '' ))<{{ data.User.
↪username | username_ms_teams:input.UserPrincipalName }}><NOT_FOUND>",
   "(( fn.is_none_or_empty previous.UserPrincipalName == fn.true ))<NOT_FOUND>((␣
↪data.User.username | username_ms_teams:previous.UserPrincipalName != '' ))<{{ data.
↪User.username | username_ms_teams:previous.UserPrincipalName }}><NOT_FOUND>",
   "(( fn.is_none_or_empty input.UserPrincipalName == fn.true ))<NOT_FOUND>(( device.
↪cucm.User.userid | userIdentity:input.UserPrincipalName != '' ))<{{ device.cucm.
↪User.userid | userIdentity:input.UserPrincipalName }}><NOT_FOUND>",
   "(( fn.is_none_or_empty input.UserPrincipalName == fn.true ))<NOT_FOUND>(( device.
↪cucm.User.userid | mailid:input.UserPrincipalName != '' ))<{{ device.cucm.User.
↪userid | mailid:input.UserPrincipalName }}><NOT_FOUND>"
    ],
```

- Perform a sync from the Microsoft tenant:
  - Syncs import Microsoft users, tenant dial plan, licenses, and policies to the customer level.

    For Microsoft Exchange, ensure that instances for all four device models (User mailboxes, Shared Mailboxes, Room Mailboxes, and Distribution Mailboxes) are synced in at the level were the tenant exists.
  - If *Security* is enabled (**Enable Defender for Endpoint** set to True in Global Settings), a data collection and schedule is added.

    A **Defender for Endpoint Data Collection <hierarchy name>** schedule is created. This schedule can sync data according to this created collection and that allows for a batch sync of the device

Copyright © 2025 VisionOSS Limited. All rights reserved.

data. The collected data is then also available when Overbuild for Microsoft is run.

- Configure the customer-wide site defaults doc (SDD), `CUSTOMER_TEMPLATE`. See *Site Defaults Doc templates*.
- Add network device lists (NDLs) with Microsoft 365 and Microsoft Teams tenant details. NDLs are required when adding sites.
- Create sites.
- Run the overbuild. See *Overbuild for Microsoft* in the Core Feature Guide
- Configure Automate for Microsoft services in the Core Feature Guide

Related topics

- Arbitrators in the Core Feature Guide
- Shared central application registration in the Core Feature Guide
- Generate a certificate for application registration in the Core Feature Guide
- Upload a certificate to use for app registration in the Core Feature Guide
- For details around the local hosts file and the TrustedHosts WinRM configuration, see *Run PowerShell proxy server setup script* in the Core Feature Guide
- Global Settings in the Core Feature Guide
- Datasync Builder in the Core Feature Guide
- Microsoft Defender setup, sync and overbuild in the Core Feature Guide
- Overbuild for Microsoft in the Core Feature Guide
- Network Device Lists (NDLs) in the Core Feature Guide

Test the tenant connection

You can test your Microsoft tenant connection parameters when adding or updating the tenant. In this step you're verifying that Automate can connect to the Microsoft tenant using the Teams and Exchange Powershell modules on the Windows server as well as using the Graph API on the Automate platform.

To run a test connection on the tenant:

1. Add or update the Microsoft tenant.
2. Open the saved tenant via the **Tenant Setup** list view.
3. From the overflow actions menu, select **Test Connection**.

   The workflow tests all configured elements and adds relevant connection parameters for solutions enabled on the tenant (provided these solutions are also enabled in the Global Settings). If a certificate exists it is pushed to Windows. Steps for disabled solutions are skipped.

   When running a test connection on an updated tenant, the workflow reviews existing connection parameters and updates these if needed. ted. We pushed the certificate to Windows because that's what Security requires. And we added all the Graph security connection parameters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Update a Microsoft tenant

Modifying a Microsoft tenant will only overwrite those driver parameters in the underlying connections (MSTeamsOnline, MSExchangeOnline, MSGraph) that are managed by the tenant workflows. Other driver parameters will be left as is.

It is NOT possible to disable/remove a solution on the tenant once you've saved the tenant.

Also refer to the **Advanced Settings** above to modify the *page size* options for the Microsoft Tenant in order to adjust the synchronization performance.

Related topics

- Microsoft Quick Start Guide for Automate in the Core Feature Guide
- Microsoft Overview in the Core Feature Guide
- Microsoft syncs in the Best Practices Guide
- Site Defaults Doc templates in the Core Feature Guide
- Run PowerShell proxy server setup script in the Core Feature Guide
- Overbuild for Microsoft in the Core Feature Guide

Microsoft tenant cloud environment type

When setting up the Microsoft tenant you can optionally choose a cloud environment type to authenticate to. Automate's default cloud environment for a Microsoft tenant is "Commercial".

On upgrade or install, the cloud environment type is set to this default value.

Automate also supports authentication to high security cloud environment types, allowing an admin to identify their Microsoft customer tenant as one that is operating in a high security cloud environment, either DoD (United States Department of Defense) or GCCH (Microsoft 365 Government Community Cloud High).

When the tenant cloud environment type is set to either DoD or GCCH, Automate sets the appropriate environment names for the Microsoft Teams and Microsoft Exchange PowerShell modules, and appropriate URLs are used for the Microsoft Graph API.

External access for MS Teams

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate allows you to view and update external access settings for Microsoft Teams users, from within the Automate Admin Portal. This feature allows you to define how Microsoft Teams users in your organization may communicate with users and domains from outside of your organization.

Any changes you make in Automate or in the Microsoft Teams online portal for external access settings, are synced.

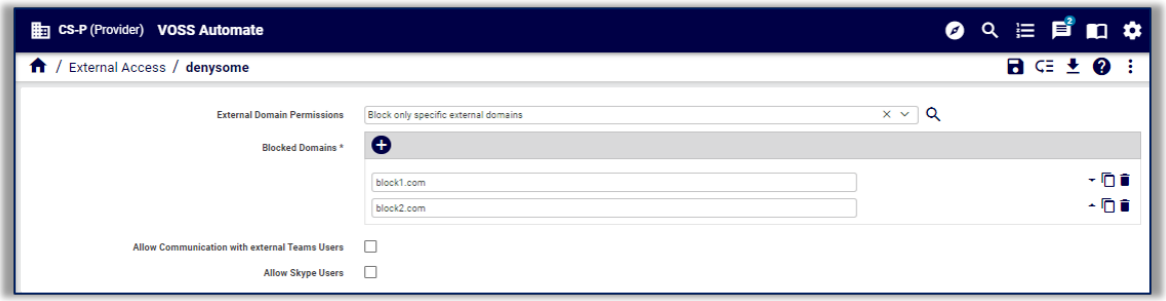
View and manage external access settings

1. Log in to the VOSS Automate Admin portal.
2. Go to **External Access** to open the **External Access** summary list view, where you can view existing external access settings.

   Note:

   - A default “allow all” instance with “Global” identity is available at the Customer hierarchy.
   - From the list view you can also export one or more items.

3. To view or update an existing external access settings configuration, click on an item in the list view to open its management page, then, choose an option:



   - To export these settings, click the **Export** icon.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To modify the external access settings you're working with, choose options on the page.

  The table describes external access configuration options:

External Domain Permissions	Choose a permission type from the drop-down. Options are: – Allow or block all external domains When external domains are allowed, users in your organization can chat, add users to meetings, and use audio video conferencing with users in external organizations. By default, your organization can communicate with all external domains. – All or block specific domains In this case you're able to specify the domains to allow or block, using the following format for the domain name: `example.com`
Allow Communication with external Teams Users	Defines whether users in your organization may communicate with external MS Teams users (MS Teams users whose accounts are not managed by your organization).
Allow Inbound Teams Users	Displays only when *Allow Communication with external Teams Users* is enabled. Defines whether external MS Teams users may contact users in your organization.
Allow Skype Users	Defines whether MS Teams users in your organization may communicate with Skype users.

4. Click **Save**.

   Any changes you made are synced to the external access settings on the Microsoft Teams online portal. Also, any settings changed through the Microsoft Teams portal will reflect in VOSS Automate.

Related topics

- Microsoft Quick Start in the Core Feature Guide

Microsoft Licenses

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate can be used to assign, modify, and remove Microsoft user licenses.

To allow Automate to manage Microsoft user licenses, you will need to enable the following setting in the site's site defaults (**MS Teams** tab): *Manage Licenses and Allow User Staging*

When Automate is enabled for license management:

- Admins can use Quick user to optionally configure the correct licensing and MS Teams configuration when onboarding new users.
- Microsoft license data can be synced in to Automate from the Microsoft cloud, and specified in the Quick Add Group (QAG) configuration templates as part of the provisioning workflow.

Important: If **Enable Microsoft User License Enforcement** is set to **Yes** in the **Global Settings**, a user can only be added if the license allocation limit for the user's hierarchy is not exceeded. For details, see *Microsoft license management and alerting* in the Core Feature Guide.

Users are placed in staging (an unsaved state) while license data is synced in to Automate. A licensed user may be assigned with a line and available number in Automate.

Targeted syncs may be scheduled from Automate to poll the Microsoft cloud for changes at regular intervals. Users are automatically provisioned in Automate, based on their service profiles and assigned licenses. The sync process moves Microsoft users to appropriate sites with the correct configuration, based on the site defaults, filter criteria, and user service profiles. The number assigned to the user is added to a number inventory in Automate, and is flagged with the user's name.

Note:

- To view staged users, go to **User Staging**.
- Starting with Automate v21.3-PB1, you can, with immediate effect, un-stage a user waiting in the staging queue. This executes a direct sync to the Microsoft cloud to determine whether the user has appeared in MS Teams after their licensing update.

Managing licenses for Microsoft users when onboarding and offboarding

Automate requires the `LicenseAssignment` permission to manage Microsoft licenses.

To avoid system errors, it is recommended that you do not use **Azure AD User (MSOL)** (`Msoluser` device model, `device/msgraph/msoluser`) to make changes, particularly when license permissions aren't assigned. Instead, it is recommended that you use the **Microsoft User Details** page (`relation/MicrosoftSubscriber`) or other Automate functionality to update users.

If a user has any group assigned license, Automate won't attempt any direct license assignment at all, via onboarding or via updates on the **Microsoft User Details** page (`relation/MicrosoftSubscriber`), regardless of what may be included in Automate configuration templates or in the Microsoft portal.

When offboarding, if Automate is set up to remove a user's direct licenses, this is only possible when Automate is also removing all the license groups. If any license group remains, the direct licenses aren't removed. For example, if a user has base licenses (for example, E3) assigned via group, and you want Automate to add *MCOEV* as a direct license, this won't be possible. In this case, it is only possible to add the *MCOEV* license via a group license assignment, since it is possible to assign or remove additional groups.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The group license assignment during onboarding and offboarding is not only used for licenses, so it can be used to add or remove non-license groups together with direct licensing, or for no licensing, as needed.

Related topics

- *Onboard user (Microsoft)*
- *Offboarding (Microsoft)*

View Microsoft licenses by customer

To view all Microsoft licenses synced currently synced in to Automate, go to the **Licenses** page. The Licenses summary list view provides the following license details per customer:

- License name (see the **Microsoft License Names** list for the mapping of the SKU ID number to the License Name)
- Number of active licenses
- Number of used licenses
- Customer name

Licensing users for MS Teams and Teams Phone by group membership

Automate provides options to manage licensing by group membership. Licenses associated with the group apply to members of the group.

Important: In Automate, licensing by group membership has priority over user licensing, so that if a user already had any individual licenses prior to group membership, these are replaced by the group license. Similarly, if a user that was licensed by group membership is removed from the group, the user becomes unlicensed.

Such licensing can be configured:

- For subscriber on-boarding and off-boarding by the selected **Quick Add Groups** in the case of:
  - **Microsoft Quick User**
  - **Offboard User**

    Selected in the Offboard User configuration template (for target model `view/MicrosoftSubscriberQas`)
  - **Flow Through Provisioning**

    Flow through provisioning uses the associated **Subscriber Profile** that selects an item from **Quick Add Groups**.

  This option requires the selection of specific configuration templates for **Microsoft** in the user **Quick Add Groups** associated with users:
  - **MS Groups Add Template**
  - **MS Groups Remove Template**

  For details on configuring these templates, refer to the *Configuration Templates for MS Groups* section below.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Manually, via **Manage Group Membership**. For details around configuring settings on this page, see *Manage group membership*.

  You can also use the Multi-vendor Quick Action to open this form - see: *Configure quick actions for multi vendor users*.

Configuration templates for MS groups

Automate ships with reference configuration templates that can be cloned to a hierarchy, renamed and modified in order to customize the group membership that will be affected by the operation associated with the configuration template.

The templates display on the **Configuration Templates** page. The menu and model associated with the configuration templates is `view/MsGraphManageGroup`.

- `Reference Microsoft Groups Add Template`

  Add one or more entries to the **Group** list to provide group membership to a user.

  If a user is already a member of a group, the corresponding entry is ignored.

- `Reference Microsoft Groups Remove Template`

  Add one or more entries to the **Group** list to remove group membership from a user.

  If a user is not a member of a group, the corresponding entry is ignored.

The **Group** names need to be typed in, and the list can be inspected via the **Groups** page. If MS licenses are associated with the groups, these will be applied or removed according to the configuration template **Operation** function. (For cloned templates, the **User** and **Operation** values do not have to be modified if the operation of the original template is to remain the same.)

Important: If the Add and Remove configuration templates contain the same list of groups, these should not both be selected when creating a Quick Add Group, since the result of applying the Quick Add Group will then be to both add *and* remove the overlapping group.

The best practice is to create separate Quick Add groups to apply for on-boarding and off-boarding a user, each containing only the required configuration template.

However, in cases where administrators wish to ensure only a standard set of groups apply during on-boarding or off-boarding, the configuration templates can be combined to achieve the desired set.

These created configuration templates can now be applied to the relevant created Quick Add Groups for use in on-boarding, off-boarding and flow-through provisioning.

Related topics

- *Microsoft Quick User*
- *Offboarding (Microsoft)*
- *Flow through provisioning (FTP)*
- *User profiles*
- *Manage group membership*
- *Quick Add Groups*

Copyright © 2025 VisionOSS Limited. All rights reserved.

View a user's Microsoft licenses

To view the license details of individual users via the user management functionality:

1. Go to the **Manage Users** list view.
2. Click on a user to open the Manage Users [user name] page.
3. Select the **MS Licenses** tab.
4. View currently enabled licenses for the user.

Related topics

- Microsoft users in the Core Feature Guide
- *Offboarding (Microsoft)*

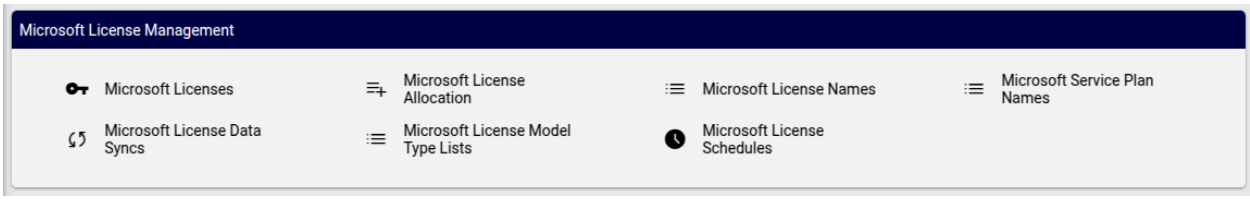
Microsoft license management and alerting

Tip: *Use the Action search to navigate Automate*

Overview

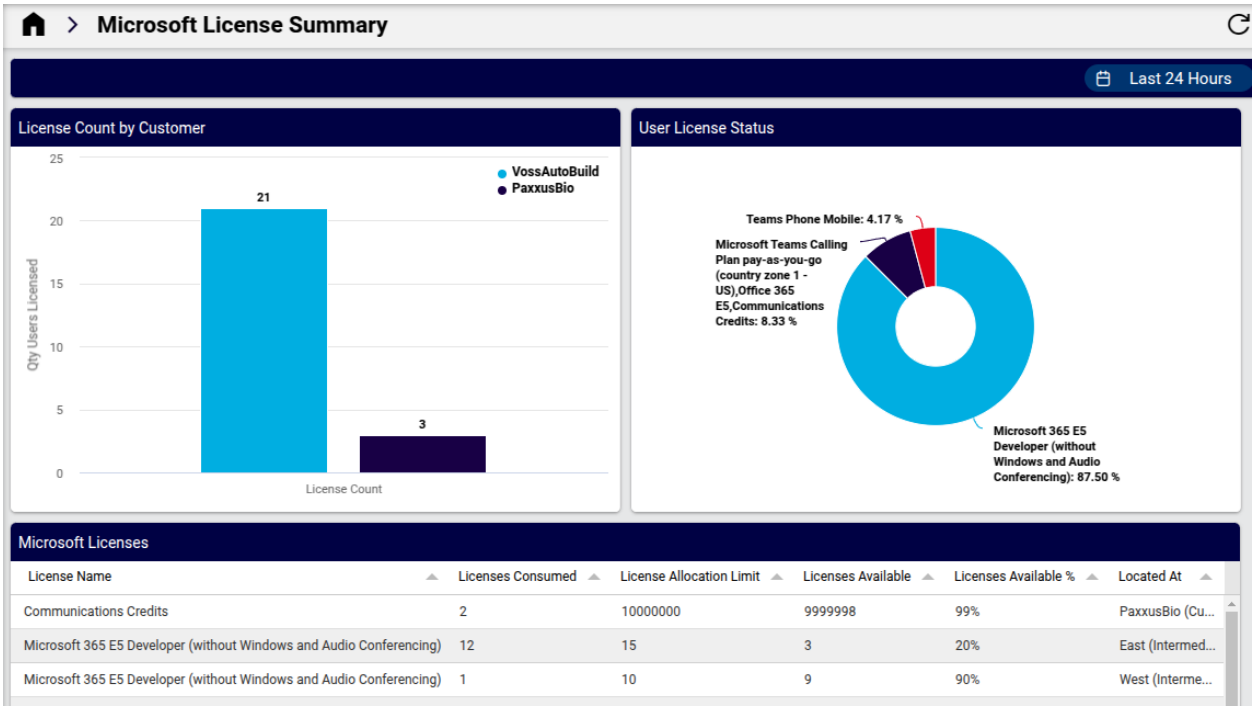
Where Microsoft 365 user licenses are available to an organization as a whole on a single Microsoft tenant, Automate offers support for the allocation of these licenses to various business units and departments within such an organization - represented as hierarchies in Automate.

License allocation at a hierarchy can be managed in Automate from the **Microsoft License Management** group of the **Microsoft** dashboard.



In addition, a number of charts and tables are available to administrators on the **Microsoft License Summary** dashboards - providing an overview of license allocation, availability and usage at hierarchies. See: *Microsoft license summary dashboard*.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Automate also enables you to set user license enforcement and allocation thresholds at hierarchies. This means that licenses will only be allocated to a subscriber at a hierarchy if these are available. Threshold availability percentage values can be set per hierarchy and allows for scheduled alerting to email groups whenever these thresholds are reached, so that timely action can be taken.

Related topics

- *Onboard user (Microsoft)*
- *Microsoft Licenses*
- *Microsoft users*
- *Microsoft Quick User*

Prerequisites and first steps

In order for the license enforcement, threshold percentage values and alerting to be available, it is necessary that:

- Microsoft Licenses are available.
- Licenses are synced from devices (device: `device/msgraph/MsolAccountSku`) to the organization hierarchy level.

  The **Microsoft Licenses** link on the **Microsoft License Management** group of the **Microsoft** dashboard provides a list view of the global pool of licenses, showing active, consumed, available (incl. percentage) licenses per hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- License data syncs are configured. The feature provides:
  - **Microsoft License Data Syncs**
  - **Microsoft License Model Type Lists**
  - **Microsoft License Schedules**

  offering default syncs and schedules that can be modified and used to manage license syncs at a hierarchy.

  Note that:
  - An alerting schedule `MicrosoftLicenseAlert` is also provided that can be further configured to schedule alerts if license alerting is enabled.
  - Quick Import is enabled by default for syncs related to *data/MSGraph* that sync Microsoft license data from Microsoft Graph.

  For details on data sync, refer to *Introduction to data sync*.
- **Global Settings** need to be set:

  Two settings are provided
  - **Enable Microsoft User License Enforcement** (default is No/Inherit):

    If this setting is enabled, license allocations per hierarchy are enforced.
  - **Microsoft License Alerting**

    If this setting is enabled, alerts are sent when configured license usage thresholds are reached at a hierarchy. See: *Microsoft license alerting*.

    Note that this setting requires that **Enable Microsoft User License Enforcement** is enabled.

  See: *Global settings*.
- Mappings for Microsoft License Names and Service Plan Names are noted.

  On the the **Microsoft License Management** group on the **Microsoft** dashboard, Automate provides:
  - **Microsoft License Names**

    A default mapping of **License Number** (SKU Part Number) to **License Name**
  - **Service Plan Names**

    A default mapping of **Service Plan Number** to **Service Plan Name**

  These mappings can be referenced and configured if required; and provide a user-friendly name display for these items on the Automate user interface.

Microsoft license allocation

Allocate licenses to a hierarchy.

Prerequisite: MS licenses have been synced in at high level organizational hierarchy.

1. Navigate to required hierarchy and open **Microsoft License Allocation** on the **Microsoft License Management** group on the **Microsoft** dashboard.
2. Add a new record to **Microsoft License Allocation**:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **License Name** dropdown list only shows names of available licenses at the selected hierarchy (as mapped on the **Microsoft License Names** table on the **Microsoft License Management** group on the **Microsoft** dashboard). In other words, there is a single, unique allocation instance for a license name at a hierarchy.
- A read-only number of the **Maximum Limit Allowed** is displayed for the selected license. This is the number of licenses un-allocated at or up the hierarchy.
- Enter a **License Allocation Limit** number for the selected license name and hierarchy and save the record. If alerting thresholds are set for this limit, this number is used to determine the threshold value. If this limit is reached during subscriber licensing provisioning - for example using *Microsoft Quick User* - the transaction will fail.

Note: When entering a license allocation limit at a hierarchy, the selected number may be less than the number of licenses *currently consumed* at the selected hierarchy - as reflected when viewing the added record. In this case, the new record requires modification in order to adjust this allocation limit.

The *maximum* **License Allocation Limit** for a specified hierarchy is obtained by the following calculation:

```
parent license allocation limit (the first instance found searching up the
↪hierarchy)

less

the sum of (all license allocation limits set at the same hierarchy level)
```

If no parent license allocation limit exists, the total active units value is used, as sourced from the `device/msgraph/MsolSkuAccount` model.

---

3. The added record displays in the **Microsoft License Allocation** list view, with columns showing:
   - The **License Allocation Limit** number as entered. (This number should not be higher than the **Licenses Consumed**.)
   - The current **Licenses Consumed** number as calculated for the hierarchy and lower.
   - The **Licenses Available** number and percentage (**%**) columns, as calculated for the hierarchy and lower.
   - The **Located At** hierarchy name.
4. In the global settings, select threshold percentages per license at a hierarchy using the **Availability Threshold Percentage** setting. If alerting has been enabled and the threshold is reached, an alert will be raised and also sent by email if enabled.
5. If alerting email groups have been selected in **Global Settings**, ensure that alerting Email Groups have been set up and selected as the global setting: **Alert Email Group**. (For details on how to set up email groups, see *Email*.)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Microsoft license alerting

1. On **Global Settings**, two settings need to be enabled to use the license altering feature:
   - **Enable Microsoft User License Enforcement** (default is No/Inherit):
   - **Microsoft License Alerting**
2. On **Microsoft License Alerting**:
   - **Enable Alert on Microsoft Licenses** (options: Yes, No, inherit. Default is No) Only if enabled, will any alerts be raised.

     A license allocation transaction above a threshold of available licenses will fail and the alert will be created.

     Fields are exposed to configure as below.
   - **Availability Threshold Percentage** (select from: 10%, 15%, 20%, 25%, inherit)

     Set a percentage value of available licenses which, when reached, should trigger an alert.
   - **Enable Email Group** (choose: Yes, No, inherit)

     An option to send the alerts to an email group.
   - **Alert Email Group** (choose an email group)

     If enabled, the default email group to send alerts to - for email group setup, see: *Email*.

Note: If alerting is *not* enabled but user license enforcement is enabled, license transactions that result in exceeding available allocations will fail without a prior threshold alert warning.

Microsoft license summary dashboard

This dashboard provides default widgets that allow for the inspection of license usage:

- Charts:
  - **License Count by Customer**

    Provides a view of the number of licenses in use at the Customer hierarchy/hierarchies, at or below the current (customer/higher level) hierarchy.
  - **User License Status**

    Provides a view of the percentage of licenses in use at the current hierarchy, grouped by license name.
- Table:
  - **Microsoft Licenses**

    Provides a detailed view of the licenses in use at or below the current hierarchy, with columns for:
    * **License Name**: the license name as mapped from the license SKU number
    * **Licenses Consumed**: number of licenses in use at the hierarchy
    * **License Allocation Limit**: license allocation limit (number) at the hierarchy
    * **Licenses Available/%**: number/percentage of licenses available at the hierarchy
    * **Located At**: hierarchy name

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manage certificates for SSO

Tip: *Use the Action search to navigate Automate*

Create a self-signed or 3rd party certificate for SSO

This procedure creates a self-signed or third-party-signed system certificate to use when setting up Single Sign-On (SSO) on the web proxy node on Automate.

Note:

- Web server certificate management is carried out on the Automate command line. Refer to the CLI documentation for details.
- During customer onboarding, SSO certificate creation is customer-specific.

1. Log in as system administrator.
2. Go to the **Certificates** page.
3. Click **Add**.
4. On the **Base** tab, configure the following:
   - Fill out a name (mandatory) and a description (optional) for the certificate.
   - Choose an option:
     - **Self-signed certificate**? For a self-signed certificate:
       - Clear the **Generate Certificate Signing Request** checkbox.
       - Define the certificate validity period. This is measured in seconds and defaults to 0 (now) and 315360000 (10 years), respectively.
     - **Third-party signed certificate**?
       - Select the **Generate Certificate Signing Request** checkbox.
       - At **Valid To**, define a value, in seconds, for how long the certificate is valid from the time it's generated. Default is 315360000 seconds (10 years).
   - At **Expires**, fill out an expiry date for the certificate, with format `year-month-day-time`, for example: *2035-05-03T09:06:33Z*
   - (Optional) Change the **Key Length** from the default (2048).
5. On the **Certificate Information** tab, configure the following:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Common Name *	Enter the FQDN for your server.
Country Code *	A two-digit country code
State *	An appropriate country subdivision
City *	Your city
Organization *	Your organization
Organization Unit	Your organization subunit

6. Click **Save**.

Note: If you created a self-signed certificate, you can exit this procedure. If you requested a third-party-signed certificate, continue with the next steps.

7. On the **Certificates** list view, select the third-party-signed certificate you created.
8. From the toolbar overflow menu, select **Export Certificate Request**, then follow your organization's procedures to obtain the third-party signature for the certificate.
9. On the **Certificates** list view, select the certificate, then from the toolbar overflow menu, select **Upload Signed Certificate**.
10. Browse to the signed certificate, then click **OK**.

Renew single sign-on certificate for Automate

If a customer's single sign-on certificate expires, this procedure renews the certificate for Automate.

1. Regenerate the certificate (either self-signed or CA signed) as described in *Create a self-signed or 3rd party certificate for SSO*.
2. Regenerate and upload SP metadata to the IdP described in *Configure Self-service SSO SP settings*.

Note: If an expired SSO certificate is being renewed and the IdP metadata has *not* changed, then the download, configure, and upload of the IdP metadata is not required and these steps can be ignored.

Generate a certificate for application registration

Microsoft

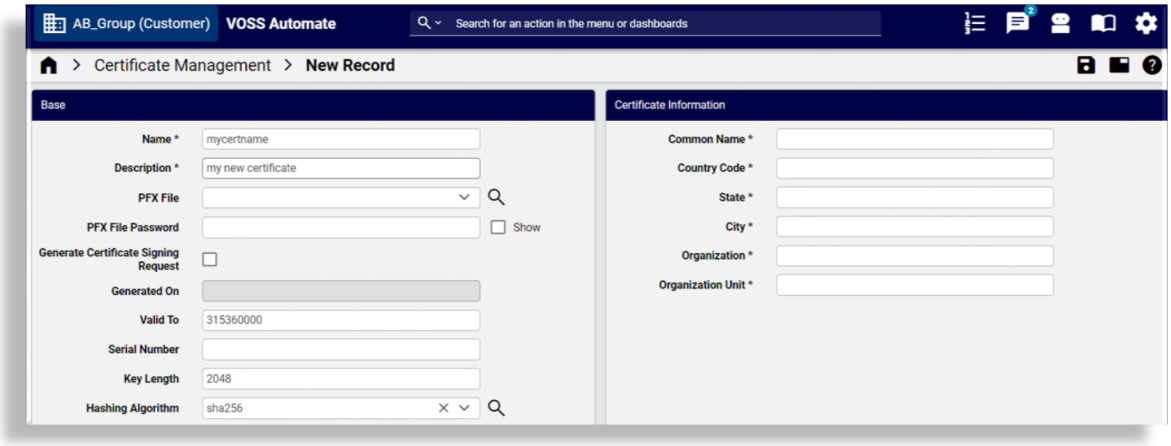
Tip: *Use the Action search to navigate Automate*

This procedure generates a certificate in Automate that you can use for application registration for Microsoft tenants.

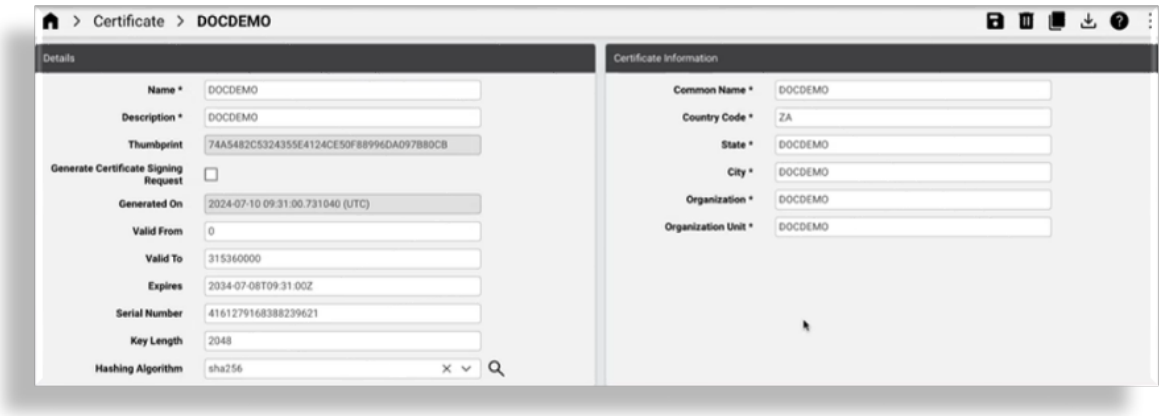
1. Go to the **Certificates** page.
2. Select the relevant Customer hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Click the Plus icon (+) to add a new certificate.
4. On the **Certificate Management > New Record** page, fill out at least the mandatory fields:
   - Fill out a name and a description for this certificate.
   - Fill out certificate details, including a common name, which must match the host being authenticated.

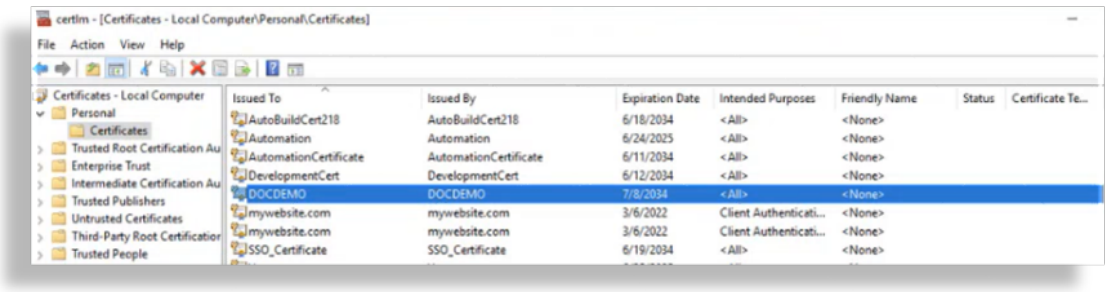


5. Save your changes to create the new certificate. A number of fields are auto-populated when the certificate is generated. The image shows an example:



6. Once the transaction completes, view your new certificate in the list view of the **Certificates** page.
7. Select the certificate, then, from the toolbar overflow menu, select **Export Public Key**, and save the exported file to your local computer or to a network location.
8. Upload the certificate you saved, to Microsoft Entra.
   - The certificate file will now be available for selection on the tenant, and will automatically populate the tenant **Certificate Thumbprint** field once you select the certificate. See *Configure Microsoft Tenant Connection Parameters* in the Core Feature Guide
   - When saving the tenant with the selected certificate, Automate pushes the certificate to the Windows PowerShell proxy. You can verify that the certificate has been added to the PowerShell proxy.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Network device lists (NDLs)

Tip: *Use the Action search to navigate Automate*

A network device list (NDL) is a list of network devices that are assigned to a site. NDLs are defined at the customer hierarchy level, and a customer can have multiple NDLs.

Only a Provider or Reseller administrator may create NDLs.

Shared UC applications (UC apps defined above the customer hierarchy level) can be included in an NDL. However, to use that NDL, the customer must be defined as allowing shared UC applications.

Each NDL can contain one instance each of the available devices. For example, for Cisco, one of each of the following: CUCM, CUC, Cisco WebEx.

Note: UC application clusters are linked to a customer only once the NDL is created.

Network device lists at sites

The following rules apply to NDLs, network devices, and device models at site hierarchies:

For a site which references a NDL, device models cannot exist at this site if these belong to a network device not referenced in the NDL.

Therefore:

1. A device model from a device cannot be added to it if it has a NDL referencing a different device.
2. A NDL cannot be added to it if it has device models that references a different network device than the one referenced in the NDL.

Choosing a network device list

If an administrator at a hierarchy has access to more than one NDL, the option to choose a specific hardware group or list may be needed in order to provision a set of devices.

The Rule Model Device Selection Type model solves this problem, and instances of it are a set of rules for views and relations at a hierarchy level. A particular NDL can then be selected from a popup form before the Add form of these model types are shown. In this way, the administrator can then select the specific required NDL.

Copyright © 2025 VisionOSS Limited. All rights reserved.

When an instance of the Rule Model Device Selection Type model is added, the target relation or view is specified and more than one set rules can be added for it - one for each relevant Hierarchy Node Type.

In addition, a default GUI Rule that is applied to the Relation or View is reflected as the default value for the Permitted Hierarchy Node Type.

In addition to this behavior, these rules apply:

- The NDL popup is only available for Relations and Views.
- Device form fields are filtered according to the device listed in the selected NDL.
- More than one type of device is supported for the selected NDL.
- Any Provisioning Workflow Network Device Filters (NDF) override a selected NDL device choice.
- Only the Add operation supported.
- For details on NDL popups, refer to the topic on Network Device List Selection Rules Advanced Configuration in the Advanced Configuration Guide.

Add a network device list

This procedure adds a new network device list (NDL).

1. Log in as a provider or reseller administrator.
2. Go to **Network Device Lists**.
3. Choose a customer on the hierarchy tree where the NDL is to be created.
4. Click the Plus icon (+) to add a record.
5. Fill out a name for the NDL, and optionally a description.
6. For each available network device that you wish to add to the NDL:
   - Click the Plus icon (+) to display the search field.
   - Click the down-arrow at the search field to select the reference instance.

   Note: For CUCM and CUC, only publisher nodes display in the drop-downs.

   - Click **Save**.

Edit or delete a network device list

Once you've assigned a NDL to any site, you can't delete it; you can only make the following changes:

- The NDL name can be changed.
- The NDL description can be changed.
- New devices can be added.

Deleting an unassigned NDL does not remove the associated customer dial plans or the assigned UC apps.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Automate configuration and sync in the Core Feature Guide

Group and Team Management

Teams

Tip: *Use the Action search to navigate Automate*

Overview

Automate allows you to manage Microsoft Teams from within the Admin portal. Changes you make to teams in Automate or in the Microsoft Teams online portal are synced.

A team comprises its members, its channels (where team members share messages and other resources), and its privacy and permissions settings.

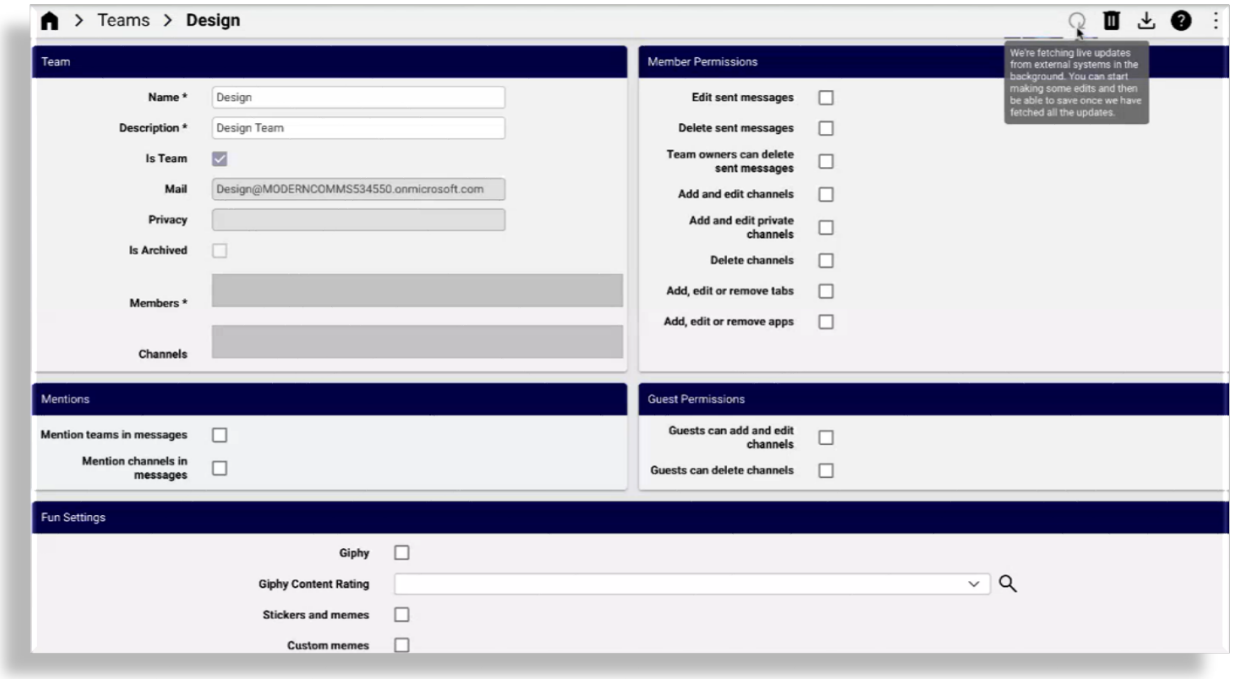
Note: A Microsoft Team is a collection of people, content, and tools that are grouped together for a common purpose. For example, you may want to add a group of engineers working for the same project, to a team.

In the Microsoft Teams online portal, an admin user can:

- Add or update a team, and give it a name and description
- Make the team private or public.
- Add a team owner
- Move a team (Provider admin only)

When using a Microsoft client (desktop or phone), a Microsoft end user can add teams from teams templates.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- *MS Teams templates*
- *Groups*
- Microsoft syncs in the Best Practice Guide

Add and update Teams

This procedure adds, edits, or deletes teams and team members in Automate.

Note: Changes you make to MS teams in Automate syncs to the Microsoft Teams online portal. You can also view changes made to MS teams in the MS Teams portal online, from Automate.

Pre-requisites:

- When configuring Automate for Microsoft, you will need to assign the following permissions to the API registration in the MS Entra admin portal to allow MS Teams objects to successfully sync in to Automate, and to allow you to manage these objects in Automate:
  - TeamMember.Read.All,
  - TeamMember.ReadWrite.All,
  - TeamMember.Read.Group

To add and update Teams:

1. In the Automate Admin Portal, go to **Teams**.
2. View existing teams in the list view.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note:

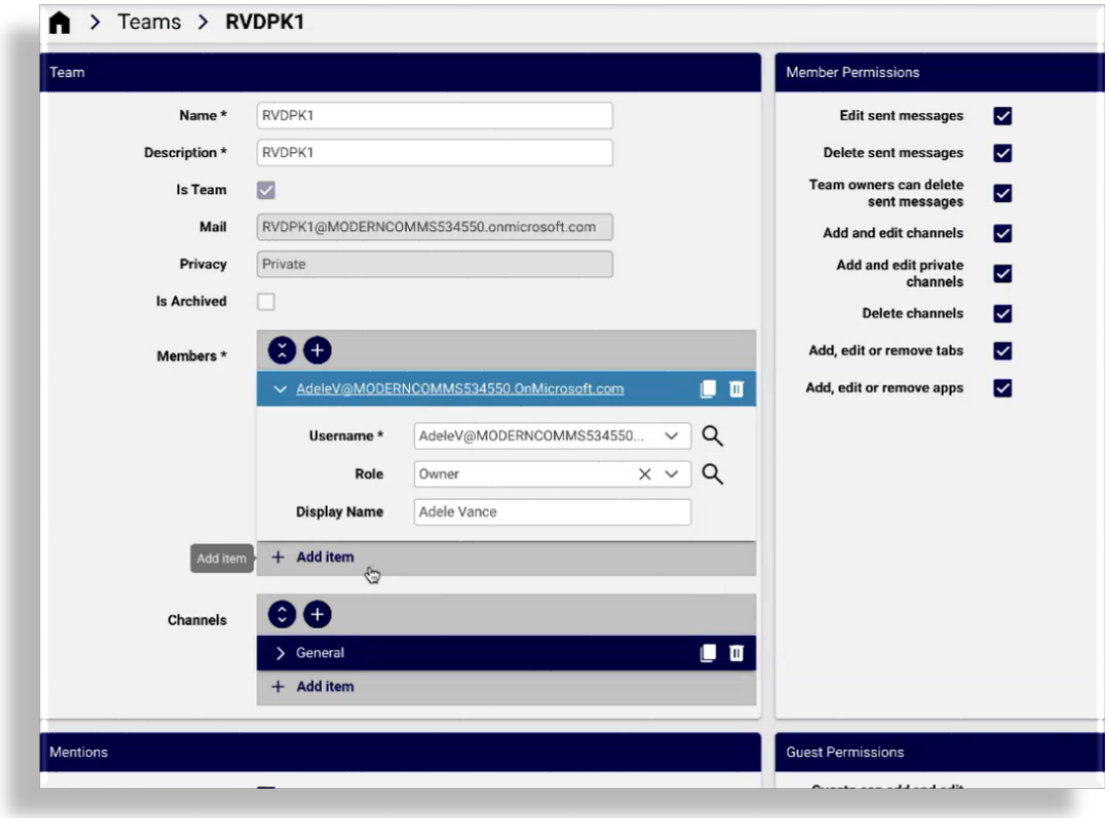
- The number of Teams in the list view matches the number of Teams in the Microsoft Portal.
- The **Teams** list view displays synced in data for MS Teams. Clicking on a Team to view its details triggers a live update from the Microsoft Entra ID portal to fetch additional details for the Team, including its members and channels. This is to ensure efficient and fast data syncing for Teams and Groups from Microsoft Entra ID. Data syncs for Teams and Groups are handled in the same way in the Automate GUI. Microsoft doesn't differentiate between Teams and Groups on the MS Entra ID portal so both the Teams and Groups list view and details page point to the same Automate model, `device/msgraph/Group`.

3. Choose an option:
   - **Edit a team**: To edit a MS team, click on the relevant team in the list view to open its management page, then update settings, and click **Save**.

     Note: You can add or remove members, change member roles, update Team settings, and archive, unarchive, or delete a team, and move a team (Provider admin only). However, channel membership type is read-only in the Automate Admin Portal, and will need to be updated in the Microsoft Portal, if required.

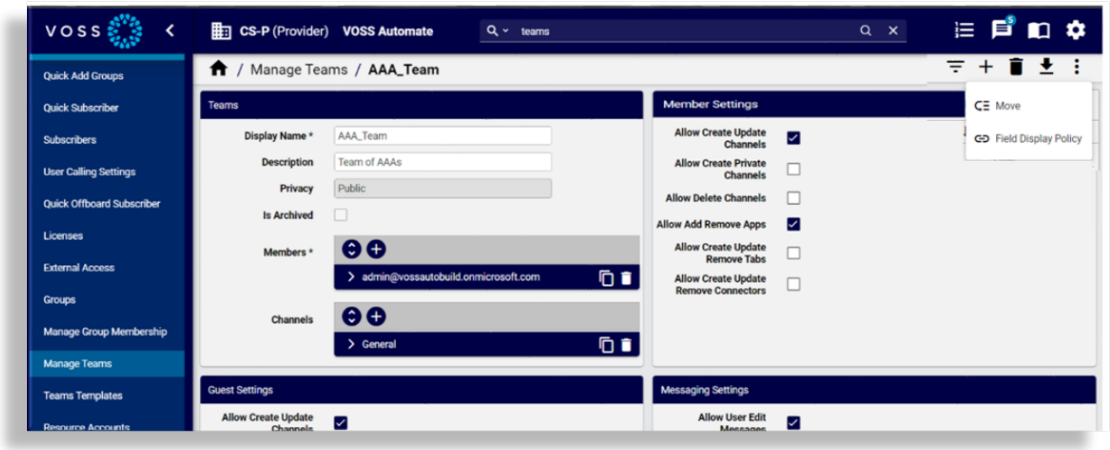
     To archive or unarchive a Team, select the relevant team(s) in the list view, then click the relevant toolbar option (Archive Team or Unarchive Team). The **Is Archived** checkbox is read-only when a team is archived, and you can't add or update team members and channels.

     All changes are synced to the Microsoft Teams online portal.



Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Move a team**: As a Provider admin, you can move one or more MS teams via the list view, or click on a team to open its configuration page, then move the team.



Note: When moving a team, team members remain at their existing location. Only the team is moved. However, let's say you moved a team to a site and you want to add additional members, then you can add new members that are at the site where the team now exists, even though the team still contains members that may be at a different location in the hierarchy.

- **Add a team**: To add a MS team, click the Plus icon (+) to open the **Teams** page, then fill out team details:
  - Fill out a display name (mandatory) and (optionally) a description.
  - Choose a privacy policy, either public or private.

    Note: The default is *Public*.

  - At **Is Archived** define whether the team may be archived.
  - At **Teams Templates**, choose a template, if you wish to create the team from a predefined, custom template.
  - At **Members**, click the Plus icon (+) to add team members (one or more), and define the member's role, either owner or member.

    Note: At least one user must be assigned the team owner role.

  - At **Channels**, click the Plus icon (+) to add channels (one or more).

    Note: The first channel (*General*), is added by default. All members you add to the team are added to this channel.

    Automate only supports adding channels with membership type *Standard*. In the Microsoft Teams online portal, you can add channels that have any of the following membership types: Private, Standard, or Shared

Copyright © 2025 VisionOSS Limited. All rights reserved.

- At **Member Settings**, select permissions that will apply to team members. For example, you can define whether to allow team members to add or update channels, to create private channels, to add or remove apps, or to delete channels.
- At **Guest Settings**, define whether to allow guest team members to add, update, or delete channels.
- At **Messaging Settings**, define permissions for messages, for example, choose whether to allow ordinary members to edit or delete messages, define whether team owners can delete messages, and whether to allow team or channel mentions.
- At **Fun Settings**, define whether to allow Giphy, set a content rating for Giphy, and define whether to allow stickers and memes.

Groups

Tip: *Use the Action search to navigate Automate*

Overview

Automate allows you to view the details of Microsoft Teams Active Directory (AD) groups synced in from the Microsoft Teams cloud portal, so that you can choose these groups for use with Microsoft auto attendants and call queues.

On the **Groups** page, you can also add, update, and delete groups.

Note: Guest users (Msol users external to the tenant) are synced in, but their group details (information about which groups they're associated with) won't be included in the sync.

Related topics

- *Auto attendants*
- *Call Queues*
- *Teams*

View and manage groups

This procedure displays groups synced in from the Microsoft Teams cloud portal, and allows you to view a group's details, and to add, update, or delete a group.

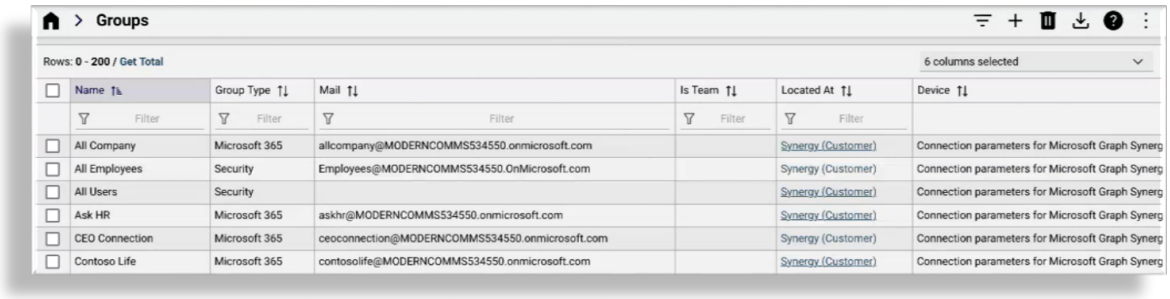
Note: Microsoft doesn't differentiate between Teams and Groups on the MS Entra ID portal so both the Teams and Groups list view and details page point to the same Automate model, `device/msgraph/Group`.

The **Groups** list view displays only high level data synced in from the Microsoft Portal. Clicking on a group in the list view triggers a live update from the Microsoft Entra ID portal to fetch additional details for the Group. This is to ensure efficient and fast data syncing for Teams and Groups from Microsoft Entra ID. Data syncs for Teams and Groups are handled in the same way in the Automate GUI.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Changes you make for groups in Automate updates the Microsoft online portal.

1. In the Automate Admin Portal, go to **Groups**.



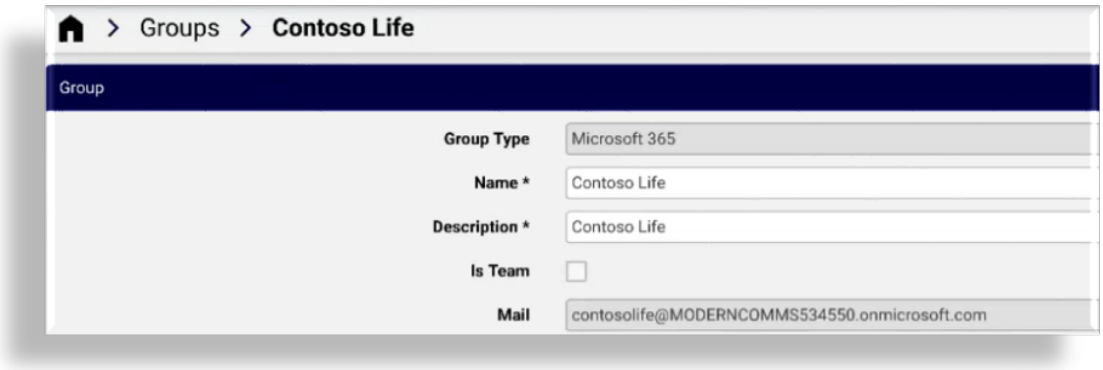
2. View existing groups in the list.

Note: The number of groups in the list view matches the number of groups in the Microsoft Portal.

3. **Do you want to** . . .
   - **View details for an existing group**? Click on a group in the list to view its details.

     Note:
     - Group members don't display on a group's detail page.
     - Assigned licenses display the friendly name (SkuPartNumber) of the Assigned License in the **SKU ID** field.
     - The **Is Team** flag is enabled only when the entity you're viewing is a Microsoft Team.

   - **Update a group**? Click on a group in the list view to open it's details page. Update the group details, then save.



   - **Delete a group**? Select the relevant group in the list view, or click on the group to view its details, then click the toolbar **Delete** icon.
   - **Add a group**? Click the toolbar **Plus** (+) icon to create a new record. Then add group details - select the group type, fill out a name and description, then save.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manage group membership

Tip: *Use the Action search to navigate Automate*

Overview

Automate allows you to add or remove Microsoft Teams Active Directory (AD) groups (and any associated group licenses) for a selected user.

This task can be carried out either the **Manage Group Membership** page for a particular user, or via Quick Add groups and related configuration templates: **MS Groups Add Template** and **MS Groups Remove Template**.

Related Topics

- *Microsoft Licenses* in the Core Feature Guide

Add or remove Microsoft Teams groups for a user

This procedure displays groups synced in from the Microsoft Teams cloud portal, and allows you to view a group's details.

1. In the Automate Admin Portal, go to **Manage Group Membership** to open the **Manage Group Membership** transfer box view.
2. Select an **Operation**, either add or remove.
3. Select a **User** from the drop-down list to whom the operation applies.
4. Under **Group**, select groups from the **Available** list and move them to the **Selected** list as required.
5. Click **Save**. In accordance with the selected **Operation**, the user is assigned to or removed from the groups in the **Selected** list.

Note:

- When adding, no change occurs if the user is already a member of the group.
- When removing, no change occurs if the user is not a member of the group.
- If the group in the **Selected** list has a MS license associated with it, the group license is then also added or removed from the user in accordance with the selected **Operation**.
- This **Manage Group Membership** transfer box is also available to be selected as a **Quick Action** for multi-vendor subscribers. See: *Quick actions for multi vendor user*.
- During the setup of Quick Add Group configuration templates to carry out these tasks, the **Operation** and **Group** as shown on this **Manage Group Membership** transfer box, is also selected. See *Microsoft Licenses* in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.1.2. Microsoft Detailed Configuration

MS Teams Network & Emergency Routing

Introduction to Microsoft Teams emergency management

VOSS Automate allows you to configure and manage all elements of emergency call routing for Microsoft Teams, from within the Automate Admin Portal.

There are two approaches to emergency call routing in Microsoft Teams:

- Location-based routing
- Dynamic emergency routing

The option you choose depends on how your sites are set up, the specific requirements of your organization, and the elements related to each option, which may be grouped as follows:

Emergency Locations	This is a group of details in MS Teams that models the Dynamic Emergency Routing elements - the Civic Address and all the related Location Information Server (LIS) details - Location, Subnet, Port, Wireless Access Point, and Switch.
Emergency Location Networks	This is for the additional emergency options not related to the Location Information Server (LIS) elements - Network Sites and Network Subnets. This can, for instance, help model routing to local security desks rather than directly to emergency services. This basically relates Network Sites and Subnets elements. This feature provides a read-only view to allow you to see Network Sites and related Subnets in a single view - editing either element is done via the dedicated menu item.
Trusted IP Addresses	Dedicated menu items in the VOSS Automate GUI allow the addition of IP Addresses or subnets external to the enterprise network that are to be trusted by the MS Teams system for location based services.

In addition to the basic setup for emergency routing, VOSS Automate allows you to create emergency policies and to assign these to users. The following policies are supported:

- Emergency call routing policy - used with direct routing
- Emergency Calling policy - used with Operator Connect and Calling Plans

Note: See the MS Teams policy management and subscriber management sections in the Core feature guides for further details.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *MS Teams emergency locations*
- *MS Teams emergency location networks*
- *Introduction to Microsoft Teams policies* in the Core Feature Guide

MS Teams emergency location networks

Tip: *Use the Action search to navigate Automate*

Overview

Automate provides a read-only overview of the elements related to Microsoft Teams emergency location networks for emergency calling, allowing you to view network sites and related subnets on a single page.

The table describes the elements that make up the emergency location networks:

Element	Description
Network Regions	Network regions can be used to logically group sites, for example, a campus, as required.
Network Sites	Network sites are location instances that group subnets and set emergency routing policies and behavior for those subnets. Network regions may align to VOSS sites, but this depends on your set up. Policies allow you to define where emergency calls are routing, for example, PSTN, or a local security desk.
Network Subnets	Network subnets are subnet instances tied to a network site. Devices and users in these subnets utilize the rules applied in the corresponding network site. Each emergency location network can have one or more subnets configured.

Related Topics

- *Introduction to Microsoft Teams emergency management*
- *MS Teams emergency locations*

Copyright © 2025 VisionOSS Limited. All rights reserved.

View configured MS Teams emergency location networks

To view configured emergency location networks, go to the **Teams Emergency Location Networks** page. This view also displays the policies associated with the networks (Emergency Calling Policy and Emergency Call Routing Policy).

Configure MS Teams emergency location network elements

Higher level administrators can view and edit the individual elements of MS Teams emergency location networks (sites and subnets) directly from the device models, via the following (default) menu paths in the VOSS Automate GUI:

- To edit sites, go to the **Network Site** page.
- To edit network subnets, go to the **Network Subnet** page.

  The subnet **Mask** is mandatory, and for IPv4 takes maskbits from 0 to 32 inclusive, while for IPv6 format, from 0 to 128 inclusive.

MS Teams emergency locations

Tip: *Use the Action search to navigate Automate*

Overview

VOSS Automate provides the ability to support all the elements related to emergency calling setup in Microsoft Teams, including Dynamic Emergency, which allows for the management of Microsoft Teams emergency locations for emergency calling.

You can set up one or more emergency dispatch locations (for example, parts of a building), for your organization's physical location (civic address).

Related Topics

- *Introduction to Microsoft Teams emergency management*
- *MS Teams emergency location networks*

Configure MS Teams emergency locations

1. In the VOSS Automate Admin Portal, go to the **Teams Emergency Locations** page.
2. Click on an item in the list to view or update its details.
3. To add an emergency location, click the toolbar Plus icon (+), and configure the new record:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Address tab	On this tab, configure emergency location details. • When adding a physical civic address, a default emergency location is added (the **Is Default** setting on the **Locations** tab is enabled and read-only for the location). • You can expose additional civic address fields via the field display policy, if required.
Locations tab	Add associated locations. Verify requirements according to the selected **Country Or Region**. For example, if this is set to UK, then it is mandatory to provide **HouseNumber**. This tab allows you to add more granular, additional locations for an address, as needed. And for each location, you can add relevant data from the Location Information Server (LIS), to identify the location. For example, subnet, port, switch, and wireless access points (WAP). Some details to this tab are mandatory, while others are optional (you can create the base civic address then add locations later), if you don't create a location when adding, MS Teams automatically generates a read-only default location, which you will see when viewing the emergency location later in VOSS Automate. You can add relevant LIS information to that default location. However, you won't be able to update the description or ELIN (Emergency Location Identification Number). You can add additional locations as needed. You can't delete the default location from the list of locations associated with a physical civic address. The default is only removed when the physical civic address is deleted. You can add relevant LIS information to the default location as required, which is useful if you plan to have only a single location for the address.

4. Save your changes.

MS Teams Voice Policies

Introduction to Microsoft Teams policies

Tip: *Use the Action search to navigate Automate*

Overview

Microsoft Teams policies in Automate are synced with Microsoft Teams at the customer level. Automate provides tools to manage these policies at both the customer and site levels. Changes made in Automate are synced to Microsoft Teams, and vice versa.

Policies are automatically assigned to users based on:

- Their roles and profiles (in the initial sync and provisioning workflow)
- Quick Add Groups (QAG) (in the initial sync and provisioning workflow)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Site Defaults settings (view and choose default policies per site on the **MS Teams** tab of the Site Defaults page)

Choosing a default policy for a site via the Site Defaults (**MS Teams** tab) automatically assigns the policy to users at the site. When creating a user via Quick User, the setting in the site defaults is used, but you can also edit the configuration template (CFT) for the Quick Add Group to use a policy different to the one selected in the site defaults, or you can edit a user directly to choose a different policy for that user.

Managing MS Teams policies

View and manage MS Teams policies via the **Microsoft Detailed Configuration** dashboard in Automate, or use the *Action search* to search for the policy in Automate.

- Calling policy
- Meeting policy
- Messaging policy
- Live Events policy
- Call park policy
- App permission policy
- App setup policy
- Teams policy
- Update policy
- Emergency calling policy
- Enhanced encryption policy
- *Voice application policy*
- Voice routing policy
- Voicemail policy
- Audio conferencing policy
- *Call hold policy (Microsoft Music on Hold)*
- *Survivable branch appliance policy*
- *Mobility policy*
- *Shared calling routing policy*

Some policies support full CRUD (Create, Read, Update, Delete) operations directly in Automate.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Microsoft Detailed Configuration dashboard
- Microsoft Users in the Core Feature Guide
- Site Defaults in the Core Feature Guide
- Quick Add Groups in the Core Feature Guide

Shared calling routing policy

Automate supports full CRUD (create, update, delete) for Microsoft Shared Calling Routing policy.

Note: This policy is integrated with CsOnlineUser (CSOL) so that management of user details and Shared Calling Routing policies are synced between Automate and the MS Teams portal.

---

1. At the customer level of the site defaults, on the **MS Teams** tab, select the Shared Calling Routing policy.

   Note: When onboarding the user via Quick Subscriber, the Shared Calling Routing policy selected in the site defaults is the policy assigned to the user.

   ---

2. To view, update, or delete existing Shared Calling Routing policies or add new Shared Calling Routing policies, go to **Shared Calling Routing Policy**.

   The list view displays existing Shared Calling Routing policies.

   - Select a policy in the list to delete it.
   - Click on an existing policy to update it.
   - To add a new Shared Calling Routing policy, click the Plus icon (+), then:
     - Fill out a name and description
     - Select a resource account
     - Add emergency callback numbers, one or more, if required.
     - Save the new policy.
3. To assign or update the Shared Calling Routing policy for a Microsoft user provisioned with MS Teams, go to **Microsoft User Details**, click on the relevant user to view their settings, then, to assign or update the policy, select the Shared Calling Routing policy for this user.

Call hold policy (Microsoft Music on Hold)

To create or update a call hold policy for Microsoft Teams, an audio file (MP3, WAV, and WMA and file size less than 5 MB) upload is required. Go to the **File Management** page for this task.

Thereafter, the **Audio file** drop-down list will show the file and can be selected to create or manage the policy.

Note:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The Call Hold policy name can't be changed upon policy updates.
- The audio file names of imported call hold policies are initially undetermined and are represented by a hash value. Subsequent syncs of the policy will resolve existing hash values to filenames.

Survivable branch appliance policy

If the Microsoft Teams client is in offline mode, the Teams Phone operations can be made available by a Survivable Branch Appliance (SBA) Policy. This allows for the placement and reception of Public Switched Telephone Network (PSTN) calls during service disruptions.

Survivable Branch Appliance Policy (SBA Policy) management is available from the **MS Teams Policies** menu. The policy can then be assigned to users, Quick Add Groups and set in Site Defaults.

The following policy fields can be managed at a hierarchy:

- **Identity**: The identity of the SBA
- **Fqdn** The FQDN of the SBA

Mobility policy

Microsoft's Teams Phone Mobility policy is assigned to a user that is given a Teams Phone Mobile number via Quick User, or you can assign the policy to an existing user via User Management. This policy tells the system where to route incoming calls, for example, to your mobile phone or to your Teams application.

Full CRUD is supported for this policy from within Automate. Changes are synced between Automate and the Microsoft Cloud portal. The Mobility policy is added to Automate via the site defaults, where you can assign a different mobility policy per site, or assign the policy at the customer level.

Automate admins onboard and provision Teams Phone Mobile users via Quick User, where the user can be assigned their Teams Phone Mobile license via a license group in a Quick Add Group. The license group can be removed for that user when they're offboarded. The policy is also assigned when updating an existing Microsoft user and choosing a Teams Phone Mobile number to the user.

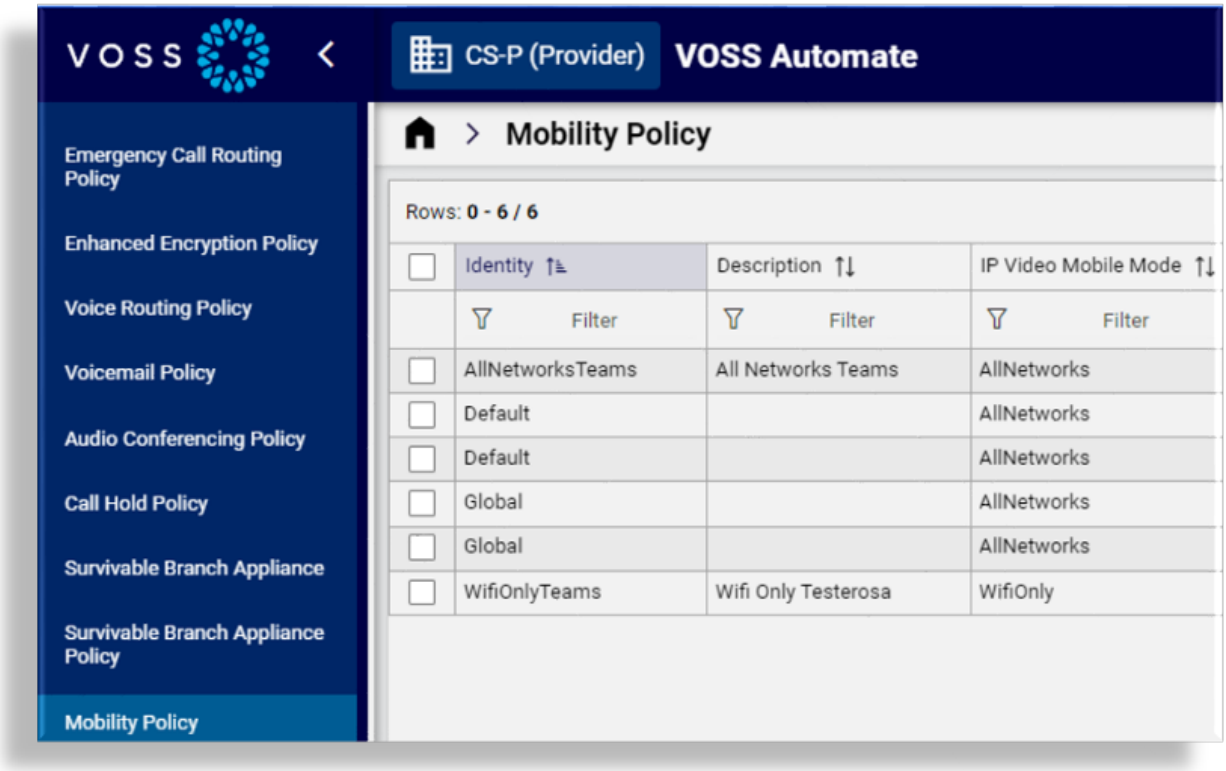
Teams Phone Mobile users are assigned numbers reserved for this functionality in the Automate number inventory. These numbers won't be available to anyone else even if a user with a Teams Phone Mobile number is offboarded.

Add a mobility policy

Mobility policies can be added on the MS Teams Cloud portal and synced in to Automate, or you can add a mobility policy from within Automate and sync the policy into the MS Teams Cloud portal. This procedure adds a mobility policy in Automate.

1. In the Automate Admin Portal, go to **Mobility Policy**. Existing mobility policies display in the list view.
2. Click the Plus icon (+) to add a new mobility policy.
3. Fill out an identifying name (**Identity**) and optionally, a description.
4. Optionally, select a mode for IP video and/or IP audio mobile, either WiFi only, or all networks.
5. Optionally, select a mobile dialer preference, either Teams, native, or user override.
6. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Apply the mobility policy to a site or customer

1. Go to **Defaults** (for a site or at the customer level).
2. On the **MS Teams** tab/panel, at **Default Mobility Policy**, select the mobility policy to apply at the site or customer.
3. Save your changes.

Assign a policy to a user

Mobility policies can be assigned automatically when onboarding a Microsoft user via Quick User, or you can modify a user and apply a mobility policy. To assign a policy to an existing user, see *Manage a user's MS Teams policies*

Related topics

- *Onboard user (Microsoft)*
- *Manage a user's MS Teams policies*
- *Quick Add Groups*
- *Microsoft Quick User*

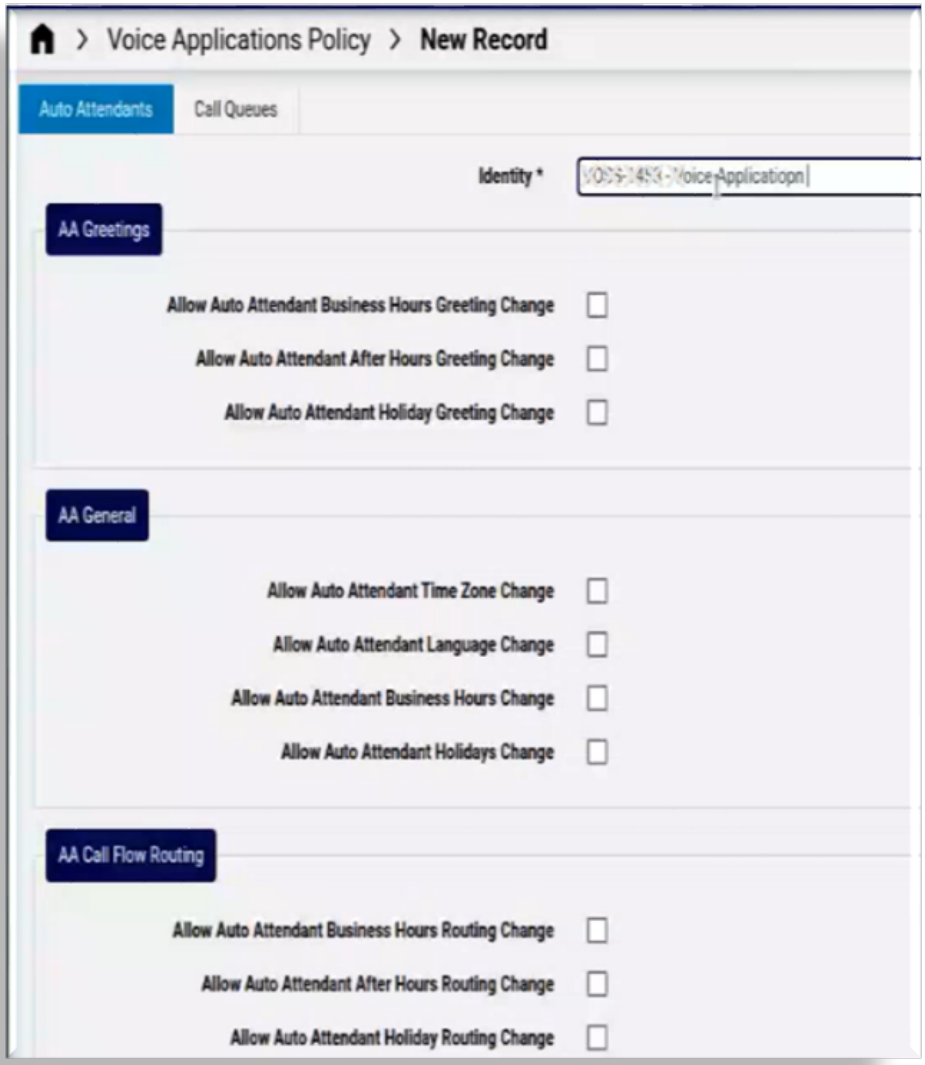
Copyright © 2025 VisionOSS Limited. All rights reserved.

Voice application policy

Microsoft Voice Application policies define the configuration changes an authorized user can make to the call queues and auto attendants they're authorized for. Automate allows full CRUD (create, update, delete) for the voice application policy from within Automate, and any changes made in either Automate or the Microsoft Teams portal are synced between these two platforms.

The voice applications policy can be assigned to a user in Quick User (from the site defaults), or a different voice applications policy can be assigned, via Automate's user management functionality.

MS Teams voice policies, including the voice application policy, is available, by default, on the **MVS-MSDialPlan** dashboard.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *MS Teams tab*
- *Quick Add Groups*
- *Manage a user's MS Teams policies*

Set up Automate for voice application policies

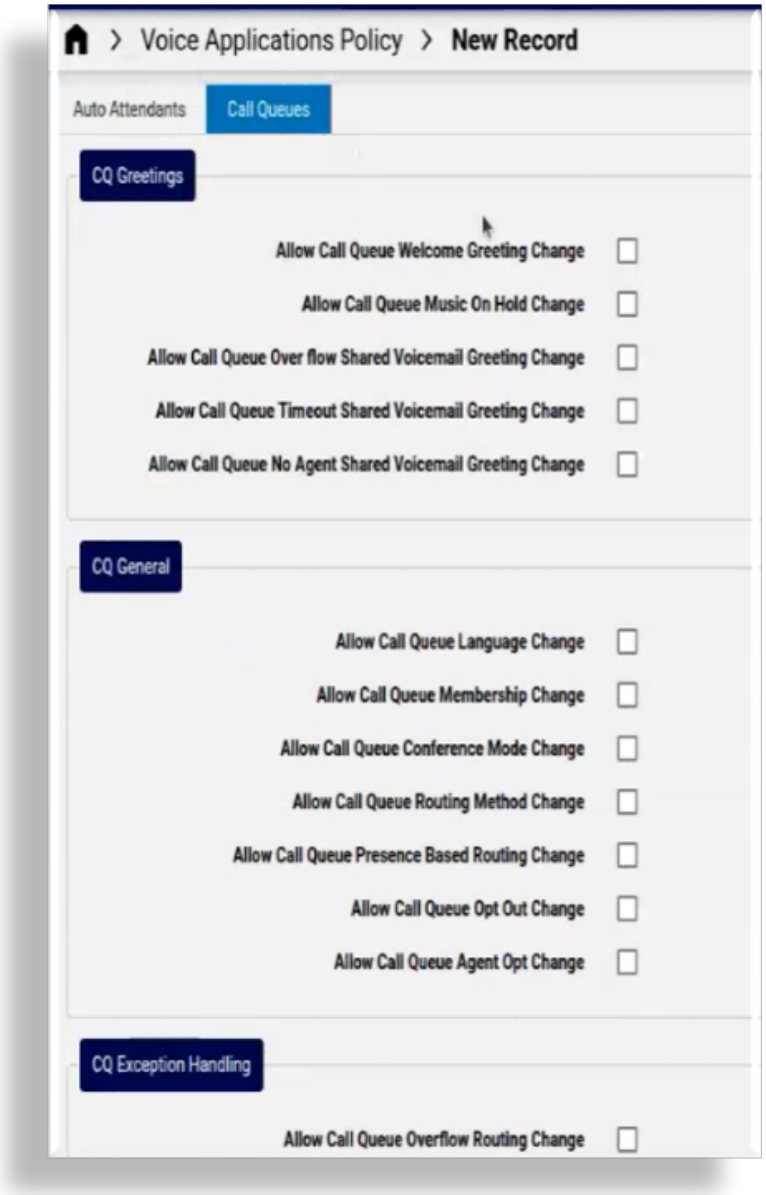
To set up Automate for managing Microsoft's Voice Application policies:

1. Add and configure voice applications policies, one or more.
2. On the **MS Teams** tab in the site defaults at the customer level, choose the default voice applications policy to apply.
3. Assign the voice applications policy to a user via Quick User or via Automate's user management functionality.

Manage voice application policies in Automate

1. In the Automate Admin Portal, go to the **Voice Applications Policy** page.
2. View existing voice application policies in the list view.
3. Choose an option:
   - **Delete a voice application policy**? Select the policy in the list, then click the toolbar **Delete** icon.
   - **Update a voice application policy**? Click on a policy in the list to view its details. Update the policy, then save.
   - **Add a new voice application policy**? Click the Plus icon (+) to add a new record. Configure the voice applications policy settings for auto attendants and call queues, then save your changes.
     - Auto attendant settings for the voice application policy include settings for greetings, time zone, language, holiday and business hours, routing changes, and reporting permissions
     - Call queue settings for the voice application policy includes settings for greetings, general settings such as whether to allow call queue language, membership, or conference mode changes, as well as settings for exception handling, agent monitoring, and reporting permissions

Copyright © 2025 VisionOSS Limited. All rights reserved.



Introduction to Microsoft Teams dial plan management

Tip: *Use the Action search to navigate Automate*

To view and update information related to Microsoft Teams dial plans, go to one of the following items in the GUI, depending on the details you wish to view and update:

- Tenant Dialplan
- SBC Gateways
- PSTN Usages
- Voice Routes

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Voice Routing Policies
- Voice Normalization Rules
- Translation Rules

Automate also allows you to predefine dial plan templates for Microsoft data models, and to push the dial plan, on-demand. For details, see *Microsoft dial plan models*

Related topics

- *Microsoft dial plan models*
- Microsoft overview in the Core Feature Guide
- Sync to site with flow through in the Core Feature Guide
- Automate configuration and sync in the Core Feature Guide
- Configure Microsoft tenant dial plan in the Core Feature Guide
- Number management overview in the Core Feature Guide
- Prevent duplicate numbers in the Core Feature Guide

Microsoft dial plan models

Overview

Automate supports the ability to predefine dial plan templates for Microsoft data models, and to push the dial plans, on-demand, for a specific customer or site.

Microsoft dial plan models workflow

To use this feature:

1. Ensure you have the **Dial Plan Management Tool** menus exposed in the Admin Portal:
   - In the Global Settings, ensure **Enforce HCS Dialplan Rules** is set to *No*.
   - Log in with an access profile that has permissions to the **Dial Plan Management Tool** menus.

   Note:
   - The **Dial Plan Input Data** menu is relevant only for Cisco dial plans.
   - For Microsoft dial plans, include the Microsoft Dial Plan Models menu and Microsoft models in your menu layout.

2. *Create the dial plan name*
3. *Create data models*
4. *Preview a configured dial plan*
5. *Push a dial plan to customer or site*

Copyright © 2025 VisionOSS Limited. All rights reserved.

The following Microsoft data models and corresponding device models (Microsoft dial plan elements) are supported:

Device Model	Menu
device/msteamsonline/CsTenantDialplan	Tenant Dialplan
device/msteamsonline/CsOnlinePstnGateway	SBC Gateways
device/msteamsonline/CsOnlinePstnUsage	PSTN Usages
device/msteamsonline/CsOnlineVoiceRoute	Voice Routes
device/msteamsonline/CsOnlineVoiceRoutingPolicy	Voice Routing Policies
device/msteamsonline/CsTeamsTranslationRule	Translation Rules

Additional Microsoft device models have been added to offer providers a one-step in the customer onboarding process: pushing provider-specific dial plan elements as well as Teams polices to the customer's tenant.

The following Microsoft device models are supported. The equivalent data models have names that match the device model name as follows:

`DP_msteamsonline_<device model name>`

For example, `DP_msteamsonline_CsOnlineVoicemailPolicy`.

Device Model	Menu
device/msteamsonline/CsCallingLineIdentity	Calling Line Identity[1]
device/msteamsonline/CsOnlineVoicemailPolicy	Online Voicemail Policies
device/msteamsonline/CsTeamsCallingPolicy	Calling Policies
device/msteamsonline/CsTeamsCallParkPolicy	Call Park Policies
device/msteamsonline/CsTeamsEmergencyCallingPolicy	Emergency Calling Policies
device/msteamsonline/CsTeamsEmergencyCallRoutingPolicy	Emergency Call Routing Policies
device/msteamsonline/CsTeamsEnhancedEncryptionPolicy	Enhanced Encryption Policies

Related topics

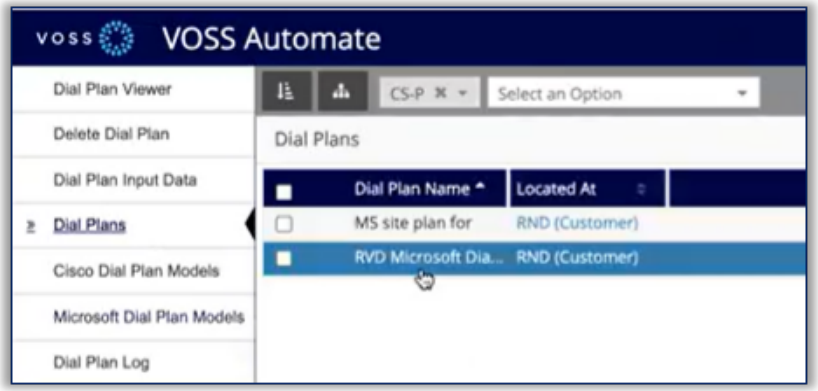
- *Cisco Custom Dial Plans*
- *Dial Plan Management Tool*
- *Dial Plan Viewer*
- *Dial Plan Maintenance*
- *Cisco dial plan models*

[1] When adding an instance by creating a data model (*Create data models*) and if **Calling ID Substitute** is set to `Resource Account`, a Resource Account which has a number can be selected.
The **Calling Party Name** is also visible and can be configured.

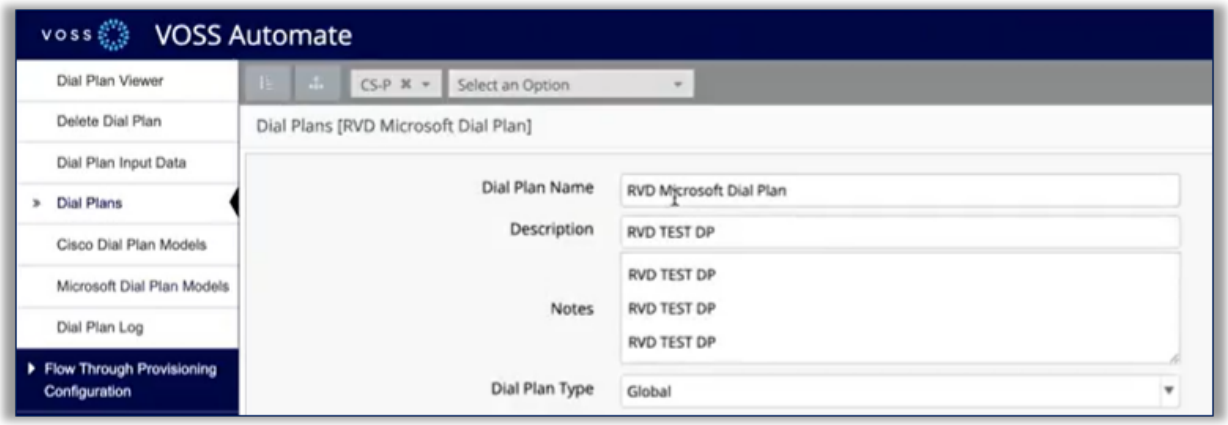
Copyright © 2025 VisionOSS Limited. All rights reserved.

Create the dial plan name

1. Go to **Dial Plan**.

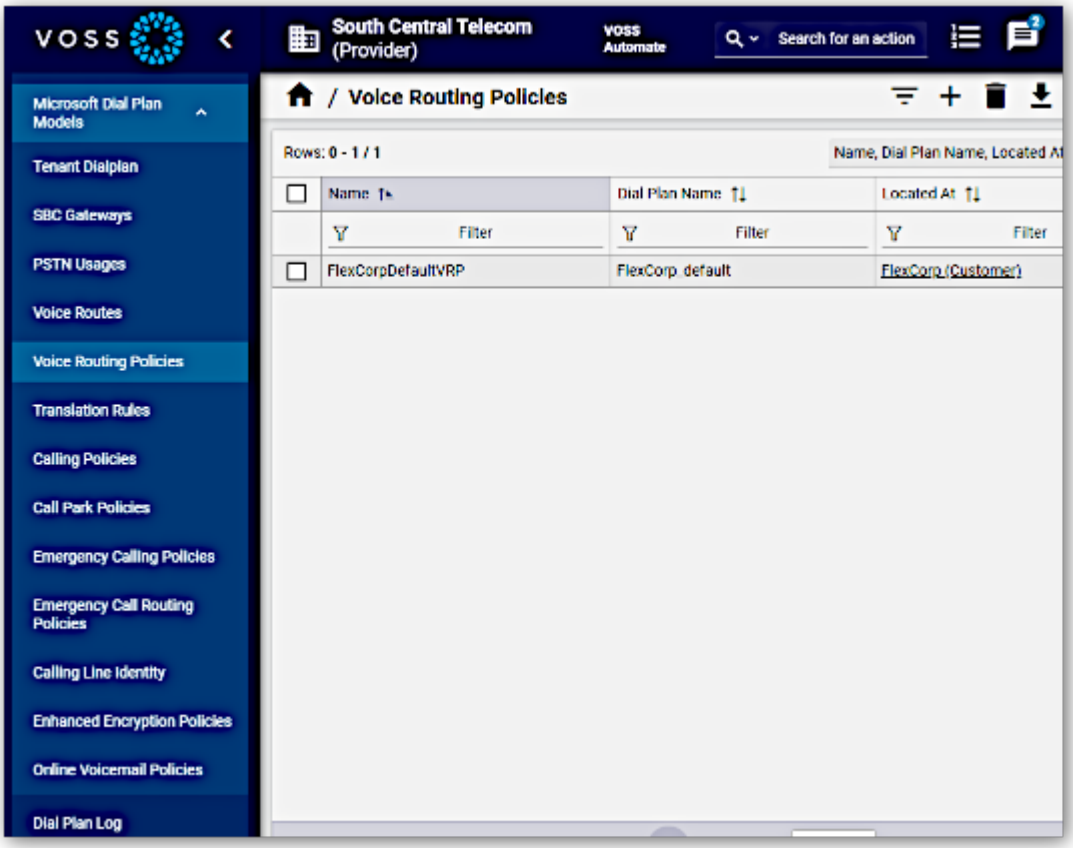


2. Click **Add**.
3. Fill out a dial plan name, and a description.
4. At **Dial Plan Type**, choose an option, either Global, Site, or Multi-tenant / Shared Architecture.



5. Save.
6. Next steps: Create the data models, with their data.

Copyright © 2025 VisionOSS Limited. All rights reserved.



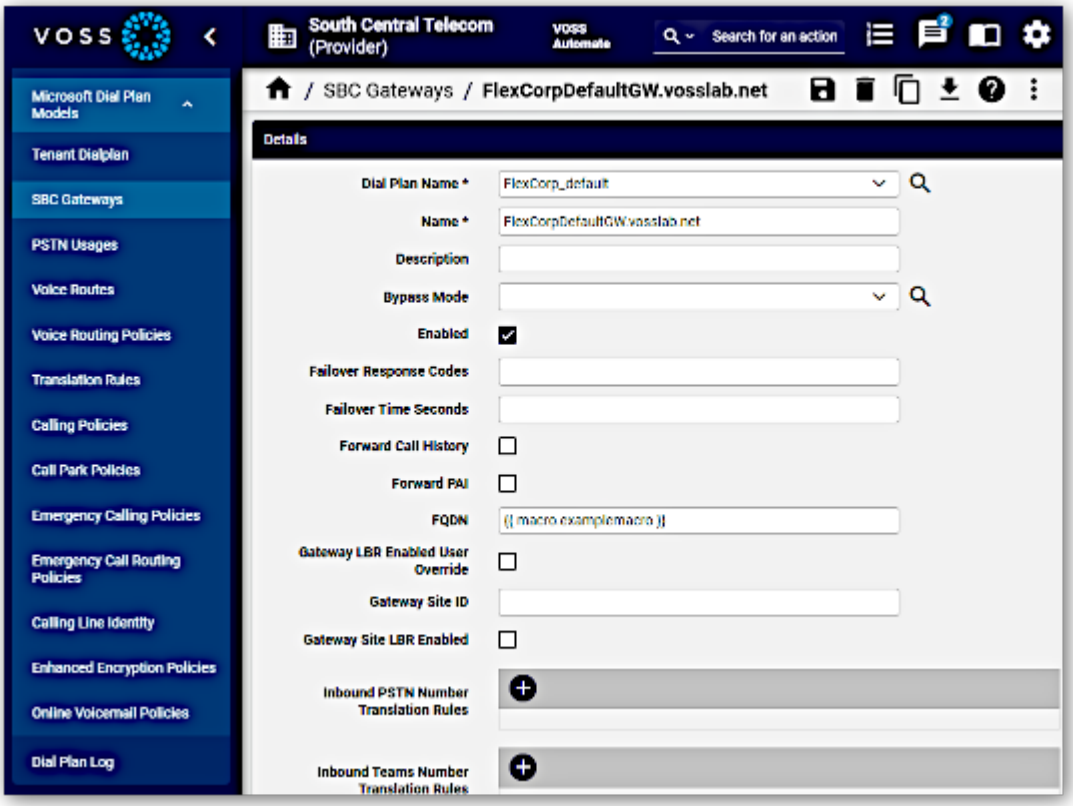
Create data models

Once you have a dial plan name you can create the data models with data in them.

1. Go to **Dial Plan Management Tool > Microsoft Dial Plan Models**.
2. Click on the relevant model.
3. Click **Add**.
4. Fill out data for the model:
   - Choose the dial plan name.
   - Configure data for the model.

Note: You can also use macros to add values in some fields.

Copyright © 2025 VisionOSS Limited. All rights reserved.



5. Save.

   The details you provided goes to the data model.

6. Next steps: Repeat this procedure to fill out data for any other models (if required) to build out your dial plan, then preview the dial plan you configured.

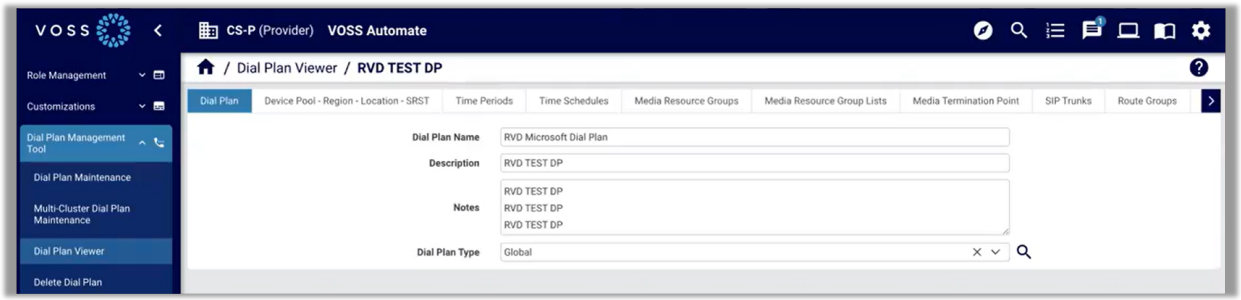
Preview a configured dial plan

You can preview dial plans via the **Dial Plan Viewer**, which provides a read-only view of all data model entries added to a selected dial plan name.

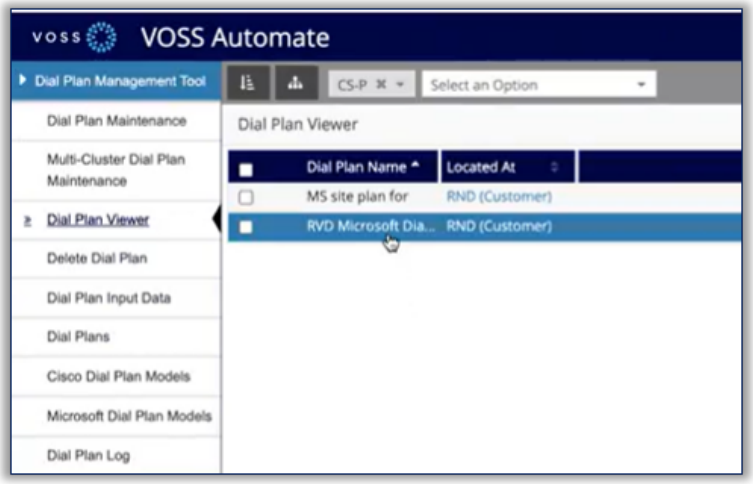
Note: The Dial Plan Viewer displays read-only data. You cannot add or update any model entries via the Dial Plan Viewer. You can modify your data entries via the menus, then return to the viewer to see your changes, if required.

If you have data model entries added to a dial plan name for both Cisco and Microsoft dial plan models, these are all accessible for inspection in the tabs of the Dial Plan Viewer.

Copyright © 2025 VisionOSS Limited. All rights reserved.



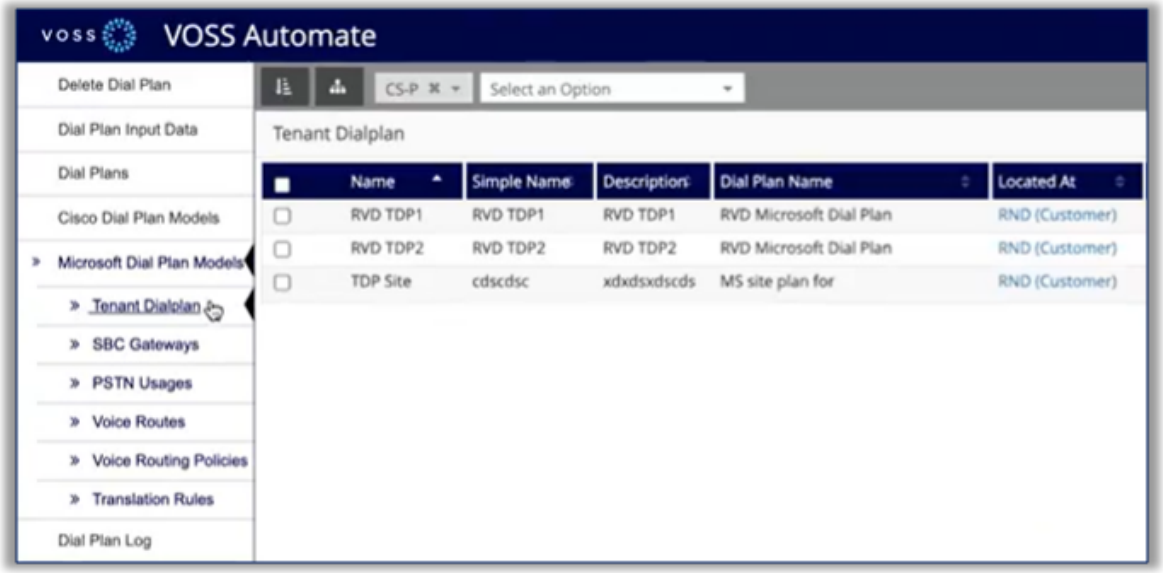
1. Go to **Dial Plan Management Tool > Dial Plan Viewer**.
2. In the **Dial Plan Viewer** summary list, click on the relevant dial plan name.



3. The tabs of the **Dial Plan Viewer** display the data for each data model entry created for the selected dial plan name.

Note: A dial plan can contain entries for both Cisco and Microsoft dial plan models, allowing you to push dial plans to both CUCM clusters and to the Microsoft tenant (for Microsoft Teams).

Copyright © 2025 VisionOSS Limited. All rights reserved.



4. Next steps: Push the dial plan, to a customer or to a site.

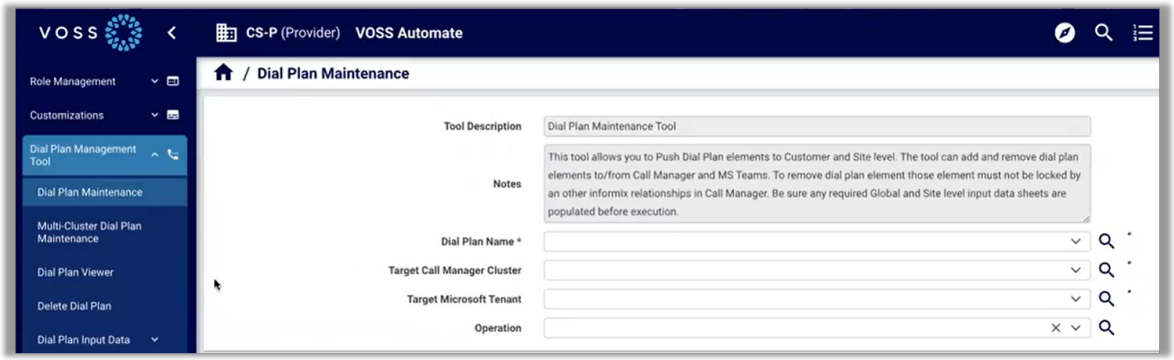
Push a dial plan to customer or site

The Dial Plan Management Tool can push dial plan data to a customer or to a site, to the Microsoft tenant and to CUCM clusters, depending on the hierarchy where you created the dial plan, and on the data model entries included in your dial plan.

Important: If your dial plan is configured at a specific customer hierarchy, you'll need to push it from that hierarchy. If a dial plan is added at a site, it must be pushed to the site at that hierarchy.

1. Choose the hierarchy where you added your dial plan (a customer or site).
2. Go to **Dial Plan Management Tool > Dial Plan Maintenance**.
3. At **Dial Plan Name**, select the name of the dial plan you wish to push to the site or customer.

   Note: The **Dial Plan Name** drop-down lists dial plan names added to the current hierarchy.



Copyright © 2025 VisionOSS Limited. All rights reserved.

4. From **Target Call Manager Cluster** and **Target Microsoft Tenant**, choose the relevant target destination for the dial plan, either a CUCM cluster or a Microsoft tenant, or both, provided you have these added to your system.
5. From the **Operation** drop-down, choose an option, either **Push Dial Plan** or **Remove Dial Plan**. To push your dial plan, select **Push Dial Plan**.
6. Click **Save**.

   The relevant workflows are triggered to determine the content of the dial plan you defined. The dial plan data is pushed to the target (CUCM cluster or Microsoft tenant, as applicable).

   For Microsoft, the dial plans are added to the Microsoft Tenant in Automate (accessible via the default menus as **MS Teams Dial Plan Management > Tenant Dialplan**), and the dial plan details are also updated to the Microsoft Teams cloud portal.

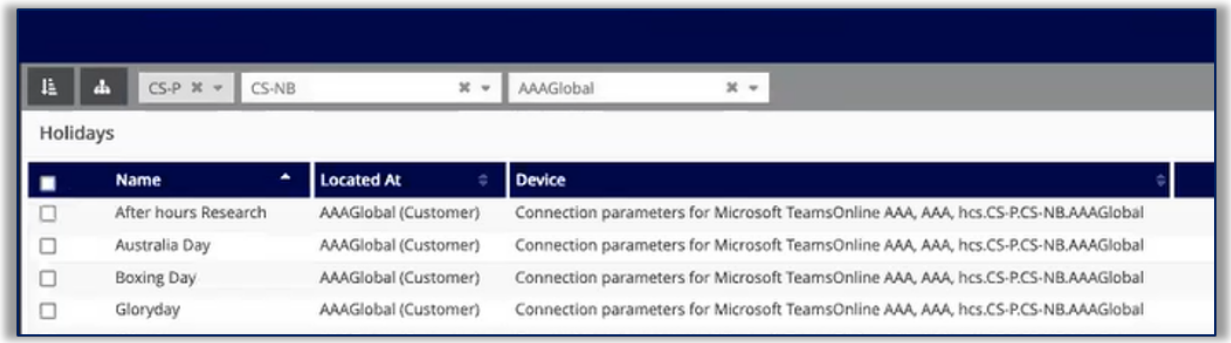
MS Auto Attendant Setup

Holidays

Tip: *Use the Action search to navigate Automate*

VOSS Automate allows you to add, edit, and delete holidays (days where your business is closed due to holidays in your region). On holidays, you may want to automate how incoming calls are routed.

To access this feature, go to **MS-Teams Holidays** to open the Holidays list view for Microsoft subscribers.

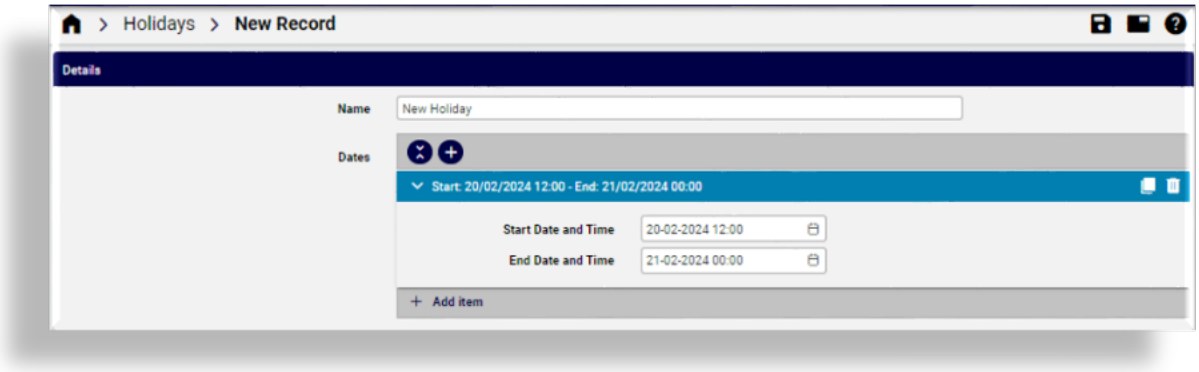


Click the Plus icon (+) in the list view to create a holiday. Or click a holiday in the list view to update it or delete it.

Note: You can set a start date and time, and an end date and time. The time selection is in 15 minute intervals.

Changes you make in VOSS Automate or in Azure are synced.

Copyright © 2025 VisionOSS Limited. All rights reserved.



MS Teams Meetings & Messaging Policies

MS Teams templates

Tip: *Use the Action search to navigate Automate*

Automate allows you to import templates from the Microsoft Teams online portal. You can view the settings for these teams templates, and apply templates to the teams you can manage from within Automate.

From within Automate, you cannot add, modify, or delete teams templates.

Note: Microsoft teams templates can be used to create teams, channels, and apps that will be available to users with common needs or a common project.

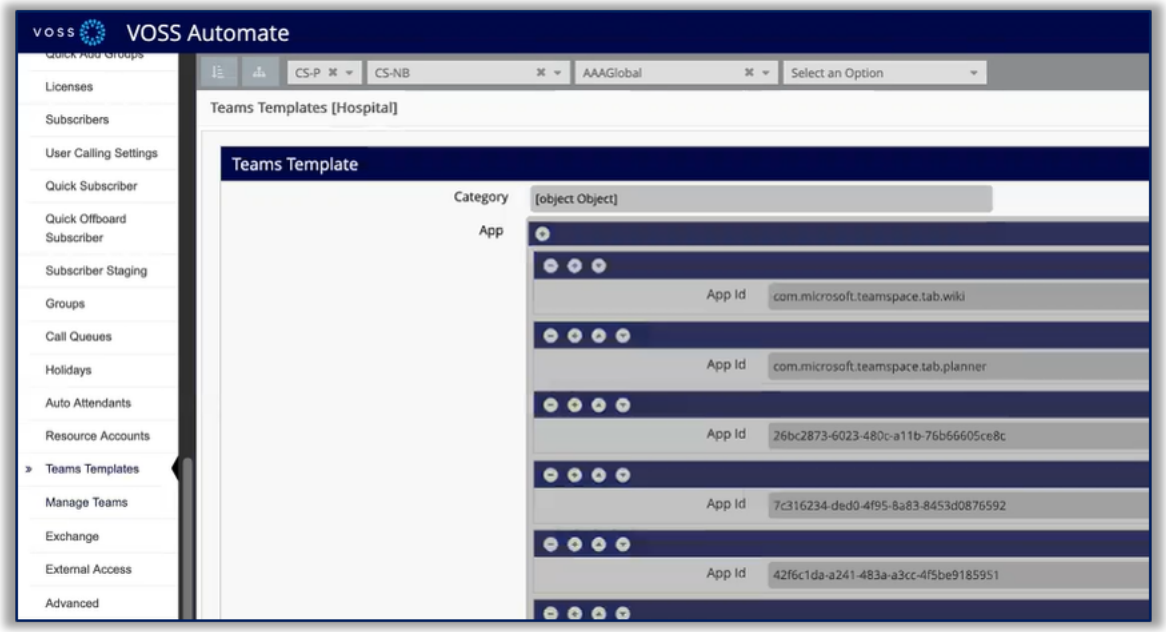
A Microsoft end user, working through a Microsoft client (desktop or phone), can add a team from a team template that has been pre-configured with resources, such as team-specific channels or applications. Users added to the team will then have access to the resources set up for the team via the template.

To view Microsoft teams templates from the Automate Admin Portal, go to **Teams Templates**. Click on a template in the list to view its settings.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Teams*



MS Teams Dialplan

Configure Microsoft tenant dialplan

Tip: *Use the Action search to navigate Automate*

This procedure displays and edits existing Microsoft Teams tenant dialplans and adds a new Microsoft Teams tenant dialplan.

Note: A default tenant dialplan can be chosen in the site defaults. When adding a user via Quick Add User, the default tenant dialplan can be overwritten if you choose another option.

Prerequisites:

- Add a Microsoft tenant

Perform these steps:

1. Log in to the Admin Portal.
2. Go to **Tenant Dialplan**.
3. View existing tenant dialplans.
4. Choose an option:
    - To edit an existing dialplan, click on a dialplan to open its configuration settings. Make your changes, then save the dialplan.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To add a new dialplan, click the Plus icon (+) to open the New Record screen. Go to step 5.

5. On the **New Record** page, fill out details for the new Microsoft tenant dialplan:
   - In the **Name** field, fill out a unique name for the dialplan.
   - In the **Simple Name** field, fill out a unique display name for the dialplan.
   - In the **Description** field, describe the purpose and users of the dialplan.
   - In the **External Access Prefix** field, define a prefix used to identify external calls. To enable this prefix, select **Optimize Device Dialing**.
   - Select **Optimize Device Dialing** to enable the external access prefix.
   - At **Normalization Rules**, click the Plus icon (+) to add a normalization rule:
     - Provide a unique ID for the normalization rule, and a description.
     - Define the priority order of this rule, for phone numbers associated with two or more normalization rules.
     - In the **Pattern** field, provide a regular expression that a dialed number must match for the rule to be applied. The default is *^(d{11})$*, which represents any set of numbers up to 11 digits.
     - In the **Translation** field, define a regular expression to apply to the number to convert it to E.164 format. The default is +$1, which prefixes the number with a Plus (+).
     - Select **Is Internal Extension** if the number should be seen as internal when the rule is applied (set to True); else, clear the checkbox (False, default), so that the number is seen as external when the rule is applied.
     - To add additional normalization rules, click the Plus icon (+) and fill out values for the next normalization rule.
6. Click **Save** to create or update the tenant dialplan.

Related topics

- Microsoft tenant setup in the Core Feature Guide
- Introduction to Microsoft Teams dialplan management in the Core Feature Guide
- Microsoft overview in the Core Feature Guide
- Sync to site with flow through in the Core Feature Guide
- Configure Automate for Microsoft services in the Core Feature Guide

MS Numbers

Tip: *Use the Action search to navigate Automate*

The **MS Numbers** page lists Microsoft Teams phone numbers synced in from Microsoft tenants, allowing Automate to stay in sync with the numbers that the Microsoft tenant stores, and is used to update Automate's number inventory data.

Click on a number in the list view to view further details for the number. At the time of writing (for Automate 24.2-PB1), most phone number properties are read-only.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Prevent duplicate numbers*

MS Blocked Calling Numbers

VOSS Automate allows for the management of Microsoft Call Blocking features if the **Global** setting for **Tenant Call Blocking** is enabled at tenant level (*Tenant Blocked Calling*).

The functionality will then be available to administrators:

- Menu: **MS Blocked Calling Numbers**
- Dashboards: the **MS Blocked Calling Numbers** widget on `MVS-Operations-CallBarring-Blocking-Dashboard` and `MVS-MSDialPlan-Dashboard`

Administrators can then:

- List all blocked and exempt number patterns added to the tenant list, including Name, Description, Enabled (True/False), and Pattern.
- Add a blocked or exempt number pattern to the tenant list.
- Remove (exempt) a blocked number pattern from the tenant list.
- Modify one or more parameters of a blocked or exempt number pattern in the tenant list.
- Test whether calls from a given phone number will be blocked (*Test IBN Pattern*).

Note: If the same number pattern is present in both the blocked and exempt pattern lists, numbers matching these patterns will be considered to have been unset, i.e. neither blocked nor exempt.

Tenant Blocked Calling

This list view shows the inbound block number patterns and the inbound exempt number patterns parameters by **Enabled** status of the **Global** blocked number list setting at a particular hierarchy, as shown in the **Located At** column of the list.

Inbound Blocked Number Patterns

The list view of all blocked number patterns according to hierarchy, showing whether the filter is enabled as well as its pattern and any details added.

- **Identity** is a unique identifier to specify the blocked number pattern to be created.
- **Description** is a friendly description for the blocked number pattern.
- **Enabled** is a parameter set to True or False, indicating if numbers matching the pattern will be blocked.
- **Pattern**: A regular expression to match the calling number, for example the pattern `^\+11234567890` blocks numbers starting with a `+` followed by the specified digits. It is best practice to start a regular expression with the caret (`^`) character and end it with the dollar (`$`) character to indicate the start and end of the pattern.

Entries can be added and modified from this list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Inbound Exempt Number Patterns

The list view of all exempt numbers patterns according to hierarchy, showing whether the filter is enabled as well as its pattern and any details added.

- **Identity** is a unique identifier to specify the exempt number pattern to be created.
- **Description** is a friendly description for the exempt number pattern.
- **Enabled** is a parameter set to True or False, indicating if numbers matching the pattern will be exempt.
- **Pattern**: A regular expression to match the calling number, for example the pattern `^\+?1312555888[2|3]$` exempts numbers optionally starting with a `+` followed by the specified digits and ending with either `2` or `3`.

Entries can be added and modified from this list.

Test IBN Pattern

Enter a number to test if it will be blocked or exempt for inbound calls by currently enabled patterns.

Microsoft License Management Mapping Configuration

6.2. Webex App Integration and Detailed Settings

6.2.1. Introduction to Cisco Webex App

Overview

Cisco Webex is a cloud-based business collaboration service that allows employees to message, meet, and call instantly in order to strengthen relationships and increase productivity.

Cisco Webex combines mobile devices and other communications tools to provide instant communications and live meetings to ensure a professional and effective collaboration experience.

The image displays the **Webex Overview** dashboard:

Copyright © 2025 VisionOSS Limited. All rights reserved.

The table describes the main Cisco Webex features:

Feature	Description
Messaging	Business messaging allows users to prepare, share, and repeat content, and it facilitates one-on-one or team messaging facilities in virtual rooms.
Meeting	Connect teams and meet customers easily with the added benefits of messaging and content sharing before, during, and after a meeting.
Call	The service enables voice and video communications via mobile, desktop, and room-based devices. Connect your existing PSTN1 services to Cisco Webex to enjoy one-touch directory dialing and join meetings from anywhere on any device. Mobile users get features such as single number reach, single voicemail service, video services, and the ability to seamlessly move between devices during a call.

Related Topics

- *Webex servers*
- Add Cisco Webex services (See *Webex Application Access (Webex Organization)* in the Core Feature Guide)
- Cisco Webex Users:
  - *Cisco Webex App users*
  - *Bulk update Webex App users*
  - *Webex App licenses*
  - *Add a user* (Webex App tab)

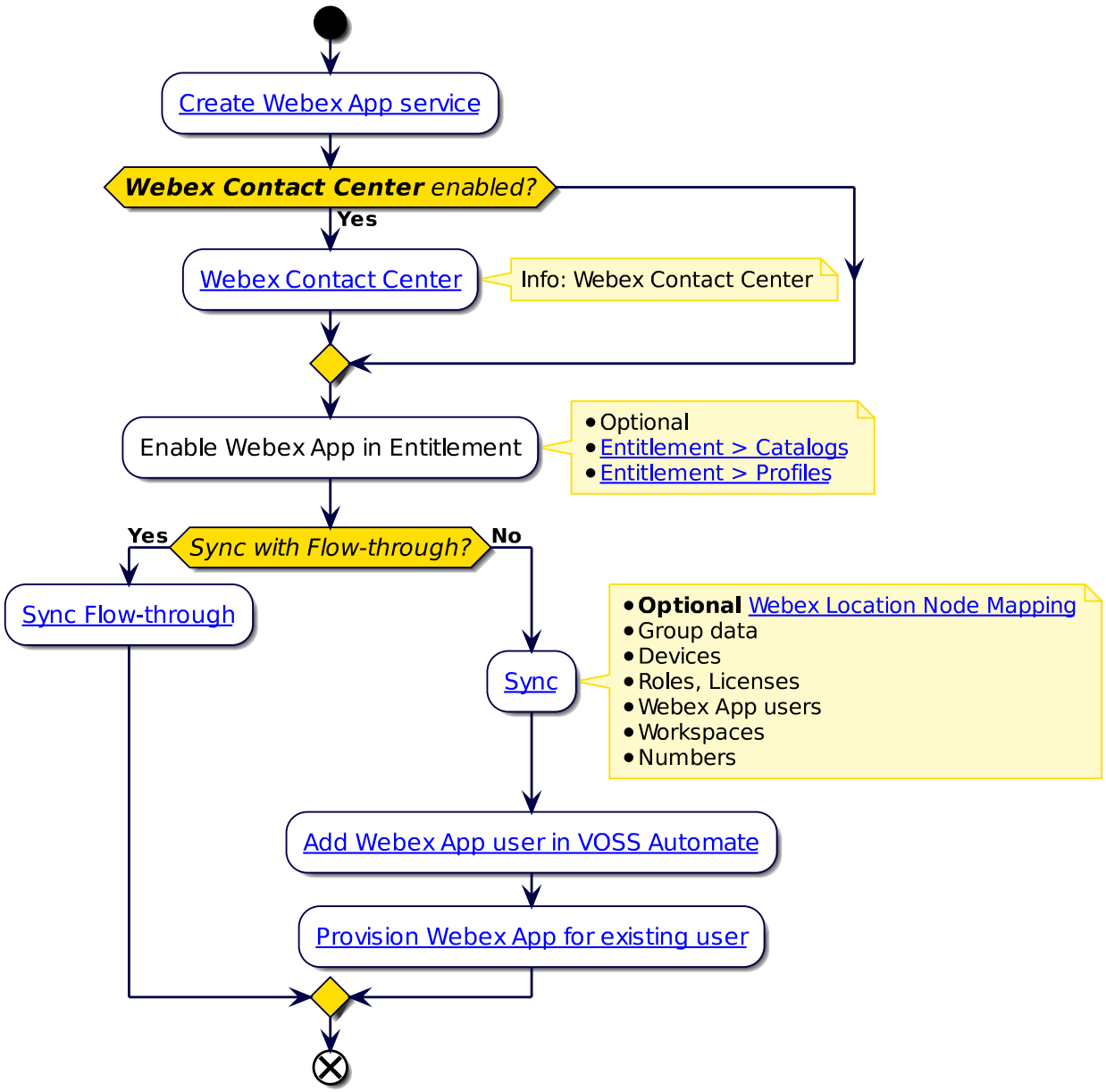
Copyright © 2025 VisionOSS Limited. All rights reserved.

- Cisco Webex Workspaces:
  - *Webex Workspaces*
  - *Webex App manual steps*
- Cisco Webex Locations
  - *Webex locations*
- Cisco Webex App Devices
  - *Webex devices*
- Webex Contact Center

  Introduction to Webex Contact Center

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate workflow for Cisco Webex



Webex App sync

Default Webex Calling data sync

Note: From release 25.1, Webex Contact Center sync excludes an updated device model instances list for Webex Calling sync - see the exclusion list at: *Webex Contact Center sync*. In particular, device models have been added to support call handling over trunks to Webex supported devices:

- `device/spark/DialPlans`
- `device/spark/RouteGroups`

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `device/spark/Trunks`

The default Webex Calling sync that is used to sync Webex Calling data and is available from the Data Sync list applies:

- **Model type list**: `SparkDataAllMTL`
- **Synchronization order**: `SparkDataSyncOrder`

This list type contains an *empty ``exclusion`` list*, that is, all device model instances are synced. If you need to exclude any models then you can update this list.

Default synced models

```
device/spark/Organization
device/spark/Role
device/spark/License
device/spark/CallingProfile
device/spark/LocationFloor
device/spark/Location
device/spark/User
device/spark/UserConfig
device/spark/Place
device/spark/Group
device/spark/Team
device/spark/Room
device/spark/Number
device/spark/AutoAttendants
device/spark/CallPickup
device/spark/LocationCallingDetails
device/spark/CallParkGroup
device/spark/Announcements
device/spark/Schedules
device/spark/CallParkExtensions
device/spark/HuntGroup
device/spark/WorkspaceCallSettings
device/spark/ActivateDevice
device/spark/Floor
```

Sync existing Cisco Webex users for a customer

Tip: *Use the Action search to navigate Automate*

A default sync schedule has the following name format: `SyncSpark-SCHED-XXX`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Two sync methods

- On the **Customer Access** page, click **Action > Sync Webex App Users**
- On the **Data Sync** page, execute **SyncSpark[Customer]** to run a sync

Important: To properly sync in calling behavior settings, ensure the sync setting **Quick Import** is set to *False* (disabled), and **Refresh Existing (Changed) Data** is set to *True* (enabled) on *all* data syncs that include the *device/Spark/user* model. By default, these are:

- *SyncSparkUsersXXX*, and
- *SyncSparkXXXX*

These are the default settings for the *device/spark/User* syncs, but it is important to ensure they correctly configured before syncing in users.

Note: When syncing in Webex data to Automate from the Control Hub, Automate's device models apply the `WebexAppCallingLicenseNameWKSP` macro in the provisioning workflows and syncs to check for the following license types, both of which are considered valid calling licenses:

- Webex Calling - Workspaces
- Webex Calling - Professional

The license checks allow the system to determine whether a device or number should be retained in a sync, preventing unintended deletions.

Synced in Webex numbers

Webex numbers are synced in and maintained in `device/spark/Number` and the Number Inventory.

The numbers of synced in Cisco Webex users display the following settings and values in the Number Inventory (see *Number status and usage*):

Setting	Value
Status	Used
Usage	User
Vendor	Webex Calling

Synced in licenses

Licenses are synced and maintained in `device/spark/License`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Synced in locations

Locations are synced - see *Webex locations*.

Synced in Rooms, Teams, Groups

Rooms, Teams and Groups details are synced in as read-only data to `device/spark/Room`, `device/spark/Team`, and `device/spark/Group`, respectively.

Synced in Calling

Calling is synced in to `device/spark/UserConfig`, where the settings can be managed per user if the assigned license of which is "Webex Calling - Professional".

Synced in devices

Devices are associated either with a person or with a workspace. For users associated with a device, the person ID (converted to an email address) is used to sync the device to the correct hierarchy. See *Webex devices*.

6.2.2. Webex App licenses

Tip: *Use the Action search to navigate Automate*

Overview

Webex App license usage counts are automatically updated in Automate after licenses are assigned (that is, after assigning a subscriber with Webex App services). A sync with the Webex Control Hub maintains the status of Webex App user licenses.

Webex App license syncs

Webex App user license syncs may be executed manually:

Admin Portal	To sync Webex App users for the customer, click the **Services** menu, then on the Customer Access form, click **Action > Sync Webex App Roles Licenses** Go to (default menu) **Administration Tools > Data Sync** and run the `SyncSparkRolesLicenses<customer_name>` instance.

Important: Webex App Licenses need to be synced after upgrading to release 21.1:

1. Execute the following data sync: `SyncSparkRolesLicenses<CUSTOMER_NAME>`
2. If the Webex App organization associated with the Customer hierarchy has multiple subscriptions, a default subscription must be configured under the Webex App Customer Access.

   See *Webex Application Access (Webex Organization)* in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. If the Webex App organization associated with the Customer hierarchy has multiple Site URLs, a default Site URL must be configured under the Webex App Customer Access.

   See *Webex Application Access (Webex Organization)* in the Core Feature Guide.

Only licenses synced and managed by Automate will be assignable to a Webex user. This means that licenses from subscriptions and sites other than the default configured above will not be retained on a user.

Note: This process only collects data at customer and site levels.

Related topics

- See *Webex Application Access (Webex Organization)* in the Core Feature Guide.

View Webex App licenses

This procedure provides a condensed view of the Webex App licenses consumed and available at the selected hierarchy level.

1. Go to the **Licenses** page for Cisco Webex App.
2. View Webex App license details in the **License** list view:
   - Name (of the license)
   - Site URL (webex hub)
   - Site Type (for example: Control Hub managed site)
   - Subscription ID (ID - useful to distinguish licenses with similar names)
   - Total Units (total number of licenses available)
   - Consumed Units (the number of licenses still available)
   - Location (where the licenses are available and used)

6.2.3. Webex bulk actions

Tip: *Use the Action search to navigate Automate*

Overview

Automate's Webex bulk actions tool allows you to perform operations on schedules and phone devices.

Add (to replicate across selected Webex locations) is valid only for schedules. *Add* cannot be used for devices since each device requires a user or workspace. *Modify* and *delete* is supported for both schedules and devices.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Webex bulk actions on schedules

Automate's Webex bulk actions tool allows you to replicate operations from a source reference to selected target Webex locations for schedules.

This procedure performs operations (add, modify, or delete) on selected Webex locations.

Before you begin

- Create a reference schedule via `relation/WebexSchedules`. Ensure the reference schedule has a unique name and is easy to find.
- Clone the reference configuration template, `WebexBulkActionSchedules-Customizable`, to the required hierarchy, and modify the macro for the schedule name to ensure that a unique name is generated. For example:

  ```
  {{pwf.referenceScheduleData.name}}-{{pwf.locationName}}
  ```

  Supported target hierarchies for the clone operation are:

  - Customer
  - IntermediateNode
  - Site
  - LinkedSite

  This macro ensures a unique schedule name that is a combination of the source schedule name and the specific Webex location name.

Note: When the selected model is *schedule*, a reference schedule serves as the source to carry out the operation (add, modify, delete) on selected Webex locations.

To perform bulk actions on selected Webex locations:

1. In the Admin Portal, go to **Webex Bulk Actions**.
2. At **Model**, select **schedules**.
3. At **Operation**, choose an option, either of the following (for add, modify, or delete):

   Note: The operation you choose displays/hides additional fields on the page, and determines the next steps to complete.

   - **Add schedules**:
     - Select operation, **add (Replicate across chosen Webex Locations)**.
     - Select the reference schedule to apply to the selected Webex locations.
     - Select the configuration template.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: The configuration template allows an admin to make structural naming changes to schedules created at Webex locations.

- At the **Target Webex Locations** transfer boxes, select Webex locations to which the *add* action should apply.
- Save your changes.

  Schedules will be added to all selected locations, with schedule names defined with the applied configuration template.

- **Modify schedules**:
  - Select operation, **modify specific schedules**.
  - Select an updated reference schedule to apply to the selected Webex locations.

    Note: The reference schedule should have been updated to change the values in events or to add a new event.

  - At the **Target Webex Locations** transfer boxes, select Webex locations to which the action should apply.
  - Save your changes.

    Selected Webex locations are modified in accordance with the modified reference configuration template.

- **Delete schedules**:
  - Select operation, **delete**.
  - At the **Delete Schedules** transfer boxes, select Webex locations to which the action should apply.
  - Click **Save**.

    Selected Webex locations are deleted.

Webex bulk actions on devices

This procedure uses the Webex bulk actions tool to bulk update or deletes the parameters of one or more, pre-existing MPP, ATA, and WiFi devices in the device inventory, allowing bulk configuration of Webex devices.

Note: Only modify and delete is supported. *Add* is not supported since each devices requires a user or workspace.

Copyright © 2025 VisionOSS Limited. All rights reserved.

To perform bulk actions on Webex phone and WiFi devices:

1. In the Admin Portal, go to **Webex Bulk Actions**.
2. At **Model**, select **devices**.
3. Select the device type. Options are:
   - All devices
   - ATA
   - MPP
   - WiFi
3. At **Operation**, choose an option:
   - Delete:
     - At **Operation**, select **delete**.
     - At the **Target Webex Devices** transfer boxes, select from the available devices and move these to the **Selected** field.
     - Save your changes.

       The device and its configuration is deleted (purged), and the Automate refreshes the workspace or user that was associated to the device.
   - Modify specific devices:
     - At **Operation**, select **modify specific devices**.
     - At **Configuration Template**, select the relevant configuration template, which will allow you to make bulk configuration changes to the selected devices.
     - At the **Target Webex Devices** transfer boxes, select from the available devices and move these to the **Selected** field.
     - Save your changes.

   Configuration changes are copied to the target devices.

6.2.4. Bulk update Webex App users

Tip: *Use the Action search to navigate Automate*

This procedure performs bulk actions into Webex App Control Hub.

1. In the Admin Portal, go to **Bulk Update Webex App Users**.
2. Choose the relevant hierarchy (Customer or below), where your Webex App users reside.
3. On the **Bulk Update Webex App Users** page, to filter users at your current hierarchy, choose a user filter from the **User Filter** drop-down. For example, all users or only users with Hybrid Calling enabled.
4. Select the relevant **User Template**, which contains the settings to apply to the filtered users. For example, to provide messaging only, select the Webex App User Messaging Only Template.
5. If necessary, you can select more users (move users from the **Available** field to the **Selected** field. Else move all users.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Click **Save**.

6.2.5. Workspace call settings

Tip: *Use the Action search to navigate Automate*

Synced Webex workspaces are maintained in Automate in the `relation/WebexWorkspaceCallSettings` model, and display on the **Workspace Call Settings** list, with corresponding Webex location, if available.

Note: Workspace call settings can't be added or removed.

6.2.6. Workspace locations

A workspace location is a physical location with a name, address, country, city, latitude and longitude that can contain many workspaces. Examples of a typical location is a floor in the building or an entire building, depending on how the administrator would like to logically group the organization.

6.2.7. Webex schedules

Tip: *Use the Action search to navigate Automate*

Overview

A Webex schedule is associated with an existing Webex location.

Existing Webex schedules from the Webex Control Hub are synced to the Webex location when running the default data sync - see the model list here: *Introduction to Cisco Webex App*.

Note: To add a Webex schedule at a hierarchy, a Webex location must be available at the hierarchy. The following message displays at the **Webex Location Name** field when there is no Webex location available: *No Webex Location Found At This Hierarchy*

Refer to *Webex bulk actions* for details on the bulk add, delete or update of Webex schedules at more than one Webex location.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a schedule

1. From the **Webex Schedules** menu, navigate to the Webex location hierarchy, then click **Add**.

   The **Webex Location Name** (read-only) shows on the **Details** form.

2. Provide a **Name** and **Type** for the schedule.
3. According to the selected **Type**, add one or more calendar **Events**, along with the event calendar from the calendar picker and associated recurrence details.

   Note: You can set up a recurrence end date for Webex schedule events, or select **Recur Forever**. If you've selected a recurrence end date *and* you select **Recur Forever**, only the **Recur Forever** setting is configured for the Webex schedule. The end date, even if present, is thus disabled.

4. Click **Save** and inspect the entry in the **Webex Schedules** list view.

Modify a schedule

Only *Event* entries can be modified on existing schedules.

Note: The schedule **Name**, **Location Name** and **Type** can't be updated. If you need to change any of these values, delete the schedule, then add a new schedule with updated values.

- You can't configure the sequence of **Events** entries.
- You can set up a recurrence end date for Webex schedule events, or select **Recur Forever**. If you've selected a recurrence end date *and* you select **Recur Forever**, only the **Recur Forever** setting is configured for the Webex schedule. The end date, even if present, is thus disabled.

Delete a schedule

You can delete Webex schedules from the list view or from the detail view.

6.2.8. Device configuration profiles

Tip: *Use the Action search to navigate Automate*

Automate ships with the following default device configuration profiles for Webex App:

`ActivateWebexRoomOSDevice`	Used for activating a device.
`ResetWebexRoomOSDevice`	Used for resetting an already active device.

Note:

- You can access device configuration profiles via the **Device Configuration Profiles** page.
- The profiles can be cloned down and customized as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

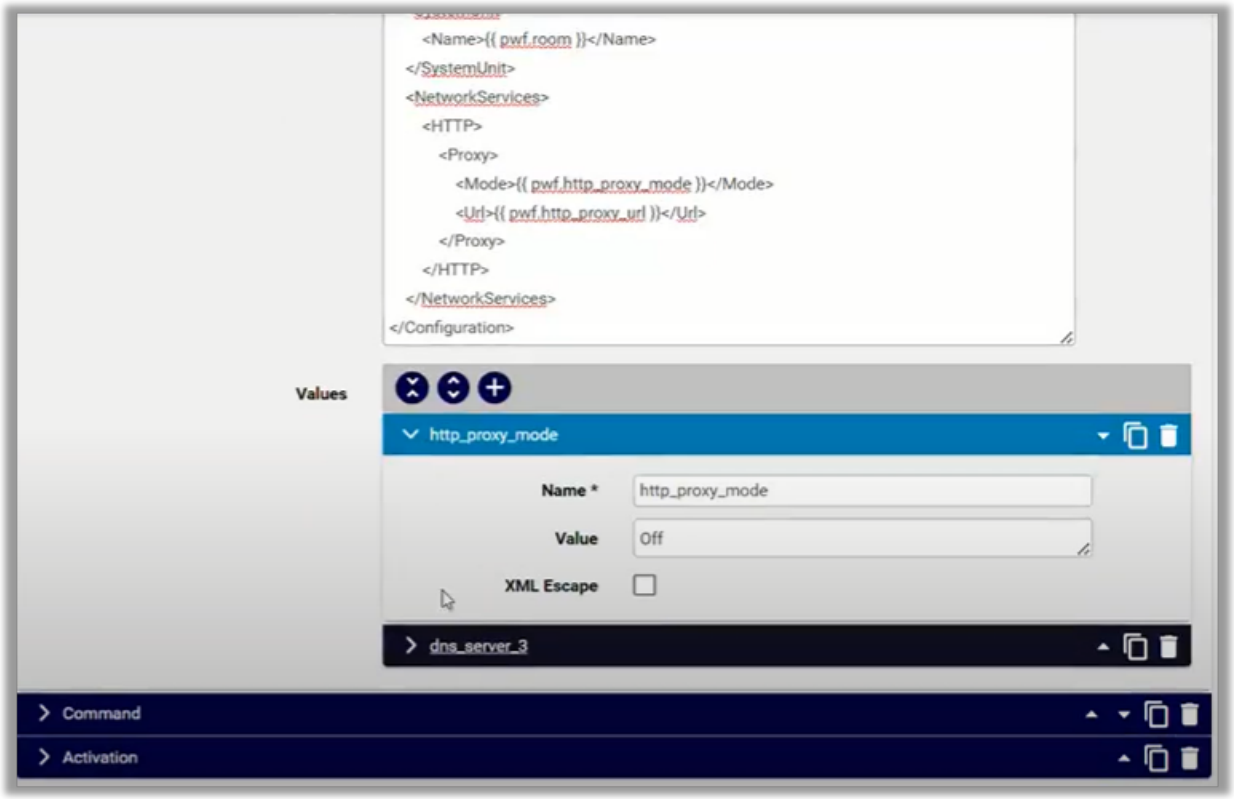
Configuration Blocks

The device configuration profiles contain configuration blocks, such as **Configuration**, **Command** and **Activation**.

Configuration Blocks	Description
Configuration	The step uses the configuration API for the device.
Command	This step uses the command API, and may be used for customization, for example, of buttons and widgets for the device user interface. The `<Upload>` section in the XML is used to upload two `.png` files to the device, which can be used for the icons or panels.
Activation	This step is only present in the `ActivateWebexRoomOSDevice` device configuration profile, and performs the last step in the device configuration, which involves activating the device in the Control Hub.

Note: You can log in to your RoomOS device and view the API developer documentation for a description of the XML in each step.

Values used inside the configuration blocks (e.g. `{{ pwf.http_proxy_mode }}`) can be managed as name-value pairs (e.g. `http_proxy_mode: Off`) in the **Values** fieldset of the profiles.



When specifying icons or images in the configuration file, the default file contains two samples:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `teams_button`
- `mm_button`

The `.png` files you're referencing in the configuration must be uploaded into VOSS Automate first via the **File Management** page. If the files are not uploaded, the configuration step will fail.

Custom device configuration profiles can be added and tested by selecting on the **Test Device Configuration Profile Rendering** page.

6.2.9. Webex App manual steps

Tip: *Use the Action search to navigate Automate*

When workspaces are created or updated in Automate on the **Workspaces** page, the data entered is formatted as a sequence of steps in an email message to be carried out on the Webex App Control Hub.

The content of these manual steps for a workspace configuration can be seen as the **Steps** content of the instance from the **Manual Steps** menu.

Related Topics

- *Webex Workspaces*
- *Global settings* for an email message example.
- *Introduction to Cisco Webex App*

6.2.10. Test device configuration profile rendering

Tip: *Use the Action search to navigate Automate*

This procedure tests the device configuration profile rendering.

1. In the Admin Portal, go to **Test Device Configuration Profile Rendering**.
2. Select an available **Profile** from the drop-down, and provide or override name-value pairs for the profile as **Mock Values** instances.

6.2.11. Webex App hunt groups

Tip: *Use the Action search to navigate Automate*

Webex hunt groups are synced from Webex Control Hub and can be added, removed, and updated from the Automate Admin Portal.

This includes the update of the internal number inventory.

- Relation (for menu item): `relation/WebexHuntGroup`

Configurable fields on the form in Automate align with available fields in Webex Control Hub.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Webex App hunt group:

1. Fill out a name for the Webex App hunt group.
2. Add one or more agents to the hunt group, and select the agent type, one or more of the following:

   Note: You can, for example, add three agents, and each agent can be a different agent type.

   - People (a user/person, and provide an email address as their ID)
   - Place (a workspace, and provide a workspace ID)
   - Virtual line (and provide the virtual line ID)
3. On the **Call Policies** tab/panel, select a policy.

Modify Webex App hunt group:

- You can update or delete agents.
- **Call Forward Settings** are available when editing Webex hunt groups. You can enable **Always** or **Selective** forwarding.

  Note: **Selective** forwarding allows for a set of **Rules** to be added according to selected and configured criteria.

6.2.12. Webex App call park

Tip: *Use the Action search to navigate Automate*

In the Automate Admin Portal you can add, update, and delete Webex Call Park service. The relevant relations (for the menu items):

- `relation/WebexCallParkGroup`
- `relation/WebexCallParkExtension`

Available fields on the input forms in Automate align with available fields in Webex Control Hub.

Add a Webex App call park group:

1. Fill out a name for the call park group.
2. Add one or more agents to the call park group, and select the agent type, one or more of the following:

   Note: You can, for example, add three agents, and each agent can be a different agent type.

   - People (a user/person, and provide an email address as their ID)
   - Place (a workspace, and provide a workspace ID)
   - Virtual line (and provide the virtual line ID)

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. On the **Recall To** tab/panel, from the **Option** drop-down, choose alert options. When choosing an option to alert a hunt group, also select the hunt group name.

Modify Webex App call park group:

- **Name** is read-only and can't be modified. Delete and re-add to update the name.
- You can update or delete agents.

6.2.13. Webex App auto attendants

Tip: *Use the Action search to navigate Automate*

Webex auto attendants are available and can be managed: added, removed, updated:

- Relation (for menu item): `relation/WebexAutoAttendants`

Available fields on the input forms in Automate align with available fields in Webex Control Hub.

Add:

- Mandatory fields are shown on the form with an asterisk (*).
- Only one of **Phone Number** and **Extension** is mandatory; for example, if **Phone Number** is selected, then **Extension** is no longer mandatory.
- On the **Business Hours Menu** and **After Hours Menu**, the selected **Greeting** allows for various additional details to be added.
  - **Business Hours Menu** is defined by a **Business Hours Schedule**.
  - At least one entry is required.
  - For **Key Configurations**, options are also determined by the selected **Action**. The **Announcement File** offers enterprise wide or local **Level** options.

Update:

- **Call Forward Settings** are available when editing Webex auto attendants. Options can be to enable **Always** or **Selective** forwarding.

  Selective forwarding allows for a set of **Rules** to be added according to selected and configured criteria.

6.2.14. Webex App call pickup

Tip: *Use the Action search to navigate Automate*

Webex pickup groups are synced from Webex Control Hub and can be added, removed, and updated from the Automate Admin Portal.

- Relation (for menu item): `relation/WebexCallPickup`

Available fields on the input forms in Automate align with available fields in Webex Control Hub.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Webex App call pickup group:

1. Fill out a name for the call pickup group.
2. Add one or more agents to the call pickup group, and select the agent type, one or more of the following:

   Note: You can, for example, add three agents, and each agent can be a different agent type.

   - People (a user/person, and provide an email address as their ID)
   - Place (a workspace, and provide a workspace ID)
   - Virtual line (and provide the virtual line ID)

Modify Webex App call pickup group:

- **Name** cannot be modified. Delete and re-add to update the name.
- You can update or delete agents.

6.2.15. Webex servers

Overview

Webex is a web conferencing facility used for collaboration with colleagues across your organization.

The support for Cisco Webex is as follows:

- Hosted Webex Cloud
- Ability to create user accounts and meetings using Webex versions:
  - 6.0 API and 27.00 server
  - 8.0 API and 29.13 server
- User and Meeting APIs are exposed and available for managing user capabilities. However, system setup, site addition, and meeting functions are done with the Webex application.

Parameters are defined when adding Webex instances of Network Devices on the Admin Portal.

Device Model Mapping

A data model is maintained in VOSS Automate where its instances map network device types to data models. For example, the network device `device/cucm` would have a mapping to `data/CallManager`. These target data models are used to maintain network device data in VOSS Automate, and any of their default connection parameters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Cisco Webex server

Tip: *Use the Action search to navigate Automate*

Important:

- The Webex Admin account on the Webex Control Hub used to connect Automate must have the administrator role: “Full Admin”.
- If the Webex admin account used to connect Automate to the Webex Control Hub is deleted, it is necessary to re-authenticate Automate using a different account. The token created by the admin user becomes invalid if the admin user is deleted.

This procedure adds and configures a Webex server.

Note: For more information about conferencing, see *Introduction to conferencing*.

1. Log in as Provider or Reseller administrator.
2. Go to the **Servers** page for Webex, then click the Plus icon (+) to add a new record.
3. Fill out at least the mandatory fields. See *Webex server settings*.
4. Save your changes.
5. Test the connection to the Webex server:
   - Go to **Webex Network Device**.
   - Click in the row for the relevant Webex server; then, choose **Action > Test Connection**.

Webex server settings

The table describes settings to be configured when adding a Webex server:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Type	Mandatory. The type of Webex server. Read-only. Set to Cloud-Based.
Protocol	Mandatory. Protocol used for communication with the Webex server, either https or http. Default https.
Address	Mandatory. The IP address or hostname of the Webex server, for example, Site-name.webex.com
Port	The port used to communicate with the Webex Server. Defaults to 443.
Site Name	Mandatory if Site ID is not specified. The name of the site to be managed. Usually matches the start of the Webex address.
Site Id	Mandatory if Site Name is not specified. The ID of the site being managed. Typically received from Cisco Webex Site Provisioning group. Provide this field value before testing the connection to the Webex server.
REST URI	Mandatory. Defaults to WBXService/XMLService. The relative URI for the XML service on the Webex server.
WebEx Id	Either the Webex ID or the Email field is mandatory. The Webex administrator ID, used to connect to the server for admin tasks, such as adding or deleting users.
Email	Either the Webex ID or the Email field is mandatory. Required if no Webex ID is provided. A valid email address for the administrator.
Password	Mandatory. The password for the administrator with the supplied Webex ID.
Version	Supported Webex server versions. Supported server versions can be either 27.00 or 29.13.

6.2.16. Webex Overview

Webex General Organization Functions

Webex Application Access (Webex Organization)

Tip: *Use the Action search to navigate Automate*

This procedure adds the Cisco Webex service (Webex Control Hub instance).

Prerequisites:

- To allow Automate to connect to the Cisco Webex Control Hub, obtain the Webex Control Hub Account Organization ID from the Cisco Webex page.

  Important: For users upgrading to release 21.4-PB2, existing access tokens must be refreshed in order to update permissions for newly added `workspace_locations`.

Note: You won't need to create Network Device Lists (NDL). When importing from Webex Control Hub the first time, the Automate workflow creates a blank NDL at the customer if no other NDL exists. When the sites

Copyright © 2025 VisionOSS Limited. All rights reserved.

are auto created based on the imported Webex Locations, the sites will use this new blank NDL.

Create the Cisco Webex service:

1. Log in to the Automate Admin portal as a provider or reseller administrator.
2. Select the relevant customer hierarchy.
3. Go to **Webex Application Access** or **Webex Organization** to open the list view of all configured Webex organizations.

   Note: Existing accounts added before Automate 21.4-PB3 will show the *internal* account ID as the **Organization Account Number**, while accounts added from Automate 21.4-PB3 onwards, show the *external* account ID.

4. Click the Plus icon (+), then, on the new record page:
   - Fill out the Webex App customer name (the default is the Automate customer name).
   - If the added service is *Webex for Wholesale*, enable **Wholesale Customer**.

     Note: The *Webex for Wholesale* service can only be configured when adding an instance under **Webex Application Access** / **Webex Organization**.

   - If the added customer service is for a Webex Contact Center, enable **Contact Center Customer**. This also enables the **Contact Center Region** dropdown list (mandatory) to select a customer's region in order to allow for access to the available API endpoint at the region. Options are:
     - US
     - ANZ
     - UK
     - EU (Frankfurt)
     - Japan
     - Canada
     - Singapore
   - Fill out your Webex Control Hub Account Organization ID (external account ID).

     Note: Obtain this value from the Webex Control Hub admin portal (under the Account menu).

   - Fill out the admin account email for the administrator managing the account.

     Note: This field value is informational only.

   - At **HTTP Proxy** and **HTTPS Proxy**, values are mandatory *only* if a proxy server is required to connect to the Cisco Webex Control Hub API. Example format: `http(s)://[user:password]@host:port/`. Special characters in either the user or password must be URL encoded. Verify the required format with the proxy administrator.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: You'll need to add the Webex organization account details to Automate before access tokens can be obtained.

5. Click **Save**.

Note: When adding a new Webex Control Hub Access entry for a customer, data syncs and schedules are automatically created. Deleting a customer's Webex Control Hub Access automatically deletes these data syncs and schedules.

6. Once the new Webex organization is saved, return to the created account to view (in the **Access Tokens** section), the **Connect to Webex Control Hub** link that is used to request the tokens.
7. Click the **Connect to Webex Control Hub** link to obtain the access tokens (Webex Wholesale tokens for Customers and Users if **Wholesale Customer** is enabled) for the Webex Control Hub account, and to be redirected to the Automate **Transactions** page.

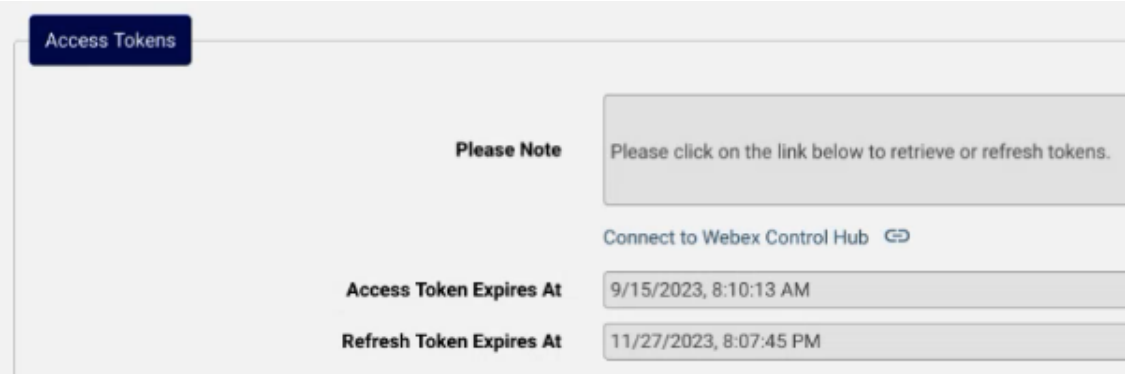
Note: When first using this link, a Webex admin user (with sufficient privileges) must log in and accept the API authorization scope that Automate requires for integration.

8. On the **Transactions** page, monitor progress for retrieving the access tokens.

Note:

- Roles and licenses are synced in to Automate.
- When the transaction completes, view expiry times for the access token and refresh token.
  - Automate automatically refreshes the access tokens every 7 days for 90 days, that is, until the expiry of the Refresh Token.
  - The Refresh Token is valid for 90 days. Use the **Connect to Webex Control Hub** link to refresh it. Automate **General Settings** provide options for Webex App Tab to send impending expiry notifications and messages. See: *Global settings*.

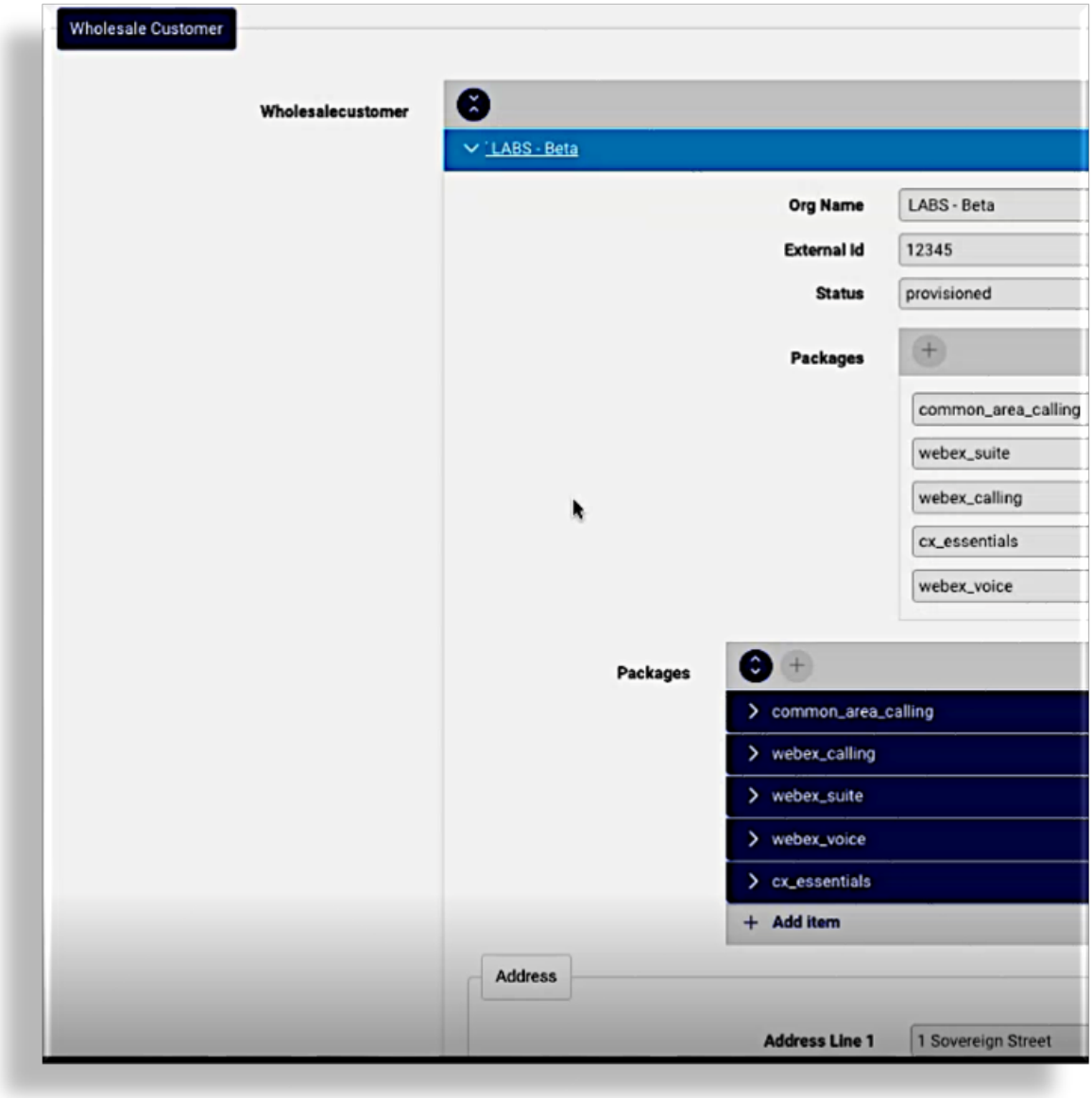
    For more information around access token management, see https://developer.webex.com/docs/integrations



9. If **Wholesale Customer** was enabled, the **Wholesale Customer** section of the **Webex Control Hub Access** form shows **Wholesalecustomer** instance(s) associated with the Webex organization account.

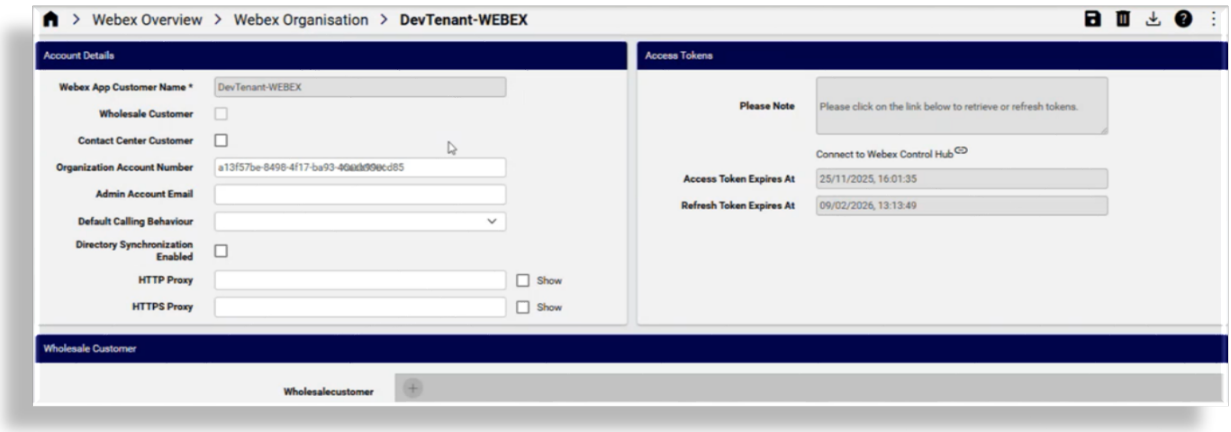
Copyright © 2025 VisionOSS Limited. All rights reserved.

Customer details and associated calling and collaboration packages can then be managed if needed:



The list view item for the Webex for Wholesale control hub will show **Wholesale Status** as true.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- *Introduction to Cisco Webex App*
- *Quick Add Groups, default model*
- *Webex App licenses*
- "Webex onboarding best practices" chapter of the Best Practices Guide.
- Network Device Lists (NDLs) topic in the Core Feature Guide.

6.2.17. Webex Detailed Configuration

Webex Calling Connection & Licenses

Webex location node mapping

Tip: *Use the Action search to navigate Automate*

The **Webex Location Node Mapping** page (`data/WebexLocationNodeMapping`) allows for the mapping of an existing Automate intermediate hierarchy node to a Webex location name. This functionality allows administrators to sort the Webex locations into business driven logical groupings. Note that the mapping of the Webex location name must be in place before the locations are synced from Control Hub. If the location match string is not found, a new location will be built directly under the customer node. If a mapping is missing, an administrator may purge that location data, create the mapping in Webex Location Node Mapping and run the data sync again.

Upon data sync, Webex locations that match the **Search String** are then moved under the Intermediate node.

Important: The text entered into the **Search String** field:

- can be case-insensitive
- should be contained in the Webex location name as uniquely as possible, to exclude unwanted location name matches

Copyright © 2025 VisionOSS Limited. All rights reserved.

- matching operator is `containsIgnoreCase`

1. Select the required **Intermediate Node** that the Webex location should be mapped to.
2. In the **Search String**, enter (case-insensitive) a distinctly matching string from the Webex location name should be mapped to the intermediate node.
3. Click **Save**.

On the next Webex data sync, Webex locations matching the **Search String** are moved under the selected **Intermediate Node**.

Related Topics

- *Introduction to Cisco Webex App*

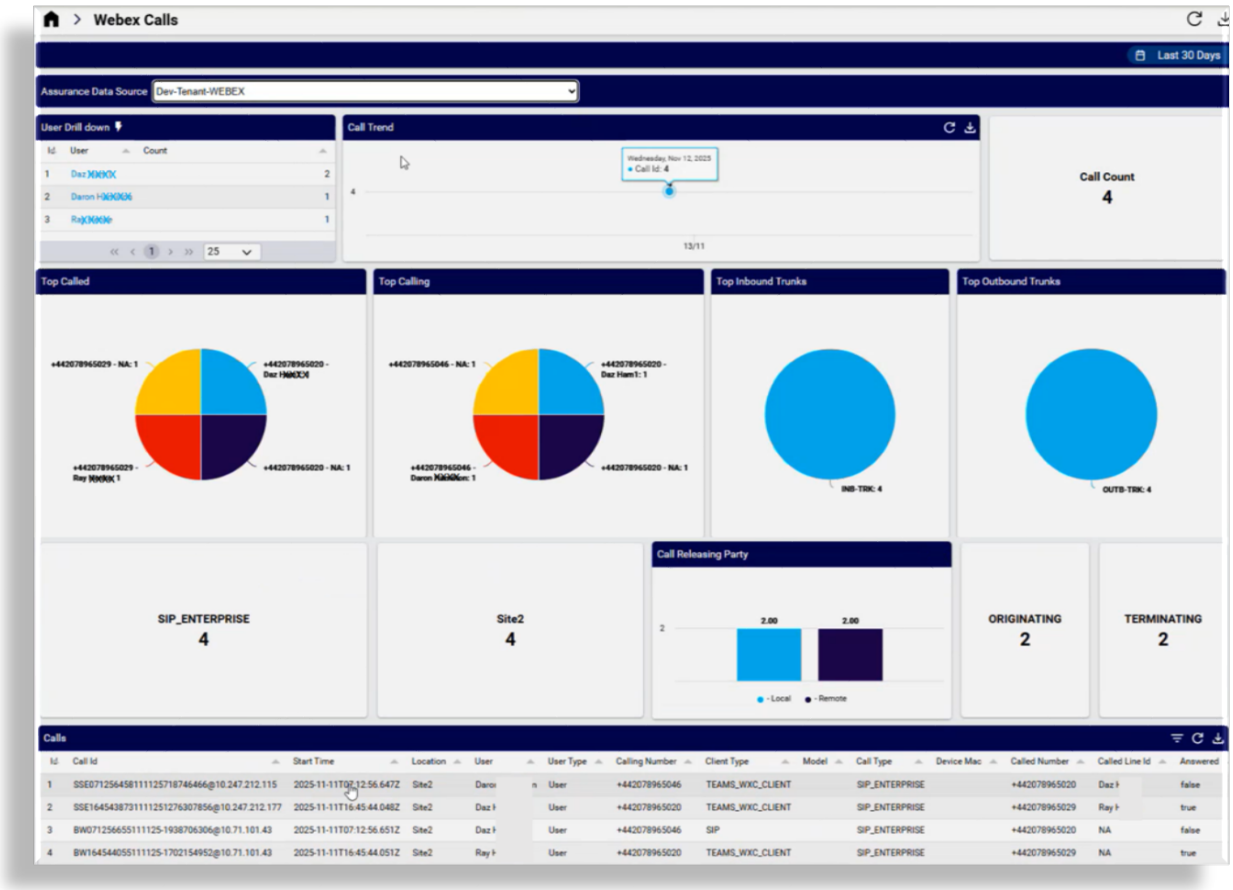
Webex Calls

The Webex Calls dashboard provides a reporting overview of calling statistics for users at a tenant, including CDR references, top inbound and outbound trunks (reflecting the number of calls that have gone through each trunk).

You can also drill down on each user to view their call statistics, including called or calling parties, their total number of calls and call trends for the query period (for example, last 30 days).

Click the information icon at each widget for details on data contained in the widget.

Copyright © 2025 VisionOSS Limited. All rights reserved.



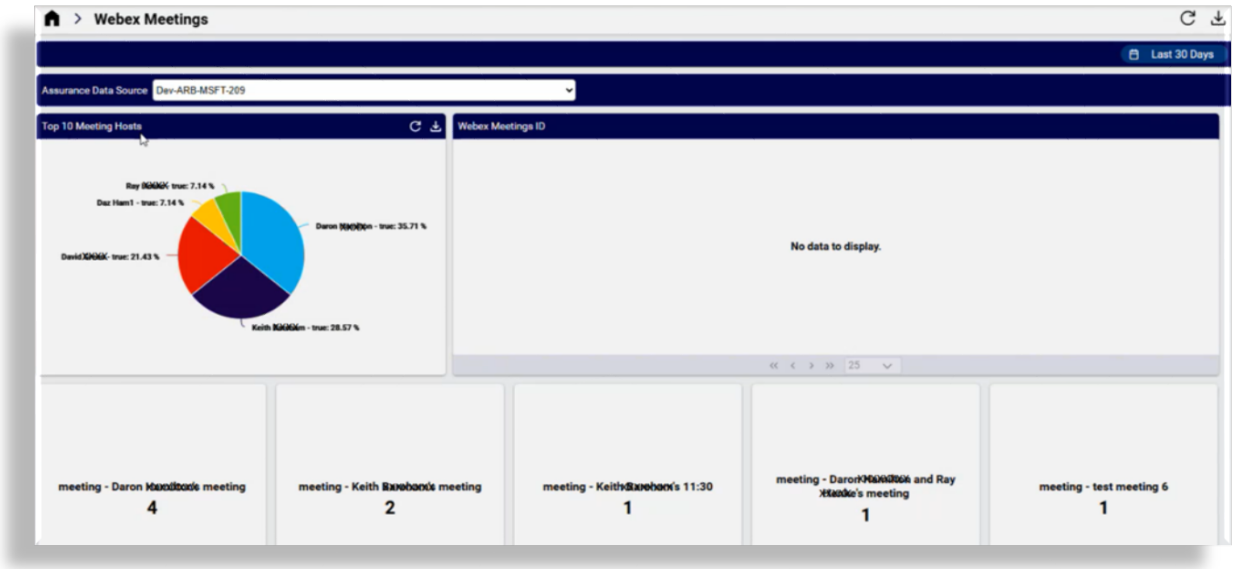
Webex Meetings

The Webex Meetings dashboard provides reporting quality metrics for Webex meetings at a tenant, including:

- Top ten meeting hosts
- Meeting IDs
- Data for devices used in the meetings (username, camera name, microphone name, speaker name, hardware type)
- Meeting quality data (such as audio quality per call participant, video quality, MOS evaluation, and whether a password was used)

Click the information icon at each widget for details on data contained in the widget.

Copyright © 2025 VisionOSS Limited. All rights reserved.

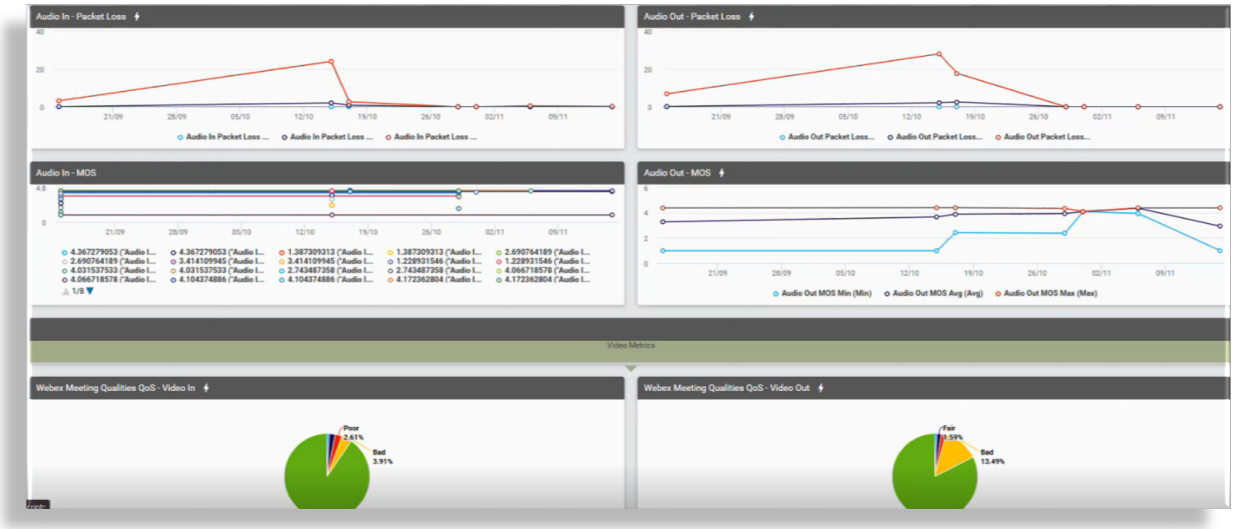


Webex Meeting Qualities

The Webex Meeting Qualities dashboard provides detailed quality of service (QoS) reporting metrics and trend graphs for each metric for each meeting participant (per meeting experience) for a Webex tenant. QoS metrics include:

- QoS audio in/out MOS
- Webex audio in/out jitter
- Audio in/out latency
- Audio in/out packet loss
- Video QoS in/out
- Screen share QoS in/out

Click the information icon at each widget for details on data contained in the widget.



Copyright © 2025 VisionOSS Limited. All rights reserved.

6.2.18. Webex Calling Locations and Settings

Webex locations

Tip: *Use the Action search to navigate Automate*

Overview

Webex locations allow you to organize users and workspaces based on a physical location. You can configure both calling and workspace management functions into the same location.

Note: With *Workspace locations*, the latitude and longitude of the location is also recorded.

Webex locations are synced in from a Webex Control Hub and maintained in `device/spark/Location`.

Site names for a sync is determined by the Site Defaults setting **Webex Location ID**. See the **Webex** tab under *Site defaults*.

Upon data sync at customer level, sites are automatically created or updated in VOSS Automate if no site exists with a matching name, in accordance with a Webex Control Hub Location.

Important: To ensure that Webex data sync can be executed successfully, the **Webex Location ID** in the respective Site Defaults needs to exist.

Synced Cisco Webex users and numbers of synced Cisco Webex users are automatically moved to the site matching the Location. For data sync at intermediate hierarchy level, see: *Webex location node mapping*. name of the Intermediate node according to the matching rules set up in the `data/WebexLocationNodeMapping` model, a site is created under this intermediate node.

Otherwise, the site will be created under the customer hierarchy.

This model needs to be exposed in the administrator's menu in order to manage the mappings. The model allows for matching to be configured between **Intermediate Node** and **Search String** values. The entered **Search String** should be as specific as possible to match the **Intermediate Node** string.

The list view of the **Webex Locations** menu shows the Webex location name and the corresponding Automate hierarchy name in the **Located At** column

Webex locations can also be added and managed from the **Webex Locations** menu in Automate, to be synced to the Webex Control Hub

For example, the **Latitude**, **Longitude** and **Notes** fields can be added or updated. Upon adding, these show as **Webex Location ID** on the site's site defaults, and upon sync of **Webex Locations**, these will then also reflect in **Workspace Locations**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

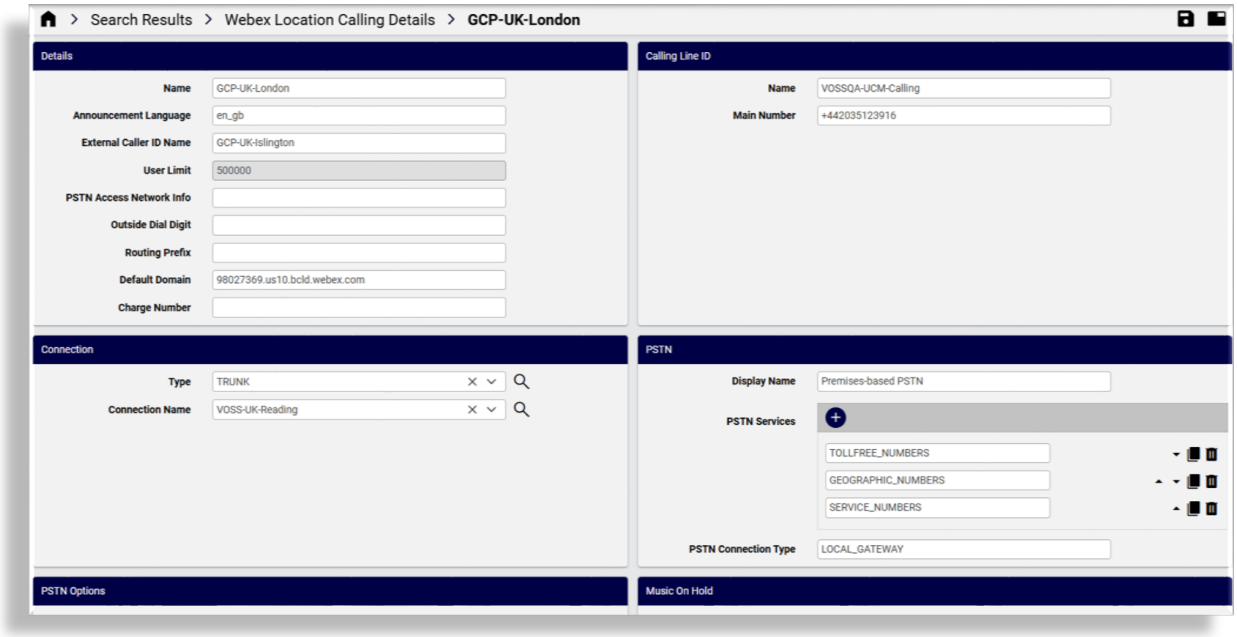
Webex location calling details

Synced Webex location calling details are maintained in Automate in the `device/spark/LocationCallingDetails` and `relation/WebexCallingLocationDetails` models, thereby providing access to a single interface to the manage a location's calling settings via the **Webex Location Calling Details** page.

Note:

- If the `outsideDialDigit` value needs to be *reset* to `None`, this reset must be carried out on the Webex Control Hub and the data sync for location calling details executed to refresh the value.
- For any new update of the **PSTN Access Network Info** in **Webex Location Calling Settings**, this will only be applied if the location's country is: Belgium, Germany, or France. Changes to other countries or to existing connection details are ignored. This functionality is in accordance with a Webex API change starting April 11, 2024.
- On the Webex **Location Calling Details** page (`relation/WebexCallingLocationDetails`), you can set the PSTN connection type (trunk or route group) and an ID for either trunk or route group, for a Webex location.

  Automate includes device models (`device/spark/Trunks`, `device/spark/RouteGroup`, `device/spark/DialPlans`) that allow for the management and selection of the route groups as connection type, thereby supporting call handling over trunks to Webex supported devices.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

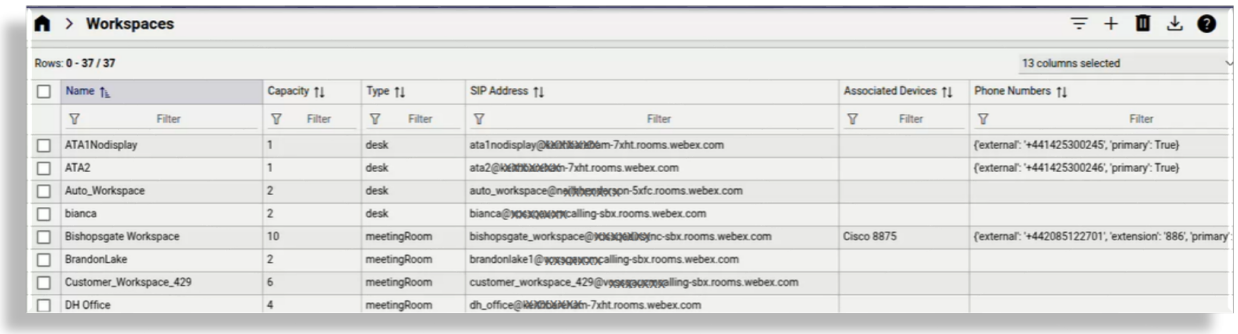
- *Introduction to Cisco Webex App*

Webex Workspaces

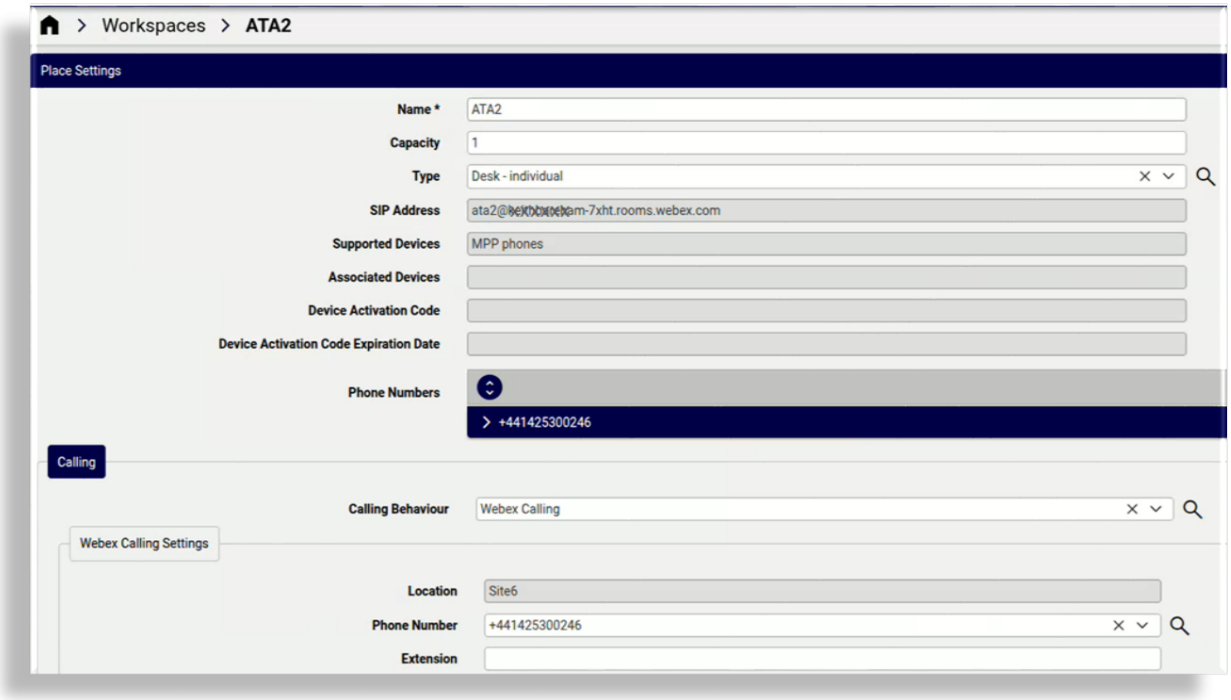
Tip: *Use the Action search to navigate Automate*

Overview

Webex App workspaces can be added in Webex Control Hub and from Automate. Workspaces can be updated in Automate and the changes are synced back to the Webex Control Hub.



Details synced in includes calling behavior and calendar settings, as well as phone numbers and device information associated with the workspace.



Copyright © 2025 VisionOSS Limited. All rights reserved.

When a sync occurs, existing numbers in the number inventory are updated with workspace details, for example, in the corresponding Usage, Description, and Vendor fields.

You can add various types of Webex App workspaces in Automate, for example, meeting rooms or open spaces.

Related topics

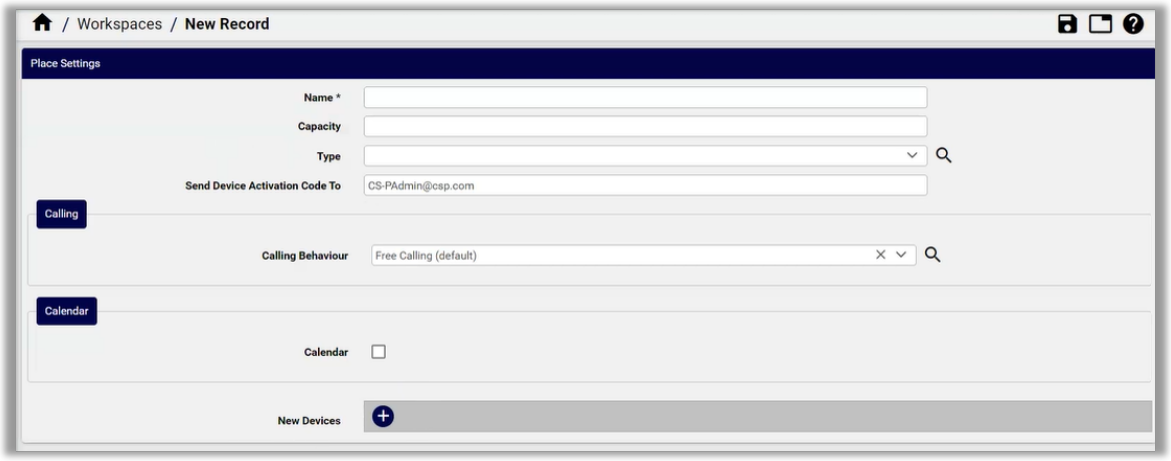
- *Introduction to Cisco Webex App*

Add a Webex workspace

This procedure adds a Webex workspace, and optionally, adds phone or conference devices.

Note: You can add devices when adding a new workspace or when updating an existing workspace.

1. Log in to the Admin Portal as provider admin, then go to the **Webex Workspaces** list view.
2. Click the Plus icon (+) to add a new workspace, then choose the relevant site.

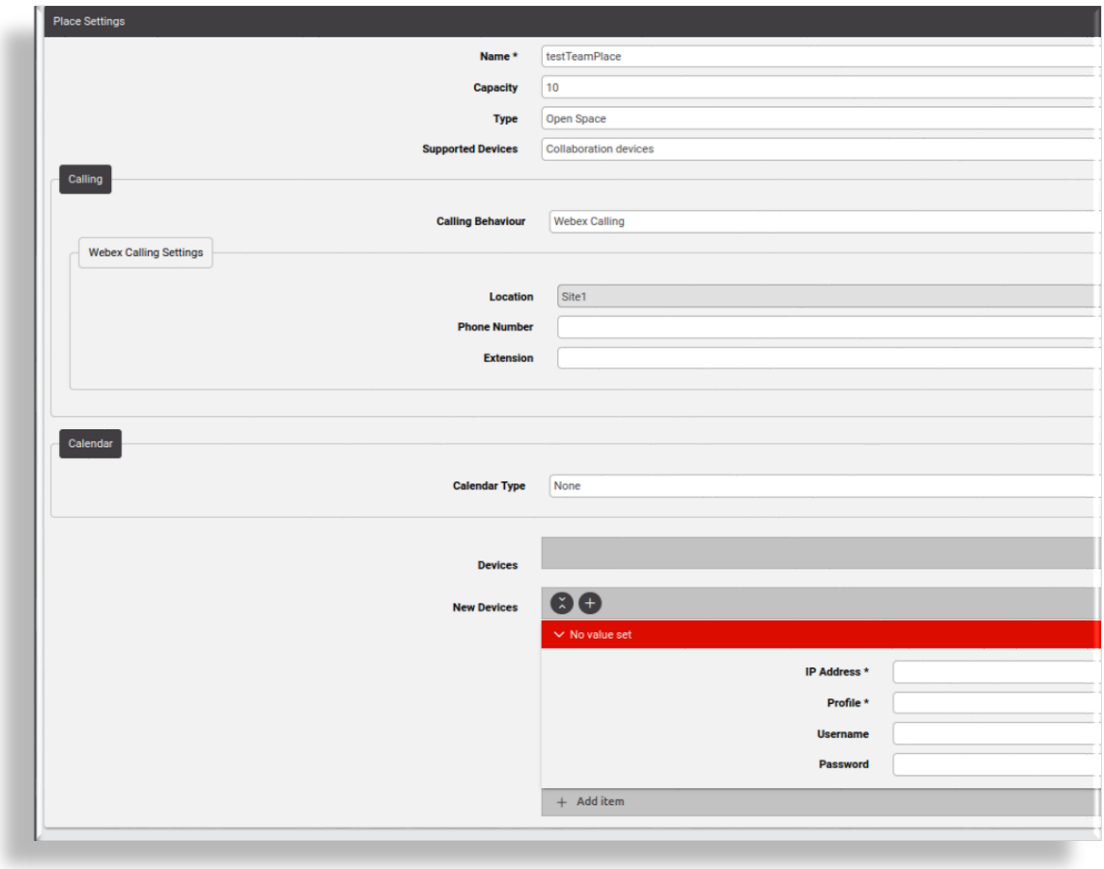


3. Fill out details for the new workspace:
   - Add a workspace name.

     Once a workspace is added, you can update its name if required.
   - Define capacity (how many persons the workspace is suitable for).
   - Select the workspace type for example, desk, focus, huddle, meeting room, or open space.
   - At **Supported Devices** choose the device type, either *Collaboration devices* or *MPP phones*.

     Note: If the supported device selected is *Collaboration*, you'll be able to add one or more devices.

Copyright © 2025 VisionOSS Limited. All rights reserved.



4. At **Send Device Activation Code To**, fill out the email address(es) where the device type code is sent.

   Note: The device activation code is unique to the workspace and is entered into the device itself.

   Once the code is created, the **Device Activation Code** (read only) value is returned and shown, as well as its **Device Activation Code Expiration Date**. An Automate system schedule checks the expiration date and generates a new code.

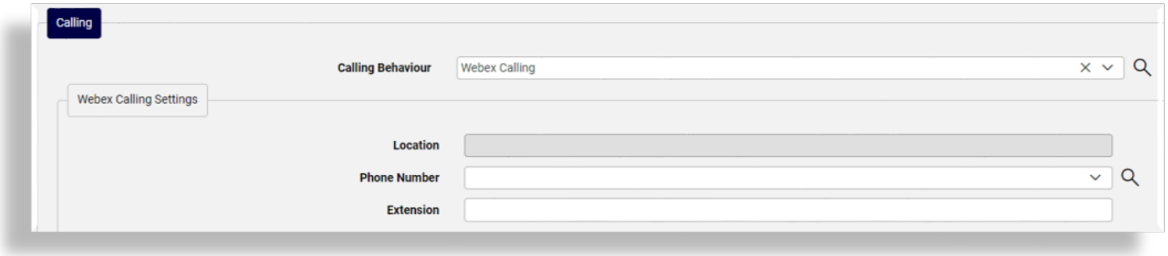
   When a workspace activation code expires, a scheduled workflow refreshes codes for places without expiry dates or with expired/expiring codes, and continues processing remaining places if individual places fail.

   The **SIP Address** of the workspace is also shown.

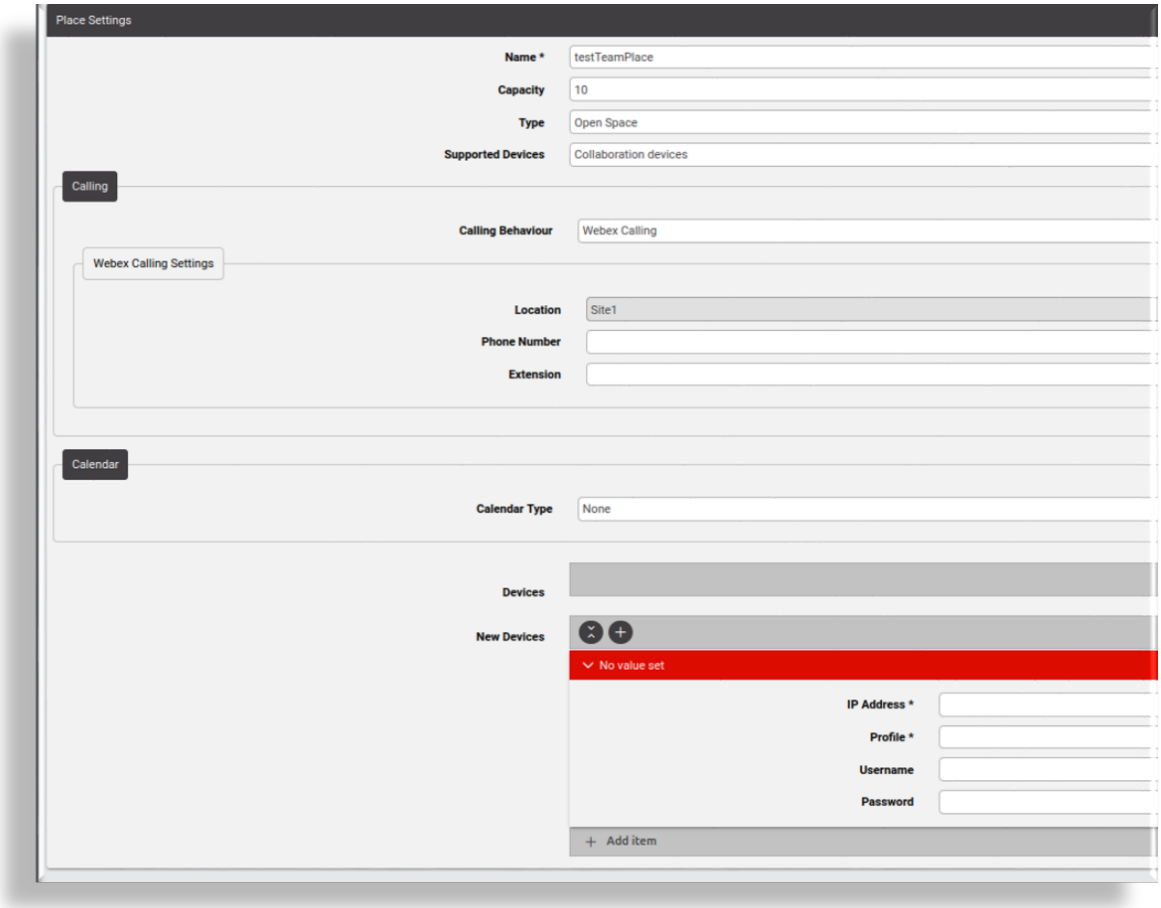
5. At **Calling Behavior**, select the workspace calling behavior:
   - No calling
   - Free calling (default)
   - Webex Calling
   - Third-party SIP URI
   - Webex Edge For Devices
6. If you've chosen *Webex Calling* as the calling behavior, at **Webex Calling Settings**, fill out a phone number and extension.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Webex Calling settings display on the page *only* when Webex Calling is selected.



7. At **Calendar Type**, optionally, select a calendar provider (these options are those available from the Scheduling section on the Webex Control Hub - for example, Microsoft Exchange / Office 365, or Google Calendar). If you choose a calendar type, you will need to fill out a workspace email address.
8. If the supported device type is *Collaboration*, at **New Devices**, add one or more new devices to the workspace. This allows for activating devices in a workspace using the RoomOS driver:



Note: Existing devices in the workspace are shown in the **Devices** group, while all devices display via the **Devices** menu.

For each new collaboration device:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Add the current **IP Address** for the Webex device.

  Note: The configured IP address must be reachable by all of the Automate unified nodes via HTTPS using port 443.

- Select the profile to use for configuring the device.

  Note: The profile includes the required parameters for the configuration. Profiles are managed on the Webex App **RoomOS Device Configuration Profiles** page.

- Add the device username and password, if needed.

  Note: You can add a device with the default username, `admin`, and no password. However, it is recommended that you add a second user on the device since, when the device registers with the Webex Control Hub, by default, Webex Control Hub disables the default username (`admin`) as part of the registration process, which prevents you from logging back in to the device using its IP address, unless you've added a second user. For example, without the second user, reset via the Admin Portal will not work because you will need to provide a username and password. If the default username is disabled, go to the Webex Control Hub, locate your device, and access the device via the UI.

9. Save your changes. Wait for the transaction to complete.

   The new workspace and devices are registered with Webex Control Hub, which assigns an activation code. The activation code is used to make a second connection to the device local IP address to run the activation step with the configuration you specified in the configuration blocks.

   In the Admin Portal, you can view the new workspace in the the **Webex Workspaces** list view. To view new devices, use the **Action** search to locate the **Webex Devices** page.

Webex Calling Devices

Webex devices

Tip: *Use the Action search to navigate Automate*

Overview

You can add, update, and delete Webex devices in Automate, including collaboration devices, ATA (analog telephone adaptor) devices, MPP (IP desk phone) devices, and Wi-Fi devices.

You can also add Webex devices in the Webex Control Hub and sync in those devices to the correct hierarchy in Automate.

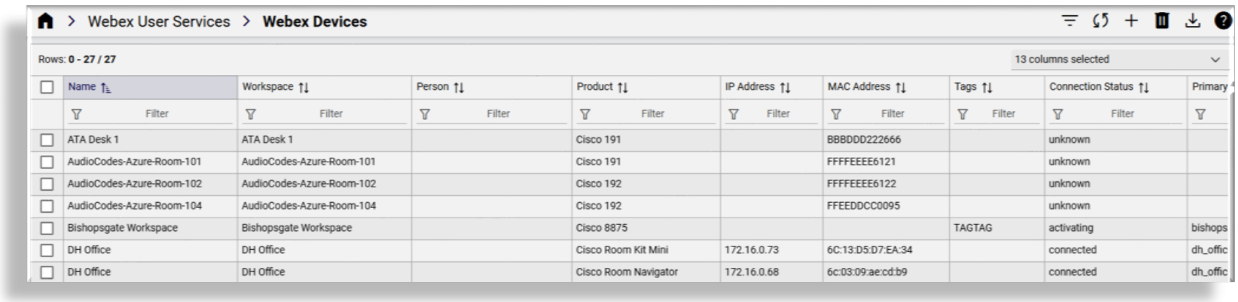
Note: MPP, ATA, and Wi-FI device types supported in the Control Hub are dynamically retrieved, along with their respective configuration settings, from the Control Hub via the Control Hub's supported device

Copyright © 2025 VisionOSS Limited. All rights reserved.

API using Automate's `device/spark/SupportedDevices` model. This model populates the drop-downs in Automate where you can select a Control Hub supported device.

Webex devices are added by their MAC address to either a user or to a new or existing workspace. In Automate, devices can be added and updated via the **Webex Devices** management page (described in this topic) or via **Quick Add Webex Device**.

Note: Several configuration options are available for each device type. You can manually configure all these options via the the **Webex Devices** page or auto apply configuration via **Quick Add Webex Device**.



Related topics

- *Webex App sync*
- *Introduction to Cisco Webex App*
- *Quick Add Webex Device*
- *Replace device*

Cisco Webex App device settings

Cisco Webex App devices are managed via the **Webex Devices** page, on the following tabs:

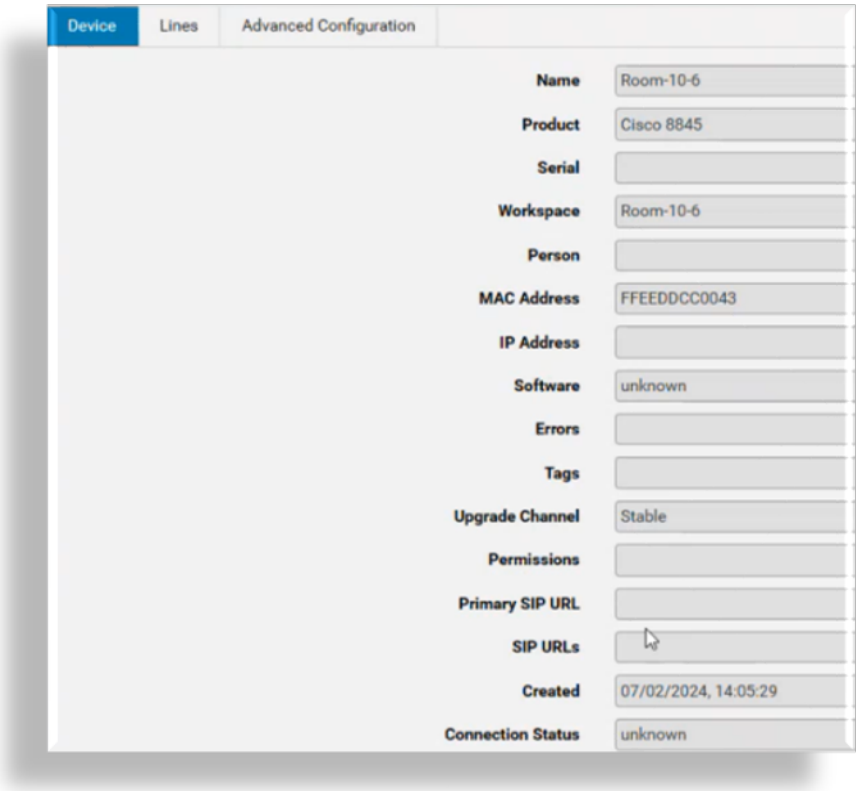
- Device
- Lines
- Advanced Configuration

Note: You can toggle the toolbar **Tab**/**Panel** icon to display the page layout as either tabs or panels.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Device tab/panel

The **Device** tab/panel displays read-only device details, such as the MAC address (device name) for a particular device.



When adding a device, you'll choose the product (device type), and define whether to associate the device with a workspace or a person. When choosing a device, configuration settings relevant to the device type become available in **Advanced Configuration**.

Note: A device can be associated either with a workspace or with a person (Webex user), but not with both.

A device associated with a person is defined as a personal device. The **Person** column in the Webex Devices summary list view displays the person ID (converted to an email address) when a person (rather than a workspace) is associated with a device.

The email address is used to identify the device and the associated user so that both can be moved to the

Copyright © 2025 VisionOSS Limited. All rights reserved.

correct hierarchy in a sync.

Lines tab/panel

On the **Lines** tab/panel, you add lines to a Webex device.

When adding a second line to an existing Webex-supported device (for example, Cisco ATA192), the line type and line weight have the following default values applied:

- **Line Type**: PRIMARY
- **Line Weight**: 1

Note: Default values are only auto-populated on new lines where field values are not explicitly set. This prevents provisioning transactions from failing due to no or incorrect configurations. You can change these values. Existing values on existing lines are not modified.

Advanced Configuration tab/panel

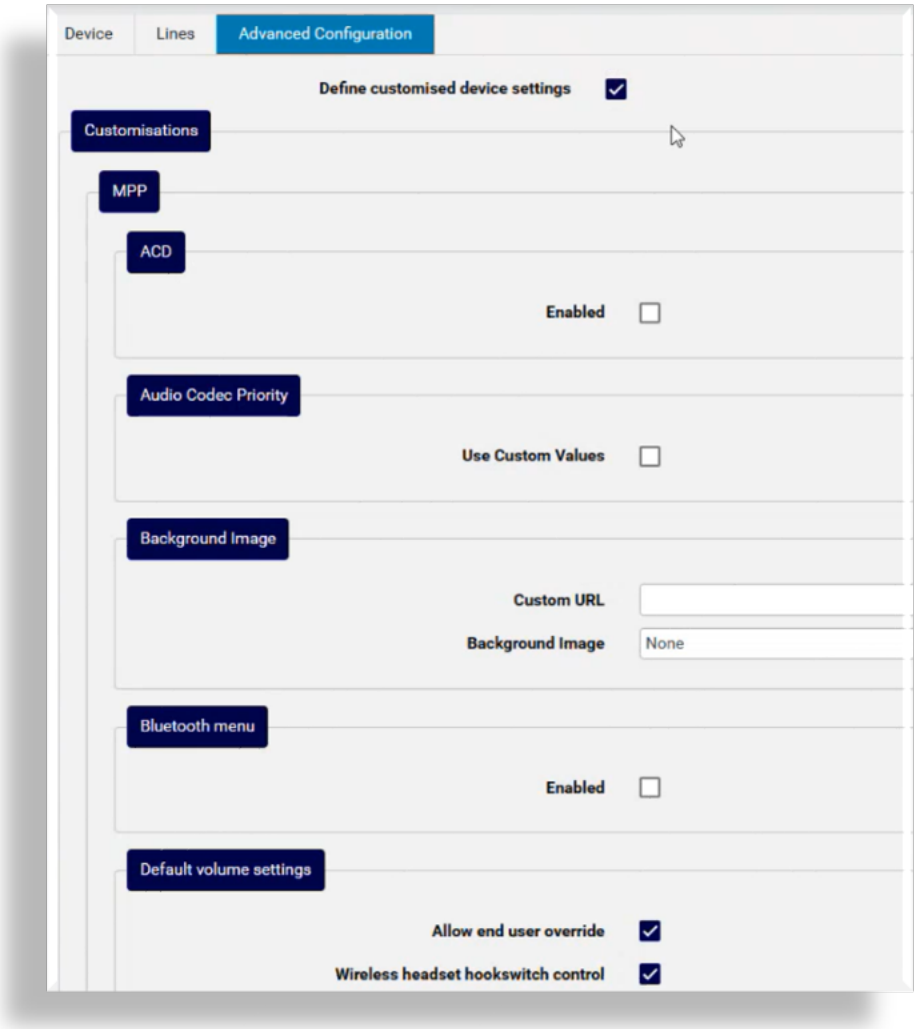
The **Advanced Configuration** tab/panel defines the calling parameters for a device. The available configuration settings depend on the device type, for example, MPP, ATA, or Wi-Fi device.

If you wish to apply custom configuration settings to the device, select **Define customized device settings** to display the additional custom configuration options for the device.

Note: Device-specific custom configuration settings are the same settings that may be defined on the Control Hub for the device type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

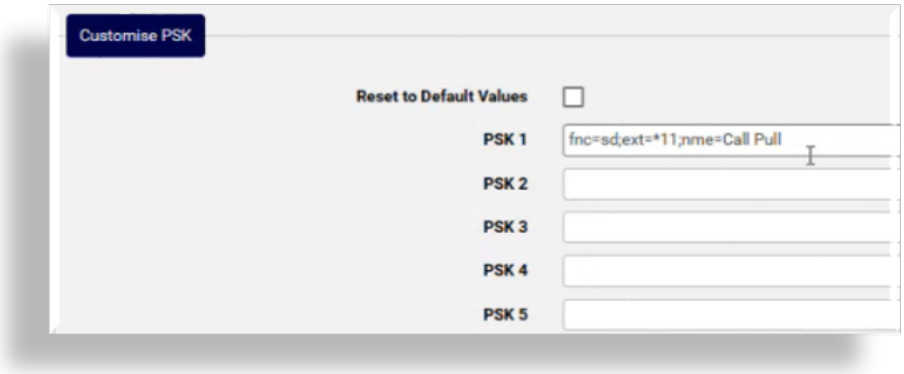
The image displays custom configuration settings for a MPP device:



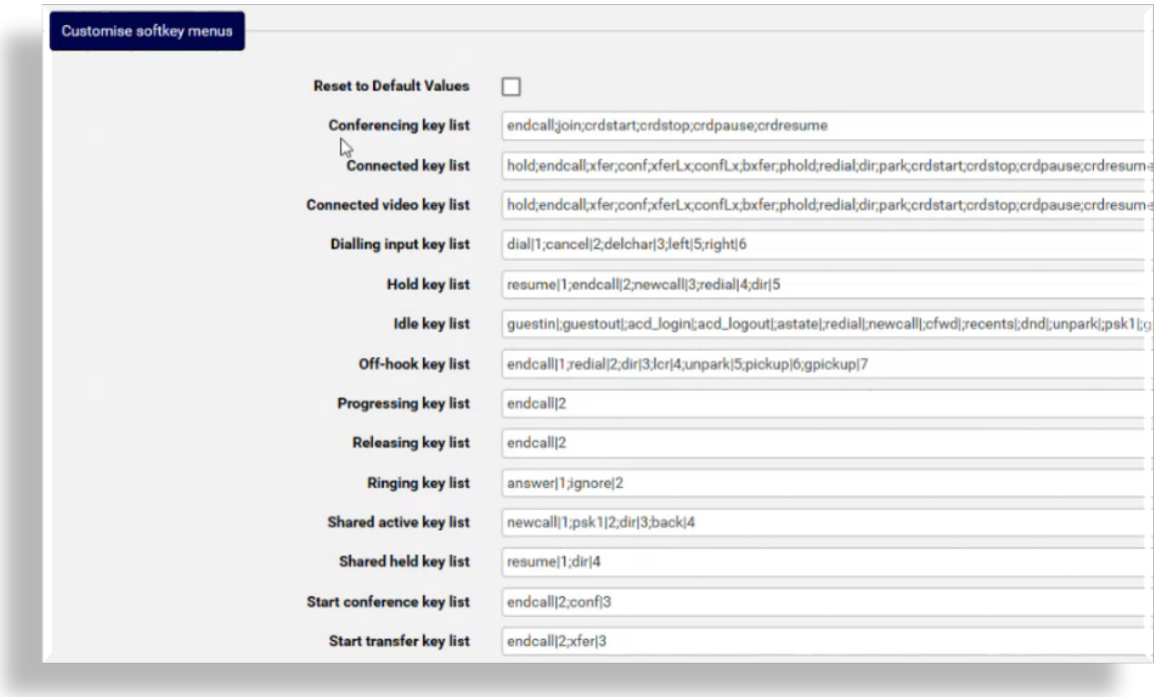
Note:

- For a MPP device, default PSK (programmable soft key) settings are automatically populated from the Control Hub. All the PSK fields on the form are editable string fields and can be added to or changed, or reset to default values, if required.

Copyright © 2025 VisionOSS Limited. All rights reserved.



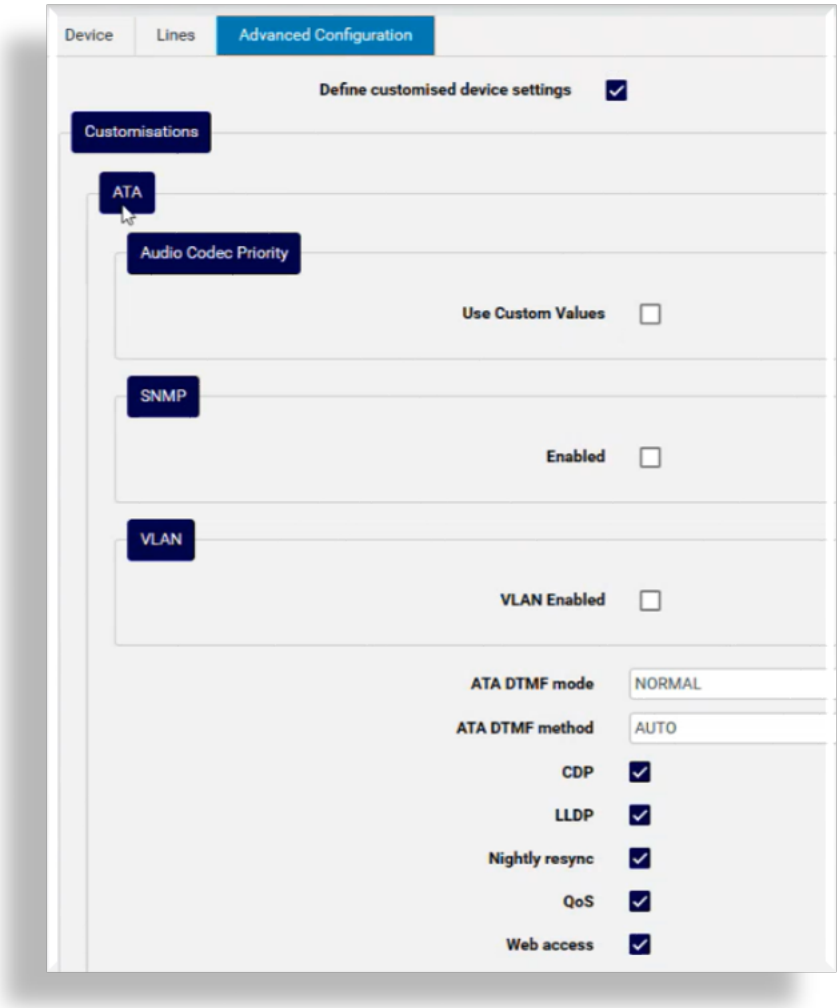
- For a MPP device, settings in the **Customize softkey menus** fields comprise default values retrieved from the Control Hub, and are semi-colon separated lists of items that will display for the softkeys. These settings are editable strings that can be customized, or reset to default values, if required.



To reset values for the custom softkey menus or the PSKs, select the applicable **Reset to Default Values** checkbox. When saving your settings, the default values are retrieved from the Control Hub to replace any custom values.

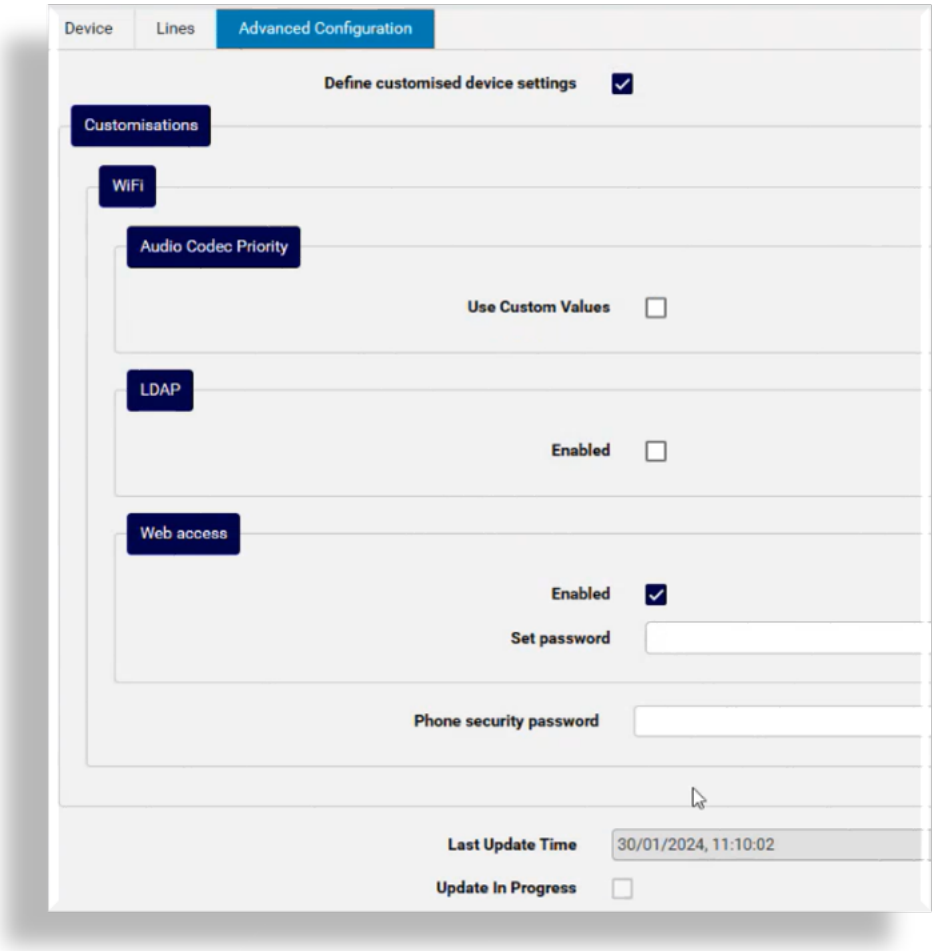
Copyright © 2025 VisionOSS Limited. All rights reserved.

The image displays custom configuration options for an ATA device:



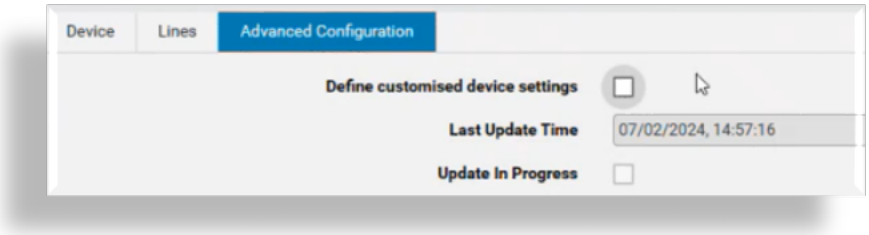
Copyright © 2025 VisionOSS Limited. All rights reserved.

The image displays custom configuration options for a Wi-Fi device:



Hide custom configuration settings

To hide the custom settings and apply default settings from the Control Hub for the customer and site, deselect **Define customized device settings**.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Configuration templates

Tip: *Use the Action search to navigate Automate*

Introduction to configuration templates

Configuration templates (CFTs) are used to define values for the attributes of any model.

Values can be fixed values, or existing macros visible from the hierarchy (for example, customer or site), where the CFT is applied.

CFTs allow you to define default values for items exposed in the Admin Portal (visible, hidden, or read-only). CFTs provide a way to map data from data input via the Admin Portal or device model events to other models or provisioning workflows in the system.

You may want to hide the attributes of a model while setting them to a specific fixed value (for example a hard-coded setting); or you may wish to derive the value based on a macro (for example, look up the value based on data in the system).

Examples

- A model with an attribute defined as a date string; a CFT for the attribute can be defined as a macro `{{fn.now \"%Y-%m-%d\"}}` in order to set the current date stamp as the value, such as `2013-04-18`. Designers can access reference material for details on macros.
- A model such as Quick Add User, which limits user input to a few fields while deriving the value of other hidden attributes from various CFTs that are each applied to different underlying models that make up a user, such as voicemail account settings, conference account settings, phone, line, or device profile settings.

When adding or updating an instance of the model, the CFT enabled on the model is applied.

For array elements of data models, a list and a variable can be specified to be looped through so that a value is applied to each element in the model array.

You can create one or more CFTs for a model, and these can be used as needed. CFTs can also be applied to models in the design of, for example, provisioning workflows.

A menu layout that can be associated with a user role can also apply a CFT to a model that is selected as a menu item.

Provider administrators (and higher level admins) can quickly add a new CFT by opening a similar CFT (via, say, the Configuration Templates menu), then making a copy (clone) of it, and customizing the clone to create a new CFT.

Administrators at levels above the site admin can also customize these templates, including Field Display Policies (FDPs).

Note:

- When modifying CFTs in the Admin Portal, numerical values must be filled out using the `fn.as_int` function, for example:

  ```
  {{ fn.as_int 14 }}
  ```

Copyright © 2025 VisionOSS Limited. All rights reserved.

- In a multi-cluster environment, CFTs that result in device model drop-down lists in the Admin Portal may contain duplicates. Any duplicated item can be selected by the user.

Related Topics

- Cisco Quick User in the Core Feature Guide
- Quick Add Groups in the Core Feature Guide

Add a configuration template

This procedure clones and edits an existing configuration template (CFT) to create a new CFT.

1. Log in to the Admin Portal as Provider administrator or higher.
2. Go to **Configuration Templates** to view the list of existing CFTs.
3. Click on a configuration template (CFT) you wish to clone, and view its details.
4. Click **Action > Clone**.
5. Edit the required generic fields, such as **Name**, **Description**, **Target Model Type**, and the fields specific to the selected model type. See *Configuration template settings*

   Note: Some fields are populated based on specific conditions. For example, when creating a device instance CFT in a multi device or clustered environment, drop-down values in the CFT that originate from a device will be the values from *all* the devices in the cluster. For this reason, the list may include duplicates; in this case, you can choose any duplicate, if required.

6. Click **Save**.

   The new, cloned CFT appears at the selected hierarchy level.

Example: Add a CFT for a Cisco 6941 SCCP phone

1. In the Admin Portal, go to the relevant hierarchy, the hierarchy where the Cisco UCM you want to use exists.

   Note: This step is required if the fields are to populate values because some of the values are derived from the actual device model through the API.

2. Click the **Default CUCM Phone Template**, and then click **Action > Clone**.

   Note: Don't save your changes yet.

3. Change the template **Name** and **Description**.
4. Edit the template fields:
   - From the **Device Protocol** drop-down, choose **SCCP**.
   - From the **BAT Phone Template** drop-down, choose **Standard 6941 SCCP**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- From the **Device Security Profile** drop-down, choose **Cisco 6941 - Standard SCCP Non-Secure Profile**.
- From the **Product** drop-down, choose **Cisco 6941**.
- From the **BLF Presence Group** drop-down, choose **Standard Presence Group**.
- In the remaining fields, use the cloned default values.

Tip: You can type in the values if you know them; else, choose values from the list.

5. Click **Save**.

Configuration template settings

The table describes general fields on the **Configuration Template** page:

Note: Fields specific to the CFT for the selected target model type are excluded.

Title	Field Name	Description
Name *	name	The name that is given to the Configuration Template.
Description	description	A description for the Configuration Template.
Foreach Elements	foreach.[n]	Iterates over the list returned by the macro and appends array elements to the specified field.
Property *	property	The field property to iterate over.
Macro List *	macro_list	The macro that produces the list to iterate over.
Context Variable *	context_var	The context variable that will contain the data from the iteration.
Schema Defaults	schema_defaults.[n]	Applicable only when the configuration template is used directly in API requests. This attribute contains a list of paths to the properties of the template section that must be used to enrich the default values of the schema. All paths specified must refer to array attributes.
Target Model Type *	target_model_type	The target model type and name that the Configuration Template applies to.
Merge Strategy	merge_strategy	Determines how this CFT will be merged into another CFT when it is being processed in a PWF. Default: additive.
Template *	template	The contents of the template, such as defaults and macros. The names shown in the template are determined by the attribute names of the Target Model Type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Webex Calling Users and Service Settings

6.3. Cisco UCM App Integration and Detailed Settings

6.3.1. Cisco UCM configuration

Tip: *Use the Action search to navigate Automate*

Overview

Cisco Unified Communications Manager (Cisco UCM) devices provide the core call processing capabilities for HCS and are a critical part of the Automate provisioning workflows.

Cisco UCM devices must be configured before setting up the dial plan (if applicable), user, line, and phone configuration. The devices must then be assigned to one or more Network Devices Lists (NDLs), and the NDL is then assigned to one or more sites. The NDL is used to choose the Cisco UCM used for configuration, based on the site selected in the hierarchy context.

Related topics

- Flow Through Provisioning in the Core Feature Guide

Shared versus dedicated Cisco UCM

Cisco UCM devices can be dedicated to a specific customer, or they can be shared between multiple customers.

- To share the Cisco UCM across multiple customers, add it at the *Provider* or *Reseller* hierarchy.
- To dedicate the Cisco UCM to a single customer, add it at the *Customer* hierarchy.

  When setting up Cisco UCM as a dedicated instance, you can choose to set up Cisco UCM after creating the customer.

Servers within a Cisco UCM cluster

Within a Cisco UCM cluster, you can configure the following nodes:

- Cisco UCM publisher node

  Note: Configure a Cisco UCM publisher node before configuring any other type of node.

- Cisco UCM subscriber node
- IM and Presence service publisher node

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Configure an IM and Presence Service Publisher node before configuring an IM and Presence Service Subscriber node.

- IM and Presence Service Subscriber node

Sync with Automate

Configuring a Cisco UCM device on Automate creates a *scheduled data sync* to import model data from the device into Automate.

Note: Some license-related models are excluded from UCM imports by default:

- `device/cucm/LicensedUser`
- `device/cucm/LicensingResourceUsage`
- `device/cucm/HcsLicense`
- `device/cucm/CiscoCloudOnboarding`
- `device/cucm/RegistrationDynamic`
- `device/cucm/RoutePlan`
- `device/cucm/EndUserCapfProfile`

The *scheduled data sync* ensures that the Automate cache maintains the most current view of the configured device. Any changes to the configuration occurring on the device, including additions, deletions, or modifications, reflect in Automate after the next data sync.

Note:

- There is no immediate data sync upon update or modification.
- The *scheduled data sync* fails if the CUCM administrator account credential has expired. Expiration of the administrator account credential can cause failures in user management activities as well.

The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule via the (CUCM) **Schedules** page.

When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync. You can also manually run the data sync at any time via the **Data Sync** page.

Important: Allow the initial data sync to complete before doing more configuration on Automate that requires information from CUCM.

To improve the performance of a data sync, control the types of data synced in. See *Model Type Lists (MTL)* for more information.

For details on Change Notification Sync in Automate and on switching between Full Sync and Change Notification Sync, refer to the topic on the Change Notification Feature (CNF) following *Cisco UCM Change Notification (CNF) Sync*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field mappings in Cisco UCM

When setting up a CUCM device with LDAP integration, you can map CUCM user data to Automate user data for any field, based on the Field Mappings in the CUCM server. These mappings are configured at the LDAP Directory in CUCM. The mapped user data, for example location data, can later be used in a filter used to move users to sites.

On the **Field Mappings** tab, you can modify the mappings except for hard-coded mappings. Hard-coded mappings appear in gray and are read-only.

Note: The field name entered in the mapping on Automate must exactly match the field name entered in the mapping in the UCM in the Custom User Field Name field. If the field names do not match, the field is skipped during the sync.

Related topics

- User Field Mapping in the Core Feature Guide

6.3.2. Add Cisco UCM group

provider-admin

Tip: *Use the Action search to navigate Automate*

This procedure creates a Cisco Unified Communications Manager (Cisco UCM or Call Manager) group.

1. In the Admin Portal, set the hierarchy as *Customer*.
2. Go to **Call Manager Groups**, then click the Plus icon (+) to add a new record.
3. At **Network Device List**, select the appropriate NDL to add a new region, and then click **OK**.
4. At the **Name** field, fill out **RSMSimPhone** for the CUCM group name.
5. Select the **Auto-registration Cisco Unified Communications Manager Group** checkbox if required. Only use this when setting **TFTP Default** to true, which will result in setting all other CUCM groups to false.
6. Click the Plus icon '+' adjacent to **Unified CM Group Items** to add CUCM group items.
7. From the **Call Manager Name** drop-down, choose the required CUCM and then enter the priority.
8. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.3.3. Clone an instance of a Cisco UCM device model

Tip: *Use the Action search to navigate Automate*

To save time, make a copy of an existing instance of a device model rather than adding a new one. To do this, use the clone operation. When you create a clone, give it a new unique name and modify other device model fields as needed before saving.

Note: You can clone an instance of a device model to the same Cisco UCM or to a different Cisco UCM.

If you clone to a different UCM, ensure that all device model fields have values that are appropriate for the target UCM. For example, make sure calling search spaces specified in the source instance exist on the target UCM.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Go to **{device_model_type}**.
3. From the device model list, select the instance to be cloned.
4. Click **Action > Clone**.
5. Depending on the device model, do one of the following:
   - When prompted, choose the NDL that contains the target Cisco Unified CM.
   - choose the target UCM from the **CUCM** drop-down menu.
6. At the **Name** field, fill out a unique name for the new instance of the device model.
7. Modify other fields, as required.

   For further details about these fields, see the corresponding topic on configuring a new instance of the device model. For example, if you are cloning a SIP trunk, see under *SIP trunks* for the SIP trunk field descriptions.
8. Click **Save** to save the cloned instance.

   The new instance appears in the list. The new instance is created on the target UCM.

6.3.4. Multi-cluster or single cluster configurations

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Previously, IM and Presence Service (previously known as CUP) was set up in a cluster separate from the Cisco Unified Communications Manager (UCM) cluster, in a configuration known as *multi-cluster*.

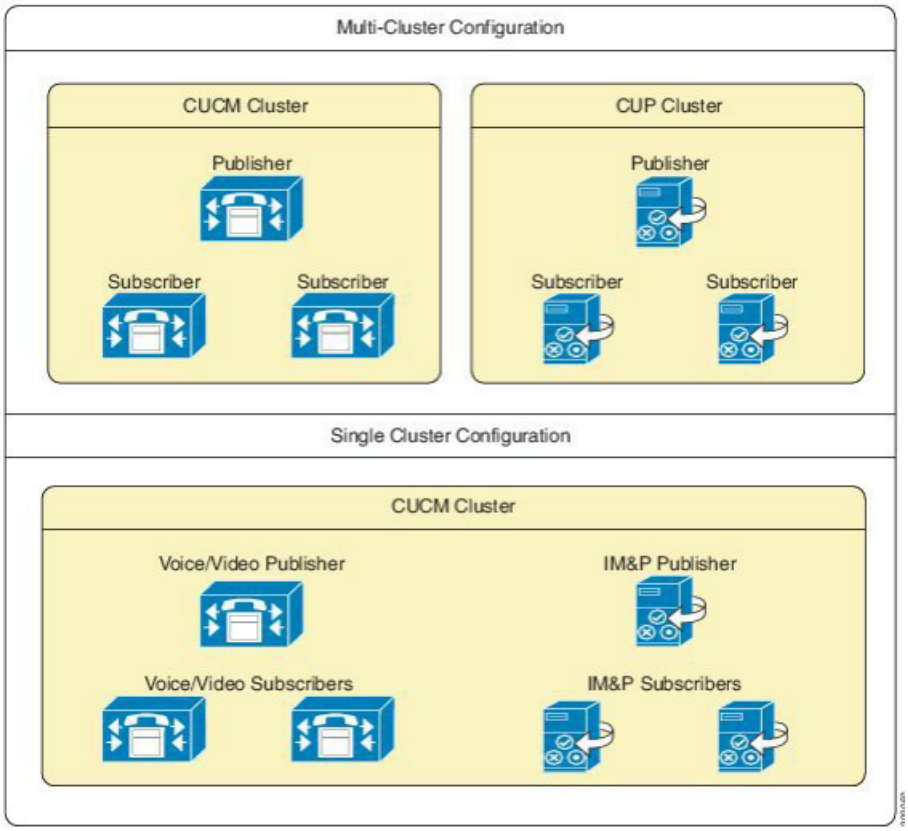
However, the IM and Presence Service servers are set up as part of the UCM cluster itself, in what is called a *single-cluster* configuration.

Advantages of a single-cluster configuration

A single cluster configuration is recommended, and service providers are encouraged to use this configuration for any new clusters.

Single-cluster configurations have the following advantages:

- Correctly represents the UCM cluster with its IM and Presence Service servers in the management layer
- Eliminates the confusion that *multi-cluster* configurations can cause for administrators when these servers are shown in different clusters.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Deprecation of multi-cluster configurations

Multi-cluster configurations are deprecated and strongly discouraged. However, Automate continues to support multi-cluster configurations for backward compatibility and upgrades.

Convert a multi-cluster configuration to single cluster

This procedure migrates your CUP (also known as IM and Presence Service) nodes to a UCM cluster (single-cluster configuration - the recommended option).

Migrating CUP nodes to a UCM cluster is hierarchy-specific:

- A Customer CUP node can only be migrated to a Customer UCM cluster (not to a Provider or Reseller cluster)
- A Publisher IM_P node is added first, then Subscriber nodes.

Conditions that apply when migrating your CUP to a UCM cluster:

- Cluster versions must be the same for both the clusters
- The IPv4 address or hostname and domain configuration must not be duplicated within the cluster
- Two devices cannot have the same server name
- No more than one CUP publisher can be migrated to the same UCM cluster
- Multiple users can be migrated to the same UCM cluster

To convert existing multi-cluster configurations to single-cluster configuration:

1. Log in as Provider, Reseller, or Customer administrator, depending on the hierarchy level where the CUP cluster was configured.
2. Set the hierarchy path to the hierarchy node where the CUP cluster was configured. Choose an option:
    - Shared configuration? Set the hierarchy to Provider or Reseller node.
    - Dedicated configuration? Set the hierarchy to a Customer node.
3. Go to (CUP - deprecated) **Migrate CUP to CUCM Cluster**.
4. At **From CUP Cluster**, select the CUP cluster you wish to migrate.
5. At **To CUCM Cluster**, select the UCM cluster to which you want to migrate the CUP cluster.
6. Click **Save**.
    - The migrated CUP server is removed from the (CUP) **Servers** list, and displays instead on the (UCM) **Servers** list as server type, **IM_P**.
    - The cluster name for the migrated servers is now the same as the UCM cluster name.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.3.5. Configure intelligent proximity for mobile voice

provider

Tip: *Use the Action search to navigate Automate*

This procedure configures intelligent proximity for mobile voice in Automate.

Prerequisites:

Ensure you have the latest COP files for your Cisco IP phone, or device package downloaded and installed in Cisco Unified Communications Manager (UCM). To do this:

- In your browser, go to https://software.cisco.com/download/navigator.html?mdfid.
- In the Product Search window, enter Unified Communications Manager Version 10.5.
- Choose Software Type Unified Communications Manager/CallManager Device Packages.
- Download and install the file cmterm-devicepack 10.5.2 12020-1cop.sgn in Unified CM.

Each phone you register to UCM contains phone-specific settings. These settings appear in UCM at the bottom of the **Phone Configuration** window under the Product Specific Configuration Layout heading.

The settings vary by phone model, and are tailored to each phone model. The phone has default settings, but in the Unified CM Phone Configuration window, you can override the settings and configure new values.

Task overview

- Ensure all required settings are enabled on Cisco Unified CM.
- Import the settings into Automate so they appear on the **Phone Management** page for each registered phone.
- Ensure the settings are correct in Automate.
- Pair the mobile phone or tablet with the Cisco IP endpoint.

Enable settings on Cisco UCM

1. Enable settings on Cisco UCM, on the **Device** page:
   - Proximity Mode - Choose ‘On’
   - Call Control - Choose ‘Enabled’
   - Proximity Content Share From Clients - Choose ‘Enabled’
   - Proximity Content Share To Clients - Choose ‘Enabled’
2. Import settings to Automate:

   Import phone features (or refresh existing phone features) using Automate’s Import/Refresh function.

   This step imports each phone type’s features as listed on the Product Specific Configuration Layout page in **Devices > Phones** in UCM, into Automate.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate imports the settings and only shows settings that were available and imported the last time the command was run.

Perform this step any time there is a change on the Unified CM, such as adding new phone types or templates. However, it is recommended that you perform this step every time.

To import or refresh phone features:

a. Log in to Automate as provider or reseller administrator.

b. Go to **Perform Publisher Actions**.

c. From the **Action** drop-down, choose **Import**.

d. From the **App Type** drop-down, choose **CUCM Device**.

e. In the **Clusters** dialog, click the cluster to be configured for the Intelligent Proximity feature in the **Available** window. Click **Select** to move the cluster to the **Selected** window.

f. Click **Save**.

3. Verify that Bluetooth settings are enabled.

   a. Log in to Automate as customer administrator and choose a valid site from the hierarchy node.

   b. Go to **Phones**.

   c. Choose the endpoint to pair with the mobile phone or tablet.

   d. On the **Advanced Information** tab, ensure these fields are set correctly if they appear for the selected endpoint type:

      - **Bluetooth** drop-down - **Enabled**.
      - **Allow Bluetooth Contacts Import** drop-down - **Enabled**.
      - **Allow Bluetooth Mobile Handsfree Mode** drop-down - **Enabled**.

4. Pair the mobile phone or tablet with the Cisco endpoint (device such as a desk phone). For more information, see 'Intelligent Proximity for Mobile Devices' in http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/8811_8841_8851_8861/10_5/ english/userguide/P881_BK_C9A41445_00_cisco-ip-phone-8811-8841.pdf.

   a. At the Cisco IP endpoint, ensure that Bluetooth and Handsfree 2-way audio are enabled.

   b. Add the mobile device. Once the mobile device is discovered, you can pair the two and also store mobile contacts on the Cisco IP endpoint.

   c. A security code may appear on both the endpoint and mobile device. Accept the security code on both the Cisco IP endpoint and mobile device before the pairing can be completed.

6.3.6. Cisco UCM Detailed Configuration

CUCM Servers and Nodes

Cisco UCM servers

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Cisco UCM server

This procedure adds and configures a Cisco UCM server within a UCM cluster.

1. Log in to the Automate Admin portal with the appropriate hierarchy administrator credentials.
   - **Creating a shared instance**? Log in as provider or reseller admin.
   - **Creating a dedicated instance**? Log in as customer, provider, or reseller admin.
2. Set the hierarchy path to the correct level:
   - **Creating a shared instance**? Set the hierarchy to the provider or reseller level.
   - **Creating a dedicated instance**? Set the hierarchy to the customer level.
3. Go to the **CUCM Servers (all Servers)** list view.
4. Click the Plus icon (+) to add a new server.
5. On the **Base** tab/panel, configure server details:

Field	Description
CUCM Server Name	Fill out the UCM server name.
Publisher	When checked, defines that the UC application instance is a publisher, and displays an additional tab/panel (Publisher). When unchecked, defines that the UC application instance is a user. When checked, you'll fill out the Publisher tab/panel fields in the next step.
Cluster Name	For a UCM Publisher node, fill out the **Cluster Name** field with the name you want for this cluster. A new cluster is created with this name. For UCM users, choose the UCM cluster from the **Cluster Name** drop-down.
Server Type	Mandatory. Choose an option, either **VOICE_VIDEO** or **IM_P**.
Sync on Create/Update	Defines whether to trigger a sync (auto-import) of the UC app server when saving the form.
Network Addresses	Add network addresses, one or more. Click the Plus icon to add a network address, then fill out details: • At **Address Space** (the type of network address), select **SERVICE_PROVIDER_SPACE**. If NAT is used, you'll need to add an additional network address (click the Plus icon at **Network Addresses**), but select address space option *APPLICATION_SPACE* as the second address space. Additional configuration of NAT on Arbitrator is automated. For more information around setting up assets and probes on Insights Arbitrator, see the Insights documentation. • The **Hostname** field is automatically populated with the UCM server name. Edit it if necessary. • At **IPv4 Address**, fill out the IP address of the UCM server. Either the hostname or the IP address is required. Ensure the hostname or IP address does not contain a trailing blank space since Automate can't validate entries that contain a blank space at the end of the hostname or IP address. • Fill out the domain of the UCM application. • Provide an optional description for the network address.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Credentials	Click the Plus icon to add a set of credentials, one or more: • Credential type is *ADMIN*. This credential is required for Service Inventory to generate reports for UC applications. Expiration of the ADMIN account results in failed data syncs between UCM and Automate. • Fill out the user ID and password that you configured when installing the UCM. • Optionally, provide a description for the credential. The UCM Admin Account requires the following roles (can be added in a group): • For normal AXL Add, Update, Delete transactions: *Standard AXL API Access* • For Extension Mobility Login/Logout: *Standard EM Authentication Proxy Rights* • For querying the Phone Status via RIS API, uploading MOH files via GUI (Selenium Driver) and enabling Headset Service (also RIS API): *Standard CCM Admin Users*

6. On the **Publisher** tab/panel, fill out details for the publisher node.

Note: This tab/panel displays *only* if the **Publisher** checkbox is selected on the **Base** tab/panel.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Call Processing ID	The Call Processing ID of this cluster
SDR Cluster ID	The SDR UCM cluster ID, as shown on **SDR Configuration > SDR CUCM Clusters**.
Version	Choose the version of the UCM servers in this cluster.
Multi-Tenant	Read-only. If creating at Provider level, this field is set to *Shared*. If creating at customer level, this field is set to *Dedicated*.
Port	The port on the UCM server to connect to. Default is 8443.
User Move Mode	Choose **Automatic** to automatically move synced in users to sites, based on the filters and filter order defined in **User Management > Manage Filters**. Choose **Manual** if you want an Administrator to manually move synced in users to a Site.
User Entitlement Profile	Choose the Entitlement Profile that specifies which devices and services users synced from this Cisco UCM are entitled to. Note: A violation of the Entitlement Profile does not prevent a user from being synced to Automate from Cisco UCM. However, subsequent updates to the user fail until the user's configuration satisfies the restrictions set in the Entitlement Profile.
Enable Change Notification Sync	Defines whether to enable Change Notification. When enabled, a Change Notification data sync and corresponding schedule will be created. The schedule is initially created as Disabled and needs to be manually enabled from the Scheduling menu. The Change Notification Sync interval is set to 14 days by default.
Monitoring	For new servers and if Arbitrator servers are available, monitoring can be enabled for this UCM on Insights. The Arbitrator server checkboxes can be selected to add the server as an asset. The Arbitrator server will be updated. Existing servers can be managed from the Onboard Assets and Offboard Assets menus under Insights. The arbitrator checkboxes will then reflect the asset status.

7. Inspect the default mappings and modify if required, see *User field mapping*.
8. Click **Save**. A UCM network device is created in Automate. (If installed, a cluster and UCM are created in the SDR.)
9. Test the connection between UCM and Automate.

Related topics

- For details on monitoring and Insights, refer to *Introduction to Insights monitoring*.
- For more information on Change Notification Feature (CNF) see *Cisco UCM Change Notification (CNF) Sync*.
- *Restore a Cisco UCM server*
- *Delete a Cisco UCM server*
- *Test the connection from the Cisco UCM server to Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Test the connection from the Cisco UCM server to Automate

Once you've added a UCM server, you should test the connection between the UCM server and Automate.

1. In the Automate Admin Portal, go to the **CUCM Network Devices** list view.
2. Click on the UCM you added.
3. Click the toolbar **Test Connection** icon.
4. If the test fails, and you used a hostname, ensure that Automate has the correct DNS and Domain set. Refer to the *Network services* topic in the Platform Guide.
   a. Log in to the platform CLI.
   b. Query the current DNS setting: **network dns**.
   c. Set the DNS if needed: **network dns <dns_server_ip_address>**.
   d. Query the current domain setting: **network domain**.
   e. Set the domain if needed: **network domain <domain>**.

Note:

- Use the **CUCM Network Device** page only for testing the connection. Do not edit UCM from this page. To change any configuration of the UCM, edit it via the **Servers** (UCM) page in Automate.
- After updating DNS servers, you'll need to restart the selenium service on the platform CLI:

```
app start selenium
```

Delete a Cisco UCM server

Deleting a Cisco UCM server in Automate also deletes local data that has been synced to it from the UCM server, including:

- Users
- Configuration parameters
- Dial plan information (if applicable)

Restore a Cisco UCM server

When restoring a UCM server from a backup, you will need to run a full sync without workflows after the restore, then run the overbuild to return your records to the correct sites.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Set Up IM and Presence Service servers

This procedure configures IM and Presence Service servers within a Cisco Unified Communications Manager (UCM) cluster.

1. Log in as the appropriate hierarchy administrator.
   - **Creating a shared instance**? Log in as provider or reseller admin.
   - **Creating a dedicated instance**? Log in as customer, provider, or reseller admin.
2. Set the hierarchy path to the correct level:
   - **Creating a shared instance**? Set the hierarchy to the provider or reseller level.
   - **Creating a dedicated instance**? Set the hierarchy to the customer level.
3. Go to the **CUCM Servers (all Servers)** list view, then click the Plus icon (+) to add a new server.
4. At **CUCM Server Name**, fill out the IM and Presence Service server name.
5. At **Server Type**, select **IM_P**.
6. To configure a publisher node, select the **Publisher** check box.

   Note: The **Publisher** tab is not populated for an IM and Presence Service publisher node.

7. At **Cluster Name**, select the UCM cluster.
8. Expand **Network Addresses**.
   a. At **Address Space**, select the *SERVICE_PROVIDER_SPACE* address space.
   b. The **Hostname** field is automatically populated with the IM and Presence Service Server Name. Edit it if necessary.
   c. At **IPv4 Address**, fill out the IP address of the IM and Presence Service server.

      Note: Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Automate cannot validate an entry that contains a blank space at the end of the hostname or IP address.

   d. Fill in the domain of the IM and Presence Service application.
   e. Provide an optional description for the network address.

   If NAT is used, also configure an APPLICATION_SPACE network address.
9. Expand **Credentials**.
   a. Add credentials for credential type *ADMIN*. ADMIN is required for Service Inventory to generate reports for UC applications.
   b. Fill in the user ID and password that you configured when you installed the IM and Presence Service.
   c. Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
   d. Provide an optional description for the credential.
   e. Click the Plus icon (+) to add more credentials.
10. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Headsets

Overview

VOSS Automate supports Cisco headset management for Unified CM (Call Manager, or CUCM) version 12.5 SU3 onwards. See: *Headset enablement*. Third-party headset management may also be supported, depending on the headset type and Unified CM version.

Headset metrics are pulled from Unified CM and displayed on an easy to understand, read-only form in an inventory in VOSS Automate.

Headset data can be used for:

- Inventory tracking of assets and usage
- Integration into VOSS Insights for compliance checks, for example, headset firmware versions, correct headsets, etc.

Subscriber or phone headset data can be viewed in VOSS Automate.

Headset templates are also listed and custom templates can be added as required.

Headset Inventory

Note: Headset details on Unified CM are updated dynamically, for example when a headset is either connected or disconnected from a phone connected to the Unified CM.

To ensure regular headset status updates in VOSS Automate, we recommend that you create a custom data sync and schedule it to run on a daily basis or more frequently if required. See also:

- *Create a custom data sync* in the Core Feature Guide
- *Schedules*

The **Headset Inventory** list view and instance form (default menu **Subscriber Management > Headset Inventory**) will display the latest headset data after you have executed a sync.

There are two ways a headset can be associated with a user:

a. When connecting the headset to a phone that is associated to a user

b. When a user logs in to the headset. This method is typically used in an extension mobility environment (on Unified CM version 12.5 SU3). The headset is paired to a phone, which automatically logs the user in to the phone.

As soon as a Cisco USB Headset gets connected to, or disconnected from a phone on the Unified CM, the phone automatically provides details about the headset to the Unified CM.

VOSS Automate pulls this information from Unified CM, and displays it on the **Headset Inventory** form, allowing you to view and track headsets across clusters, providing headset details such as Headset Serial Number, Vendor, Model, Owner, Connected Device Owner, Connection Type, Connected Device Name, and so on.

- **Headset Last Change**: The date and time is the last connected time if a headset is disconnected.
- **Located At**: Derived from the location of the phone to which the headset is connected.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: For non-Cisco headsets, the Device Name is used as the Serial Number. Using the same non-Cisco headset in multiple phones creates duplicate headset records.

Headset Templates

The headset template allows you to associate User Profiles. The **Headset Templates** list (default menu **Subscriber Management > Headset Templates**) shows the following types of headset templates:

- Standard Default Headset Configuration Template - System default template. This template contains the headset settings supported by the latest headset firmware installed on your system for all your headset model series. You cannot edit the default settings though you can change the profile configuration setting.
- System Generated Custom Headset Template - This template has the headset configuration settings that were manually uploaded to the Unified CM server.
- Custom Headset Configuration Template - create customized headset templates as per your deployment needs:
  a. Clone an existing template.
  b. Rename the template.
  c. Change the configuration as required.
  d. Save it to the desired hierarchy level.

  See also *Create a clone*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Headset Configuration Settings

Field	Description
Name*	Enter a unique name to identify the headset template.
Description	Enter a description that identifies use of the template.
Associated User Profiles	To associate a User Profile to this template, click '+' and select the profile from the drop-down, which displays all User Profiles that are available to use with this headset **Note:** By default, all User Profiles are assigned to the Standard Default Headset Configuration Template. To associate a User Profile to a different template, create the new template and assign the User Profile to the new template.
Model Specific Settings	
Models	E.g. 521, 522, 531, 532
Model Series	E.g 500
Model Firmware	Select the required firmware version: • Remain on current version - choose this option if you want the headset to remain on the existing firmware version, i.e. the headset firmware version is not upgraded to the latest firmware version on the system. • Latest - choose this option if you want to upgrade the headset firmware version to the latest firmware version on the system.
Firmware parameters	Parameters as set on Unified CM: • Name: e.g. SpeakerVolume • Value: integer, e.g. 5 • Access: e.g. User • Usage ID: e.g. 32 One or more parameters can be set.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Headset enablement

Tip: *Use the Action search to navigate Automate*

To enable the Cisco Headset Service for a CUCM server listed on the (CUCM) **Servers** page, select **Enable Services** from the **Action** menu.

A **Headset Enablement** menu option is also available to carry out this action by means of transfer boxes for all the **Available** servers in a **Call Manager Cluster**.

A data sync instance is also created for each server, in the format: *HcsPull-<host>-headset_models* that can be used to schedule a move of new Headset Inventory instances down to the matching user's hierarchy when it is run.

Related topics

- *Headsets*

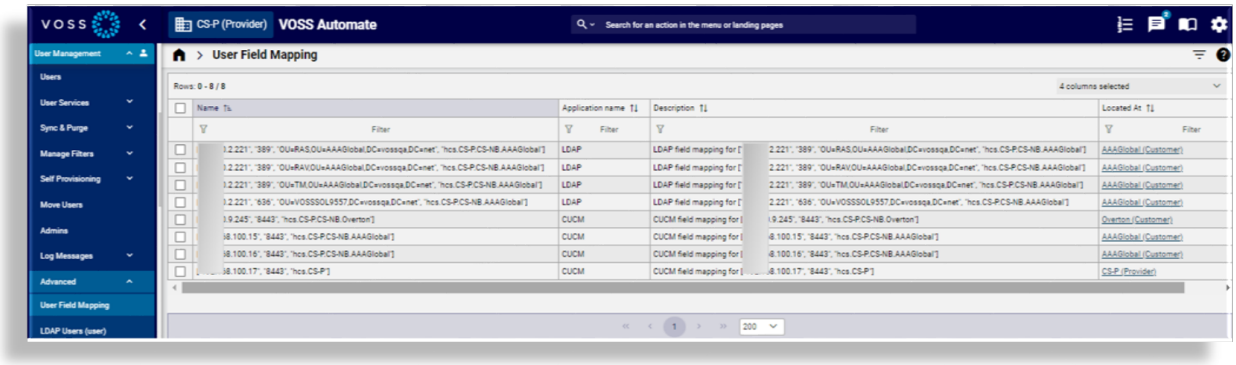
User field mapping

Tip: *Use the Action search to navigate Automate*

Overview

User field mapping in Automate refers to the alignment of data fields between Automate user data and other applications. The field mapping is required when syncing data between Automate and other systems.

To view available field mappings at the current hierarchy and below, go to **User Field Mappings**.



Automate provides a set of default (read-only) field mappings (named `default`) at the system level (`sys`) hierarchy. The default user field mappings are cloned and given an application name whenever an application is added at a hierarchy. For example:

- For CUCM applications, the name may be the IP address
- For LDAP applications, the name may be the business key of the LDAP server

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Users are only sourced from CUCM and LDAP (MS LDAP and OpenLDAP) instances so only these instances are created. The `default` instances are only visible at `sys` level.

When a CUCM cluster or LDAP server is added at, for example, customer level, these default mappings are cloned down to that customer level, and then become editable.

LDAP is used for both Microsoft AD and OpenLDAP

The cloned mapping displays on the **User Field Mappings** page and applies to user management at the hierarchy.

The mapping that applies at the sync hierarchy is used when values are written to Automate user data (for an application that is the sync source).

For example, the default CUCM mapping contains a mapping between the Automate "User Name" and the CUCM `userid`. When syncing user data from a CUCM source, the sync updates the Automate user.

The table describes mapping for applications stored in the `data/UserFieldMapping` model. These applications create cloned instances at the server level:

Application Name	Model Type	UC Source
CUCM	`device/cucm/User`	CUCM
LDAP	`device/ldap/user`	MS Active Directory
LDAP	`device/ldap/InetOrgPerson`	OPEN_LDAP

When syncing user data from a CUCM source, where this default CUCM field mapping applies at the hierarchy, the sync updates the Automate user. You can view the sync source for these users in the **Sync Source** column in the list view of the **Users** page. In this case, the sync source is `CUCM`.

Important: If application users related to a custom field mapping exist in Automate, existing mapped fields are read-only and can't be updated.

You can define up to ten custom values for each of the following field types, which can also be mapped:

- Up to 10 custom strings
- Up to 10 custom list of strings
- Up to 10 custom booleans

After a sync, custom values display on the **Custom** tab of an entry on the **Users/username** page.

Related topics

- For MS_365, see: *Microsoft mappings*

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP mappings

- LDAP Username
  - For Microsoft Active Directory, this is typically the `sAMAccountName`.
  - For AD LDS (ADAM), the `sAMAccountName` attribute is not part of the default schema, but can be added if required. Confirm with the LDAP server administrator. Alternatively, use `uid`.
  - For OpenLDAP, this is typically the `uid`.
- Sn (Surname)

Microsoft mappings

This section lists the user mappings from Microsoft users (`device/msgraph/MsolUser`) to Automate users. This `default` mapping instance in `data/UserFieldMapping` is not available for further configuration.

Note: For `email`, Automate captures and stores the primary email address from Microsoft 356 (0365) data where the value for the proxy address field starts with *SMTP* (case-sensitive, all caps). If a value is unavailable (the user doesn't have an Exchange mailbox), the value for UPN (UserPrincipalName) is used. If the user later obtains an Exchange mailbox, since `PrimarySmtpAddress` is on the `device/msgraph/MsolUser` allowlist, a user sync workflow is triggered to update the user's email address. See *Allowlists and denylists*.

```
"name": "default"
"description": "Default MS_365 field mapping"
"application": "MS_365"
"model_type": "device/msgraph/MsolUser"
"username": "UserPrincipalName"
"email": "PrimarySmtpAddress"
"first_name": "FirstName"
"last_name": "LastName"
"country": "Country"
"department": "Department"
"display_name": "DisplayName"
"city": "City"
"mobile": "MobilePhone"
"physical_delivery_office_name": "Office"
"postal_code": "PostalCode"
"state": "State"
"street": "StreetAddress"
"telephone_number": "PhoneNumber"
"title": "Title"
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

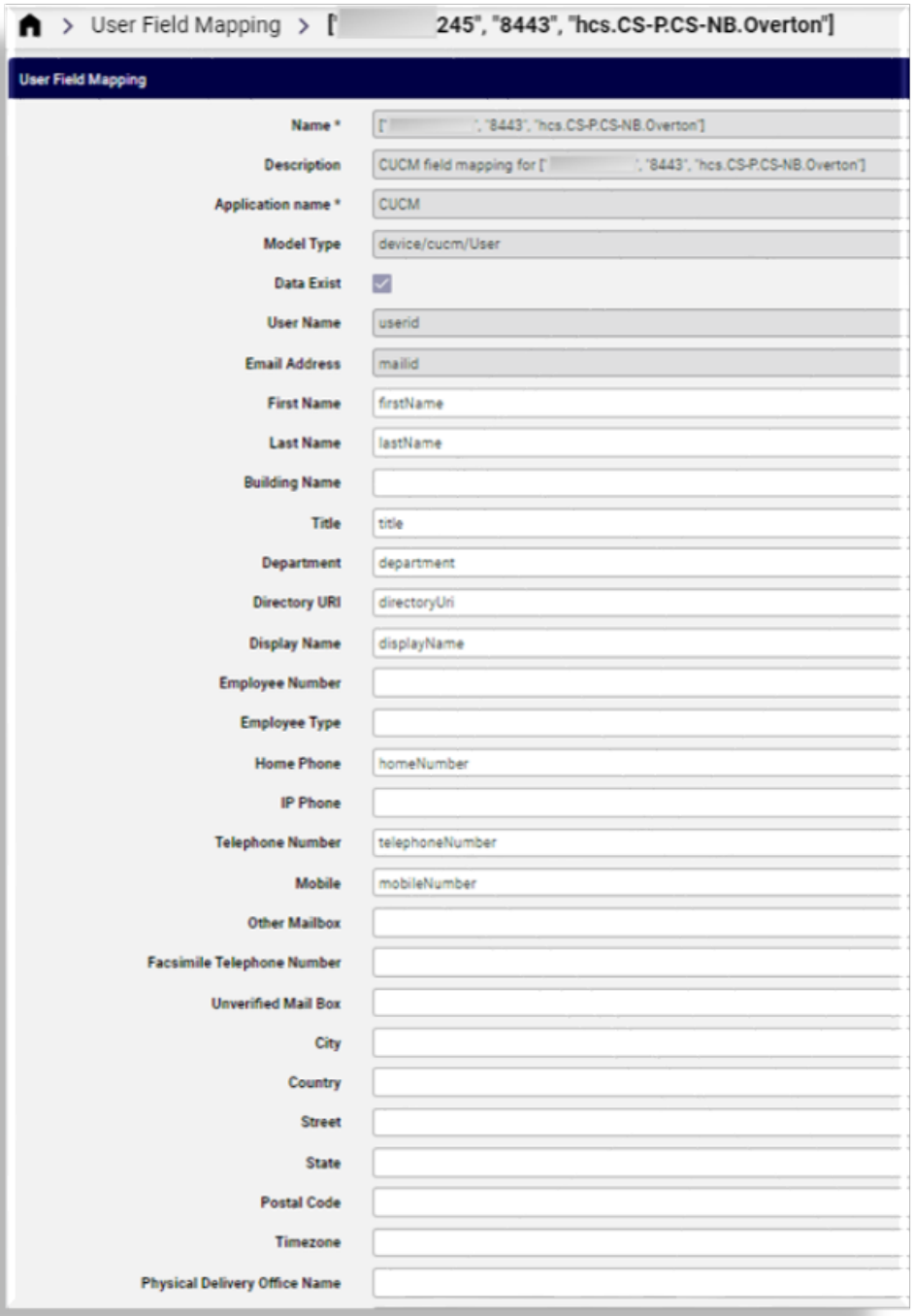
View user field mappings

To view LDAP and CUCM user field mappings:

1. Log in to the Admin Portal.
2. Choose a hierarchy.
3. Go to **User Field Mappings**.
4. View the list of mappings at the hierarchy.
5. Click on a user field mapping to view its details.

Important: Some fields in the hierarchy-specific field mapping are read-only. Any changes you make apply only to *new* users (field mapping changes won't apply to existing user data at this hierarchy).

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.

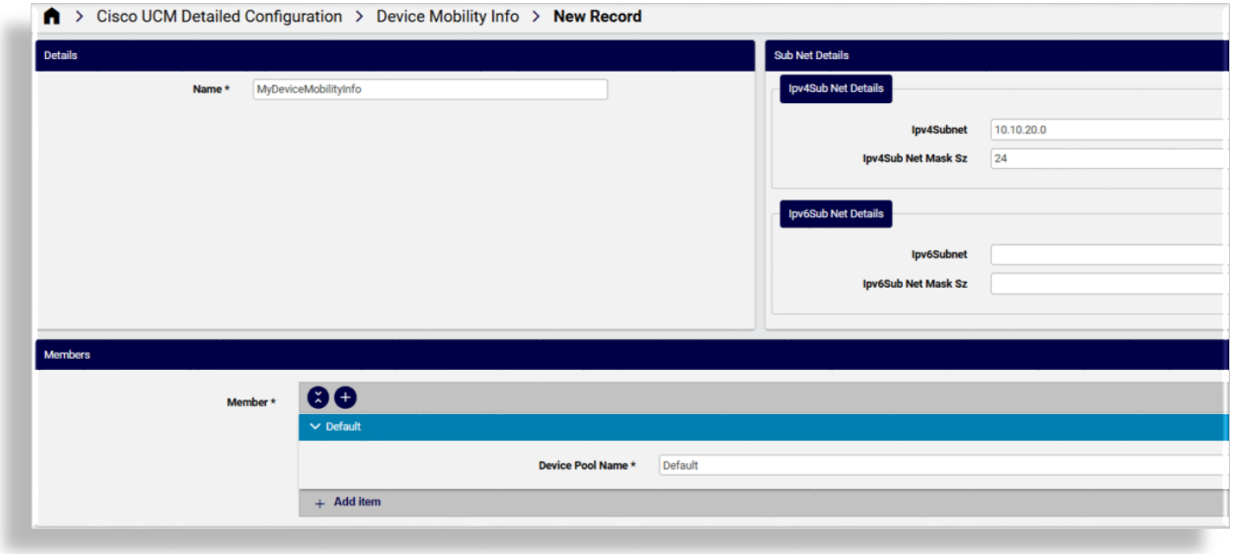
CUCM Parameters and Options

Device Mobility Info

Tip: *Use the Action search to navigate Automate*

On the Cisco UCM **Device Mobility Info** page you can add or update device mobility records for users to support roaming between sites.

Note: You can configure Cisco UCM device mobility records with either Ipv4 or Ipv4.



Phone Resources

Softkey templates

Tip: *Use the Action search to navigate Automate*

Introduction

Softkey templates manage softkeys that are used by the CUCM IP Phones, for example 7970. There are two types of softkey templates:

- Standard
- Customized

Automate includes the following CUCM system softkey templates - these can't be modified or deleted:

- Cisco Assistant with Feature Hardkeys
- Cisco Chaperone Phone with Feature Hardkeys

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Cisco Feature with Feature Hardkeys Standard
- Cisco Manager with Feature Hardkeys Standard
- Cisco Protected Phone with Feature Hardkeys
- Cisco Shared Mode Manager with Feature Hardkeys
- Cisco User with Feature Hardkeys
- Personal Conference User
- Public Conference User
- Standard User

A reseller administrator (or higher) can create customized softkey templates from the standard templates, make modifications as required and save them at the required hierarchy level, i.e. customer or higher.

Manage customized softkey templates and related softkey layout configurations

Note: The following device models need to be imported from Unified CM post upgrade before Softkey Templates can be managed.

This can be done by either performing a full import of Unified CM or using the "CUCM Softkey Templates" Model Type List which is available from Release 19.3.1.

```
device/cucm/SoftKeyTemplate
device/cucm/SoftKey
device/cucm/SoftKeyCallState
device/cucm/SoftKeySet
```

1. Browse to the required hierarchy.
2. Click **Add** to add a new customized softkey template.
3. From the **Create a softkey template based on** drop-down, choose an existing softkey template on which to base the customized template.
4. Enter a unique **Name** and **Description** for the customized template. The description can be a maximum of 50 characters but cannot include ", %, &, <, or >.
5. Select or clear the **Is Default** checkbox. If selected, this softkey template becomes the default standard softkey template.
6. Click **Save** to save the customized softkey template and simultaneously add it to the **Softkey Template** list view.
7. Select the newly created softkey template and configure the required softkey layout by modifying the designated softkeys for each call state.
   a. CUCM baseline softkey templates cannot be updated. Any change to such a template will result in a failed transaction.
   b. Some of the selected softkeys of the different call state are mandatory and cannot be removed from the CUCM standard set of templates. For example, template Standard User-Custom, Call State – On Hook, Softkey – NewCall.

   When a mandatory softkey is deleted, the transaction will be successful but the softkey will not be removed - when opening the template again it will still be there.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8. Click **Save** when complete.

Note: To modify a customized softkey template, select it from the **Softkey Template** list view and update as described in the above procedure.

Before deleting a softkey template, which has been marked as **Is Default**, a different softkey template must first be set as **Is Default**.

Related topics

- LDAP user sync in the Core Feature Guide.

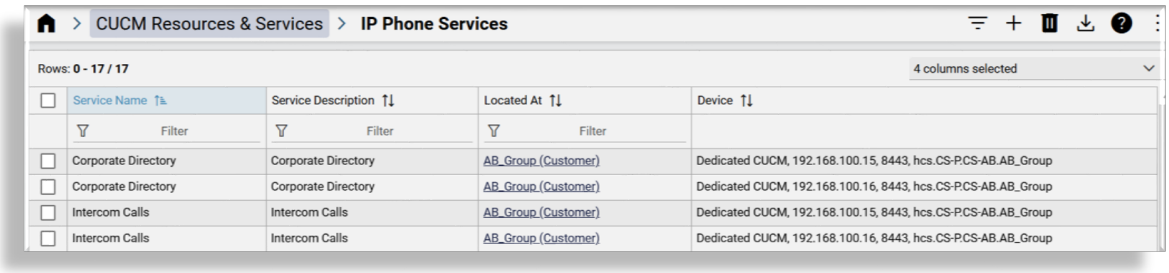
UC and Phone Services

Cisco UCM IP phone services

Tip: *Use the Action search to navigate Automate*

Automate supports the ability to add Cisco UCM IP phone services in a multi cluster environment.

1. Go to **IP Phone Services**.
2. At **UC and Phone Services**, click on **IP Phone Services**.
3. View the list of currently configured IP phone services at your current hierarchy level.



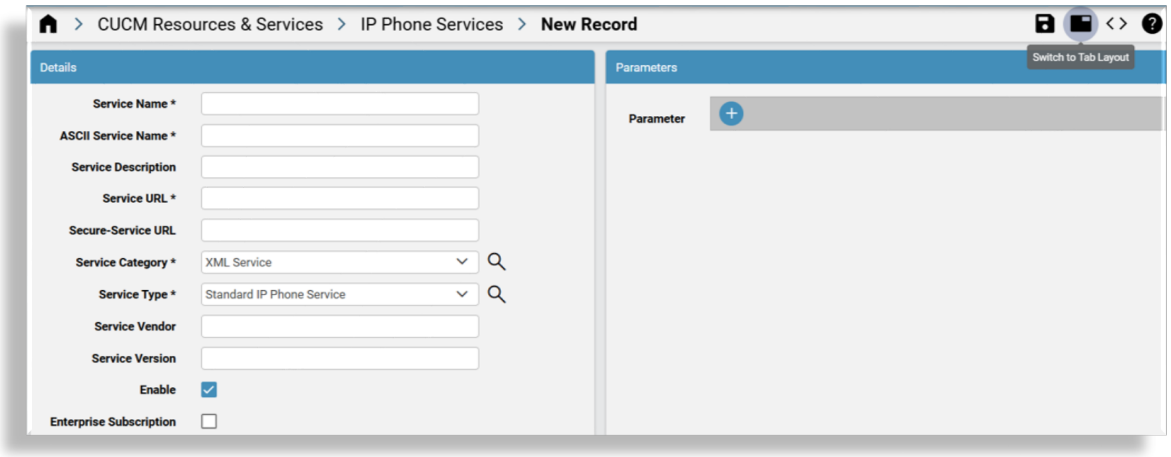
4. To add an IP phone service, click the toolbar **Plus (+)** icon.
5. If you're at a customer or higher hierarchy level, select a network device list (NDL).

   Note: You won't need to choose a NDL if you're at a site.

6. On the **IP Phone Services** > **New Record** page, fill out configuration details on the two tabs/panels that display - Details and Parameters.

   Note: The page displays as tabs or panels. You can toggle the layout via the **Switch to Tab/Panel Layout** button.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- On the **Details** tab/panel, configure IP phone service details.
- On the **Parameters** tab/panel, add IP phone service parameters, one or more.

The table describes the configuration required on the **Details** tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Service Name	Mandatory. The name of the service, maximum 128 characters. This service name displays wherever you can subscribe to a service, provided the service is not marked as an *Enterprise* subscription. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file. Cisco UCM allows you to create two or more IP phone services with identical names. Cisco recommends that you don't do so unless most or all phone users are advanced, or unless an admin always configures the IP phone services. If AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services. When the service URL points to an external customized URL, you can't localize the service name as per the device locale of the phone.
ASCII Service Name	Mandatory. The name of the service to display if the phone can't display unicode.
Service Description	Description of the content the service provides. Maximum 50 characters in any language. Double or single quotes are not allowed.
Service URL	Mandatory. The URL of the server where the IP phone service application is located. Ensure that this server remains independent of the servers in your CUCM cluster. Don't specify a CUCM server or any server that is associated with CUCM (such as a TFTP server or directory database publisher server). For the services to be available, the phones in the CUCM cluster must have network connectivity to the server. For Cisco-signed Java MIDlets, enter the location where the JAD file can be downloaded; for example, a web server or the backend application server to which the Java MIDlet communicates. For Cisco-provided default services, the service URL displays, by default, as `Application:Cisco/<name of service>`; for example, `Application:Cisco/CorporateDirectory`. If you modify the service URL for Cisco-provided default services, verify that you configured *Both* for the Service Provisioning setting, which displays in the Phone, Enterprise Parameter, and Common Phone Profile Configuration windows. For example, you use a custom corporate directory, so you change `Application:Cisco/CorporateDirectory` to the external service URL for your custom directory. In this case, change the Service Provisioning setting to *Both*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Secure-Service URL	The secure URL of the server where the UCM IP phone services application is located. Ensure that this server remains independent of the servers in your CUCM cluster. Don't specify a CUCM server or any server that is associated with CUCM (such as a TFTP server or publisher database server). For the services to be available, the phones in the CUCM cluster must have network connectivity to the server. If you don't provide a Secure-Service URL, the device uses the non-secure URL. If you provide both a secure URL and a non-secure URL, the device chooses the appropriate URL, based on its capabilities.
Service Category	Mandatory. Select a service application type (XML or Java MIDlet). If you choose Java MIDlet, when the phone receives the updated configuration file, the phone retrieves the Cisco-signed MIDlet application (JAD and JAR) from the specified Service URL and installs the application. The default is *XML Service* Options are: • XML Service (default) • Java MIDlet • Web Widget • Web Link • Android APK
Service Type	Mandatory. Defines whether the service is provisioned to the services, directories, or messages button/option on the phone; that is, if the phone has these buttons/options. To determine whether your phone these buttons/options, see the Cisco Unified IP Phone Administration Guide that supports your phone model. Options are: • Standard IP Phone Service (default) • Directories • Messages
Service Vendor	The vendor/manufacturer for the service. Optional for XML applications. Mandatory for Cisco-signed Java MIDlets. For Cisco-signed Java MIDlets, the value you provide for this field must exactly match the vendor that is defined in the MIDlet JAD file. This field displays as blank for Cisco-provided default services. Maximum 64 characters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Service Version	The version number for the application. Optional for XML applications (used for informational purposes only). For Cisco-signed Java MIDlets, consider the following: if you fill out a version, the service version must exactly match the version that is defined in the JAD file. If you fill out a version, the phone attempts to upgrade or downgrade the MIDlet if the version is different than what is installed on the phone. If the field is blank, the version gets retrieved from the Service URL. Leaving the field blank ensures that the phone attempts to download the JAD file every time that the phone re-registers to CUCM, as well as every time that the Cisco-signed Java MIDlet is launched. This ensures that the phone always runs the latest version of the Cisco-signed Java MIDlet without you having to manually update the Service Version field. This field displays as blank for Cisco-provided default services. You can enter numbers and periods in this field (up to 16 ASCII characters).
Enable	Defines whether to enable or disable the service without removing the configuration from CUCM administration (and without removing the service from the database). Clearing the checkbox removes the service from the phone configuration file and the phone. The default is *True*.
Enterprise Subscription	Defines whether to automatically provision the service to all devices in the cluster that can support the service. When enabled (checkbox selected), it's not possible to subscribe to the service. When disabled, you'll need to manually subscribe to the service for it to display on the phone (either in the Phone Configuration window, in BAT, or in the CUCM Self Care Portal). This setting displays only when you configure a service for the first time. After you save the service, the checkbox does not display in the window. To identify whether the service is provisioned to all devices in the cluster that can support the service, go to the Find and List IP Phone Services window and display the services. If true displays in the Enterprise Subscription column, you can't manually subscribe to the service. When *False*, you can manually subscribe to the service; for example, an end user can subscribe to the service through the CUCM Self Care Portal.

Phone-Based Registration Support

Introduction to Phone-Based Registration (PBR)

Overview

This topic provides an introduction for the installation, configuration, operation, and troubleshooting procedures for VOSS Automate's Phone-Based Registration (PBR) feature.

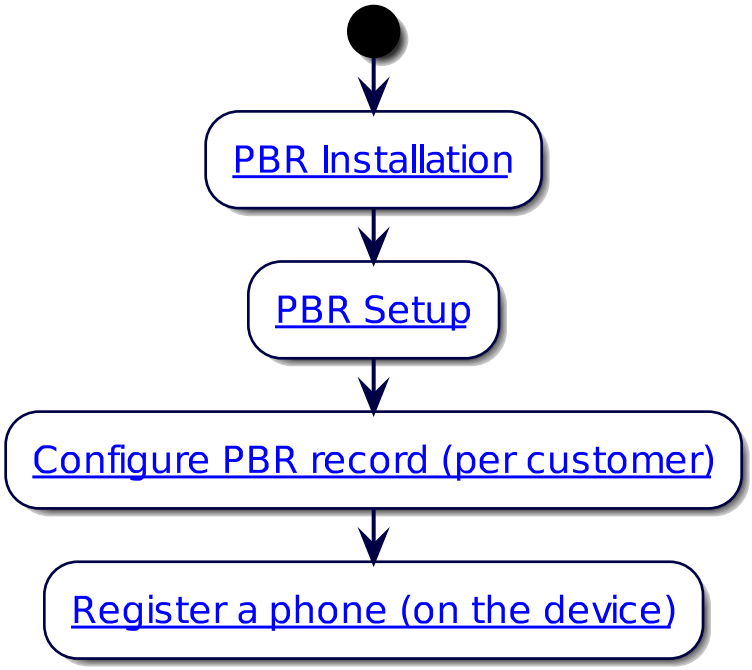
PBR allows an administrator to pre-provision Cisco phones for UC subscribers with rich and detailed configuration without requiring advance knowledge of the phone MAC address.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Given a pre-configured phone, PBR allows an end-user to access an auto-registered phone to register their pre-configured device via the Phone Services menus.

The flowchart provides a high-level workflow for PBR, including these steps:

- Install PBR (See *Install Phone-based Registration (PBR) Web Service*)
- Set up PBR (See *Configure Cisco UCM for AutoRegistration and PBR*)
- Add PBR Config records (one per customer) (See *Add PBR config records*)
- Register a phone (on the device) (See *Register a phone for phone-based provisioning*)



Related Topics

- *Install Phone-based Registration (PBR) Web Service*
- *Configure Cisco UCM for AutoRegistration and PBR*
- *Add PBR config records*
- *Register a phone for phone-based provisioning*
- *Add phone-based registration menus and access profile*
- *Create Restricted API Role and Admin User*

Copyright © 2025 VisionOSS Limited. All rights reserved.

PBR Architecture

VOSS Automate's Phone-Based Registration (PBR) feature is implemented as a Cisco Unified IP Phone Services Application.

This operates a web service on the VOSS Automate platform, for example, when installed on a multi-node cluster on all unified nodes, as shown in the following diagram:

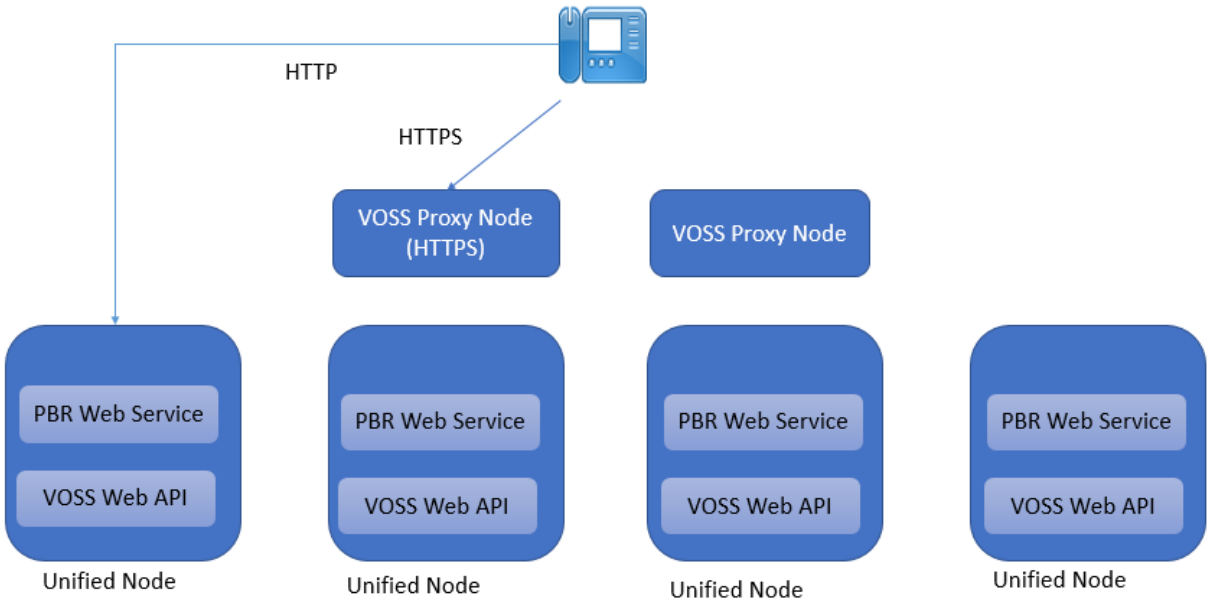


Figure 1: PBR network connectivity

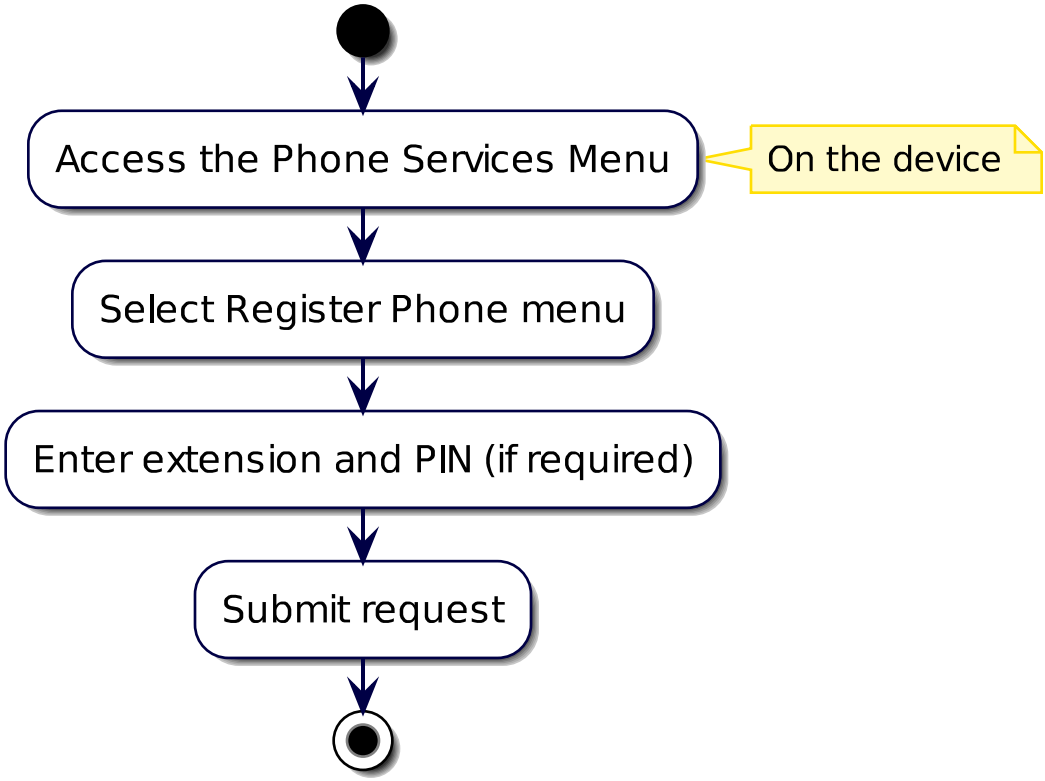
Register a phone for phone-based provisioning

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

The flowchart sets out the high-level steps for registering a phone:



Related topics

- *Introduction to Phone-Based Registration (PBR)*

Register and provision phone

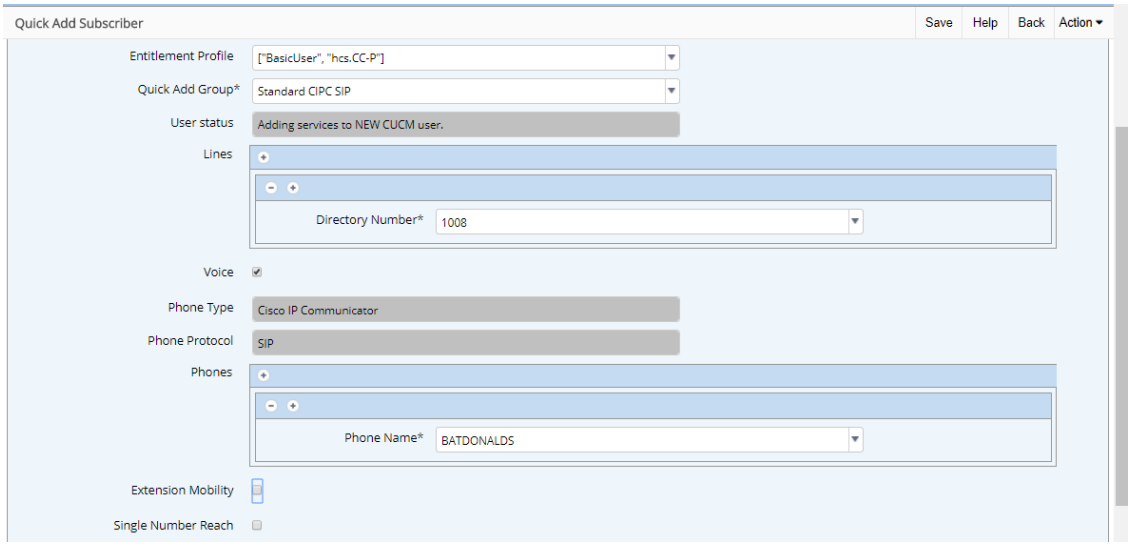
This procedure sets up a phone for PBR, provisions a PBR device record, and auto-registers the physical phone with UCM.

1. Set up a phone for phone-based registration:
   a. Provision a phone with a fake MAC Address, for example, *BAT000008012005*

      Note: You can provision a phone with a fake MAC address using bulk loaders, or via the Automate Admin Portal you can use Quick Add User, Automate Phone Management, or Advanced User features. In this case, we're using Quick Add User.

      The fake MAC address must have a BAT prefix, for example, BATABCABCABCABC.

Copyright © 2025 VisionOSS Limited. All rights reserved.



2. (Optional). Provision a PBR device record for the phone with a PIN:

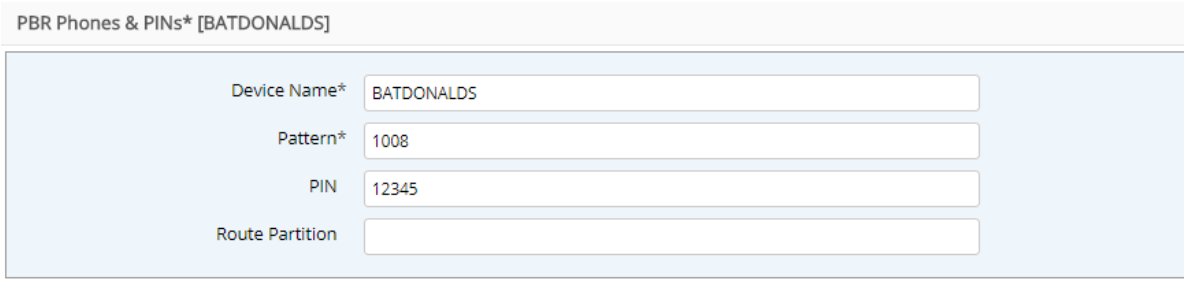
Note: Configure a PIN code that can be used to authenticate requests to register phones with Phone Based Registration.

The PBR device record assists with unique identification of device to replace where directory numbers are not unique within a UCM cluster.

---

   a. Go to **PBR Phones and PINS** then click the Plus icon (+) to add a new record.
   b. At **Device Name**, specify the device name of the pre-provisioned device with the fake MAC.
   c. Fill out the PIN. The minimum PIN length is 1 digit and the maximum is 6 digits.

Note: Route partition is not required unless a site-wide PIN is used.



3. Auto-register the physical phone with UCM:

Copyright © 2025 VisionOSS Limited. All rights reserved.

a. Select **Phone Services**.

b. Select **Register Phone**.

c. Enter extension and PIN (if required).

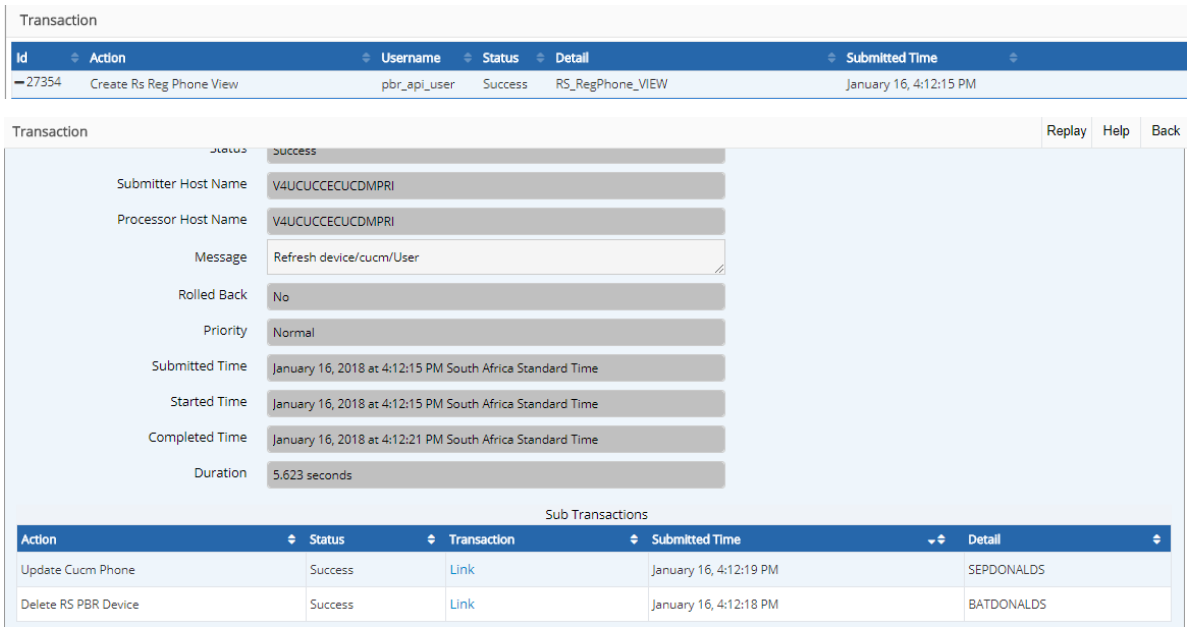
d. Submit request.

Copyright © 2025 VisionOSS Limited. All rights reserved.

A request is initiated to Automate to replace the configuration of the auto-registered phone with the rich settings defined for the pre-provisioned device with fake MAC.

The phone screen displays status, **Registering Phone**.

Verify in the Automate transaction log that the phone registration transaction displays.

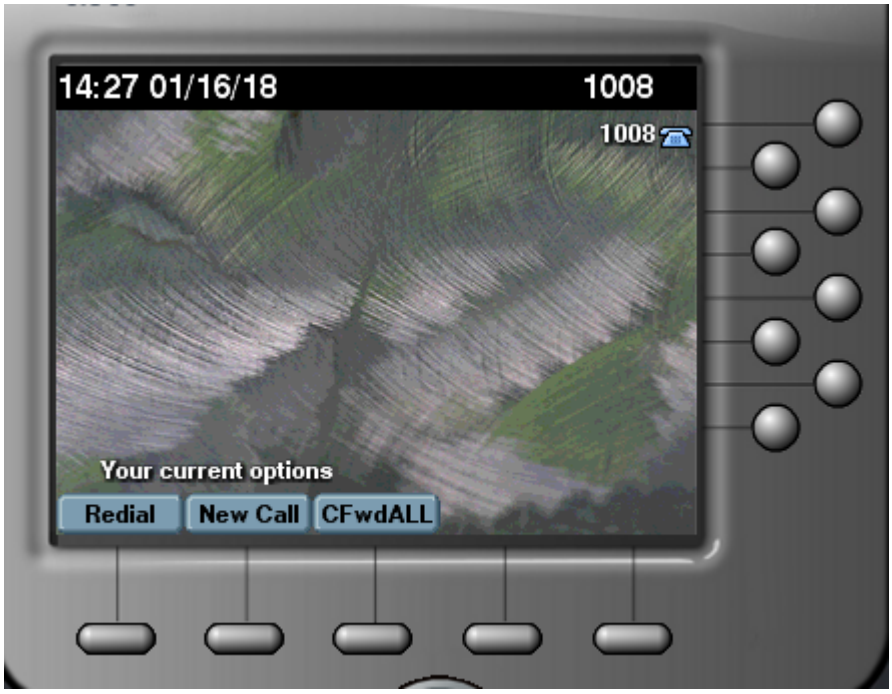


Note:

- The PBR device record is deleted (if you need to re-register this phone then a new record is required).
- The device name of the pre-provisioned phone (BATDONALDS) is updated to match the name of the auto-registered phone.

4. Once the transaction completes, verify that the phone reboots and shows the device configuration of the pre-provisioned phone.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Introduction to Phone Services

VOSS Automate's phone services feature provides a XML-based interface to user settings that can be utilized via Cisco IP phones.

Enabling phone services makes the following services available for users to interact with via their IP Phones, using the Telephone User Interface (TUI):

Service	Description
Speed Dials	Allows a user to manage and use their speed dials for the phones/extension mobility profile.
Call Forward	Allows a user to manage call forward destinations per line for key call forward options (all, busy, no answer).
Reset Pin	Allows a user that has Extension Mobility to reset their Extension Mobility PIN (CUCM PIN), provided they're logged in to the phone, and that the *RS_PBR_RestrictedAPIAccess* access profile has the *Create* permission configured for the following model: `view/ResetUCPasswordPinVIEW` Resetting the PIN also updates CUCM. **Note:** Reset phone has been tested on the following devices: Cisco 7970 SCCP, Cisco 7960 SCCP, Cisco 9951 SIP, Cisco 8841 SIP, IP Communicator
Corporate Directory	Search for and initiate calls with other users, from within VOSS Automate.

Copyright © 2025 VisionOSS Limited. All rights reserved.

These services display alongside other phone services that are set up in the system.

To use phone services, you'll need network connectivity between the phones and the VOSS Automate Proxy server instance. HTTP is supported only from the phones.

The phone services feature has been tested for support of the following phone types:

- 78XX, 88XX, 89XX, and 99XX
- Cisco IP Communicator

Note: Other Cisco phone models may also work with this feature. However, since we haven't tested them, it is strongly recommended that you use other phone models with caution and test them thoroughly in a lab environment before using them in production.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Configure phone services*
- *Manage Phone Services*

Add PBR config records

Tip: *Use the Action search to navigate Automate*

Overview

Phone-based registration (PBR) supports a number of configuration parameters that define how the service operates in a specific provider or customer environment.

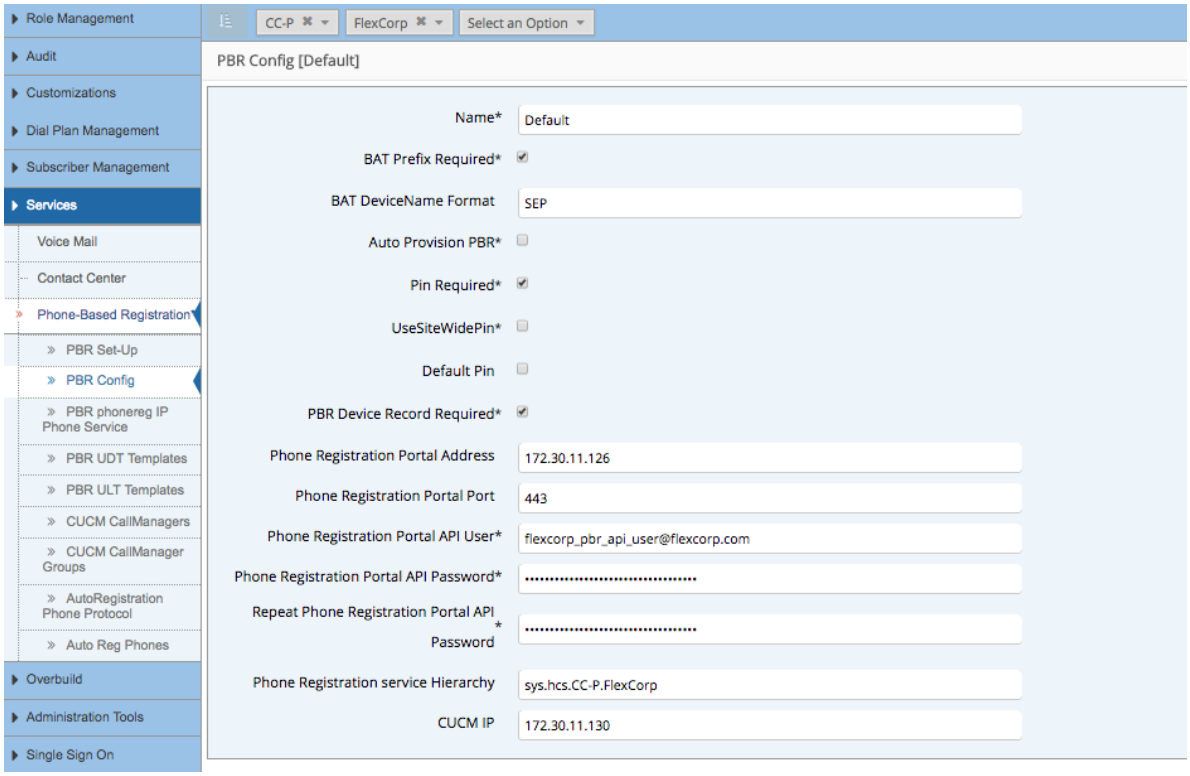
You will need to create PBR configuration (PBR config) records, as follows:

- Create a single PBR config record, globally, at Provider level.

  The global PBR config record at the Provider level allows the PBR web service to make the initial connection to the Automate API.

- Create a PBR config record for each customer that will use the phone-based registration add-on.

  The PBR config record at the Customer level defines the specific connection parameters for a specific customer, and eventually will allow per customer Automate user to be used.



Copyright © 2025 VisionOSS Limited. All rights reserved.

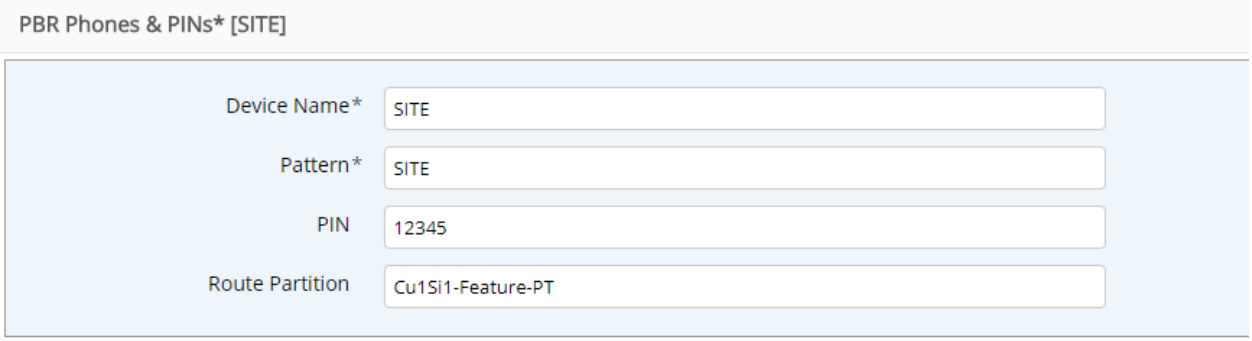
Related topics

- *Introduction to Phone-Based Registration (PBR)*

Provisioning PBR device records with site-wide PINs

Site-wide PINS are useful when PINs are required for either security or to address use-cases where DNs are not unique.

However, the operational overhead of provisioning a device record per unique device is not acceptable. In this case, create a single PBR device record at each site:



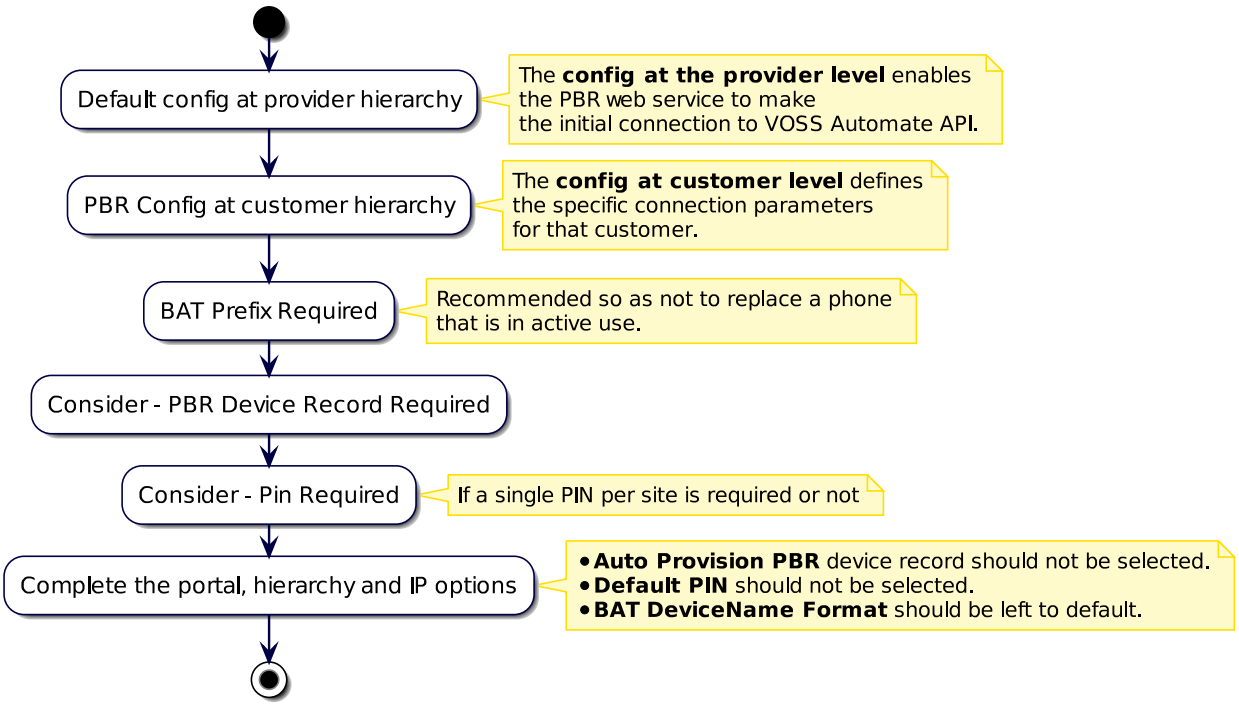
Note:

- When using site-wide PINS the device name and pattern must be hardcoded to use SITE. This is case sensitive.
- When using site-wide PINS the administrator must specify the route partition for the site.

Add PBR config records

This procedure configures the PBR registration. Instructions are provided for the PBR config record at the Provider level (global) and per customer.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Important: Do not select the following options. These features are experimental and should not be enabled:

- Auto Provision PBR device record
- Use default PIN

1. In Automate, go to **PBR Config**, then choose the hierarchy:
   - To set up the global PBR record, choose Provider hierarchy.
   - To set up the per customer PBR record, choose the relevant customer hierarchy.
2. Fill out a name for the PBR config record.
3. Select the **BAT Prefix Required** checkbox.

   Note:

   - It is recommended that PBR configuration should only allow the replacement of phones with fake MACs with device name prefix starting with BAT. This ensures that it is never possible for a user to replace a phone that is in active use.
   - Leave **BAT DeviceName Format** as *default*.

4. Choose options based whether the use of PBR device records is required in this environment?
   a. The PBR device record allows an administrator to explicitly specify that a device is eligible for phone-based registration.

      Select the **PBR Device Record Required** checkbox, if required.

   b. The PBR device record allows an administrator to specify that a PIN that should be used when performing phone-based registration for a specific phone or for all phones at a site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Select the **Pin Required** checkbox, if required.

c. The PBR device record can be used to guarantee that the correct device is replaced in environments where directory numbers are not unique within a CUCM cluster, for example, multiple directory numbers are configured with the same DN, but located in different partitions.

In this case, clear the **UseSiteWidePIN** checkbox.

Note: By default, Automate requires a PBR device record per device, but in some cases, it may be sufficient to use a single pin per site. In this case, you can enable (select) the **UseSiteWidePIN** checkbox. This provides limited security to ensure that a PIN is still required to register a phone, but reduces the operational burden by eliminating the need to provision a PBR device record for each phone. See *Provisioning PBR device records with site-wide PINs*

---

5. At **Phone Registration Portal Port** and **Phone Registration Portal Address**, specify the port and the IP address or hostname:
   - For HTTPS-based connectivity, the port should be *443* and the address is the IP address or hostname of an Automate proxy node in a cluster.
   - For HTTP-based connectivity, the port can be *80*, and the address is the IP address or hostname of the primary Automate unified node in a cluster.

Note: The phone registration portal address and the port you specify must be accessible from the phone network.

---

6. At **Phone Registration Portal API User** and **Phone Registration Portal API Password**, fill out the email address for the API user previously created, and fill out the password.

   See *Create Restricted API Role and Admin User*

Note: The portal API user credentials (username and password), is required for both the Provider-level PBR config record and for the PBR config record for any customers.

---

7. At **Phone Registration Service Hierarchy**, specify the hierarchy:
   - If the PBR config record is defined at Provider level, specify the hierarchy as in the following example: *sys.hcs.CC-P*.
   - If the PBR config record is defined at the Customer level, specify the hierarchy as in the following example: *sys.hcs.CC-P.FlexCorp*
8. At **CUCM IP**, specify the IP address of CUCM that is accessible to Automate using HTTPS SOAP requests.
9. Save the PBR config record you configured, then run the following CLI command on the primary node to restart the services:

```
cluster run all app start phone-based-registration
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a self-provisioning universal device template

When the administrator or user self-provisions a phone, Cisco Unified Communications Manager (CUCM) deletes the auto-registered phone and adds the phone back into the database. The Universal Device Template (UDT) for the user's profile determines the various phone settings for the user's phone.

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Go to **Universal Device Template**.
4. Click **Add**.
5. Enter the following required UDT information.

   Note: These fields can be pre-populated, depending on customer, site, and dial plan configuration: Name, Location, Common Phone Profile, BLF Presence Group

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Name	Enter the name of the UDT.
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC regulates audio quality and video availability by limiting the amount of bandwidth for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.
Common Phone Profile	Choose a common phone profile.
Phone Personalization	Enable this setting to allow the UDT to work with Phone Designer, a Unified Communications widget. The widget lets a user customize the wallpaper and ringtones on a device.
Busy Trigger	This setting, which works with Maximum Number of Calls and Call Forward Busy, determines the maximum number of calls to be presented at the line. If the busy trigger is set to 40, incoming call 41 is rejected with a busy cause (and is forwarded if Call Forward Busy is set). If this line is shared, all the lines must be busy before incoming calls are rejected.
Max Number Of Calls	You can configure up to 200 calls for a line on a device. As you configure the number of calls for one line, the number calls that are available for another line decreases.
MultiLevel Precedence and Preemption	This setting specifies whether a device that can preempt calls in progress uses the capability when it places an MLPP precedence call.
Do Not Disturb Option	When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls.
Blf Presence Group	Enter the presence group applicable for busy lamp field buttons.
Device Mobility Mode	Turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device.

6. Enter the following optional, but highly recommended information. These fields can be pre-populated, depending on customer, site, and dial plan configuration.

Field	Description
Device Pool	Enter a site-specific device pool.
Owner User ID	The userid of the user associated with the phone. The recommended is Current Device Owner's User ID.

7. Enter other optional settings, if applicable.
8. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a self-provisioning universal line template

The Universal Line Template (ULT) is used before self-provisioning actually takes place. ULTs are used to create directory numbers on Cisco Unified Communications Manager (CUCM). A directory number is identified by a pattern (the number portion) and a route partition. A directory number also has various settings that can be configured for the line. When a directory number is created using a ULT, the ULT determines the route partition and the line settings.

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Go to **Universal Line Template**.
4. Click **Add**.
5. Enter the following required Universal Line Template information.

Field	Description
Name	The name of the universal line template
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC regulates audio quality and video availability by limiting the amount of bandwidth for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.
Partition	Enter the route partition used to create lines at the site.
Blf Presence Group	Enter the presence group applicable for busy lamp field buttons.

6. Fill out additional optional settings, if applicable.
7. Click **Save**.

Cisco phones

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes how to manage Cisco phones in the Automate Admin portal.

Copyright © 2025 VisionOSS Limited. All rights reserved.

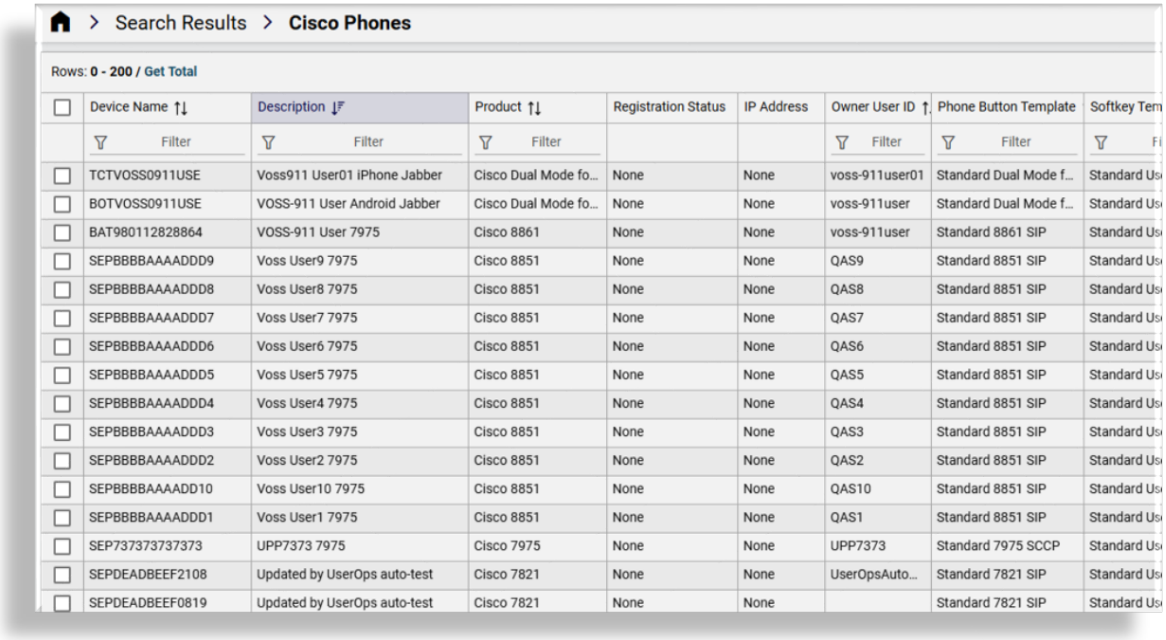
View phones

This procedure displays existing phones.

1. Log in to the Admin portal as a Provider, Customer, or Site admin.

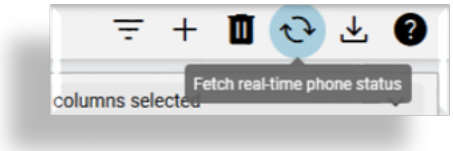
   Note: Only a subset of fields are available to Site admins.

2. Go to the **Cisco Phones** list view.
4. View existing phones.



Device Name	Description	Product	Registration Status	IP Address	Owner User ID	Phone Button Template	Softkey Tem
TCTVOSS0911USE	Voss911 User01 iPhone Jabber	Cisco Dual Mode fo...	None	None	voss-911user01	Standard Dual Mode f...	Standard Us
BOTVOSS0911USE	VOSS-911 User Android Jabber	Cisco Dual Mode fo...	None	None	voss-911user	Standard Dual Mode f...	Standard Us
BAT980112828864	VOSS-911 User 7975	Cisco 8861	None	None	voss-911user	Standard 8861 SIP	Standard Us
SEPBBBBAAAADDD9	Voss User9 7975	Cisco 8851	None	None	QAS9	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD8	Voss User8 7975	Cisco 8851	None	None	QAS8	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD7	Voss User7 7975	Cisco 8851	None	None	QAS7	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD6	Voss User6 7975	Cisco 8851	None	None	QAS6	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD5	Voss User5 7975	Cisco 8851	None	None	QAS5	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD4	Voss User4 7975	Cisco 8851	None	None	QAS4	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD3	Voss User3 7975	Cisco 8851	None	None	QAS3	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD2	Voss User2 7975	Cisco 8851	None	None	QAS2	Standard 8851 SIP	Standard Us
SEPBBBBAAAADD10	Voss User10 7975	Cisco 8851	None	None	QAS10	Standard 8851 SIP	Standard Us
SEPBBBBAAAADDD1	Voss User1 7975	Cisco 8851	None	None	QAS1	Standard 8851 SIP	Standard Us
SEP737373737373	UPP7373 7975	Cisco 7975	None	None	UPP7373	Standard 7975 SCCP	Standard Us
SEPDEADBEEF2108	Updated by UserOps auto-test	Cisco 7821	None	None	UserOpsAuto...	Standard 7821 SIP	Standard Us
SEPDEADBEEF0819	Updated by UserOps auto-test	Cisco 7821	None	None		Standard 7821 SIP	Standard Us

Note: An administrator with the required access profile can click **Fetch real-time phone status** on the toolbar to fetch the Cisco UCM phone IP address and status *directly* from the Cisco UCM. Data is fetched in real-time and displays read-only values in the following columns:



- **Registration Status** column (for example, “None”, “UnRegistered with CUCM-11-5-IP2”, “Registered with CUCM-11-5-IP2”)
- **IP Address** column

Fetched data is not cached or stored in the database, and can’t be exported or filtered. Real-time data displays the latest data for the *current* list of phones on the Admin portal. Prior to fetching real-time status updates, existing column values display cached values from the RIS data collector (if enabled).

The **Activate Phone Status Service** setting is enabled by default and can be managed by system level administrators. See the Advanced Configuration Guide for details.

Copyright © 2025 VisionOSS Limited. All rights reserved.

If the **Registration Status** and **IP Address** columns are not visible at a hierarchy level, run the following command from the CLI:

```
voss migrate_summary_attributes device/cucm/Phone
```

Add a phone

This procedure adds a new Cisco phone via the **Cisco Phones** page.

Note: It is recommended that you use *Smart Add phone* to add standalone phones (not associated to any user) and use Quick User to add phones to users. See *Smart add phone* and *Cisco Quick User*.

Before you start

Before adding Cisco phones in Automate, add and configure the following items on Cisco UCM, and then import these items into Automate:

- Softkey templates (Softkey templates can be set up on Cisco UCM or in Automate)
- Phone button templates
- Service parameters and enterprise parameters for user services
- Custom SIP profiles
- Service profiles for Jabber
- Phone services

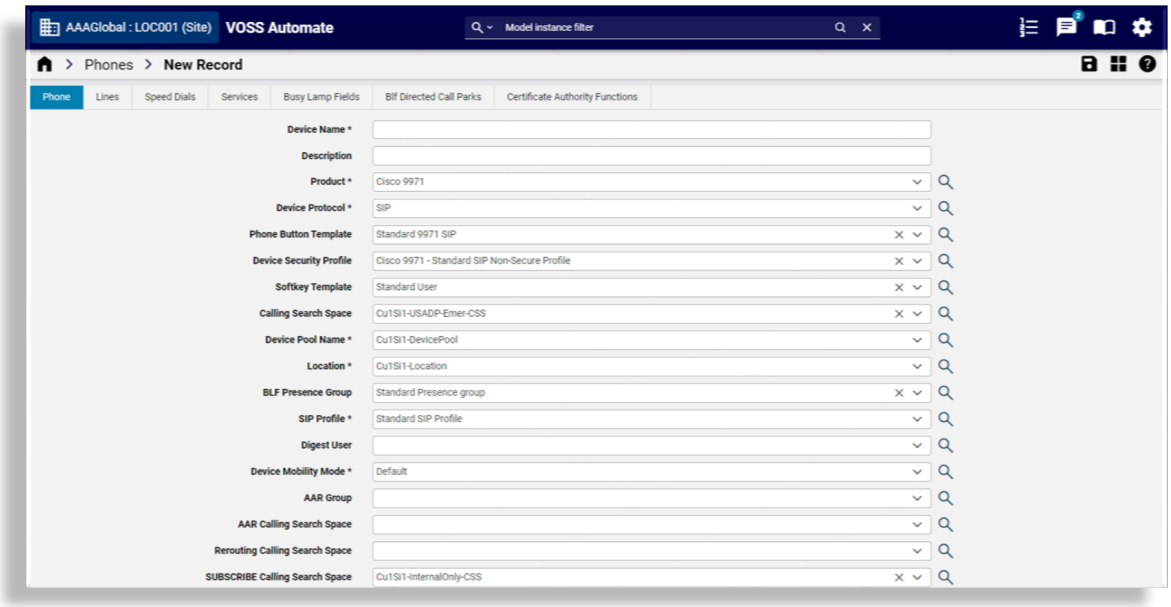
To add a phone (Cisco UCM users):

1. Log in to the Admin portal as a Provider, Customer, or Site admin.

   Note: Only a subset of fields are available to Site admins.

2. Go to the **Cisco Phones** list view.
3. Click the toolbar **Plus (+)** icon, then choose the hierarchy where you want to add the phone.
4. On the **Cisco Phones > New Record** page, fill out details for the phone you're adding:

Copyright © 2025 VisionOSS Limited. All rights reserved.



- On the **Phone** panel/tab:
  - Fill out the device name, including a prefix, for example, *SEP0C0011010003*, choose the product, for example, *Cisco 8865*, and (optionally), fill out a description.

    Note: If you don't see the phone or endpoint you want, you'll need to install a COP file for the endpoint you want, in Cisco UCM. Install the COP file only once for the Cisco UCM instance where the endpoint is added. In Automate you will need to import the phone button template from Cisco UCM.

    When adding a device name, add a prefix, such as SEP, before the mac address. For example, if the mac address is *000000000AB1*, the device name must be *SEP000000000AB1*.

    If the Global Setting **Prevent Duplicate MAC Addresses for Cisco Phones** is enabled for the current hierarchy, a check will also be carried out for duplicates in all clusters. See *Global settings*.

  - Choose a device protocol.

    Note: The phone type you're adding must support the protocol you wish to use. A default protocol can be defined in the site defaults (**Device Defaults** tab). Some phone types support multiple protocols (for example, Cisco 7960 with SCCP and SIP), and some phone types support only one protocol (for example, Cisco 9971 with only SIP). If the phone type you're adding does not support a selected protocol, the protocol defaults to the one set up in the site defaults. You can choose or update the protocol (if allowed by the phone type), when adding a phone, when adding a user, or when adding a phone to an existing user.

  - Choose a phone button template for automatic configuration of settings, and a device pool name.
  - If this is a standalone phone, leave **Owner User ID** blank, else, choose a user to associate with this phone.

Copyright © 2025 VisionOSS Limited. All rights reserved.

> **Note:** If you're adding the phone at a site, the user (Owner User ID) may exist at a higher level in the hierarchy, such as customer level.

- In the **Lines** panel, click the Plus (+) icon to add a line, then configure line settings:
  - Choose a line template.
  - Choose an inventory filter. Find out more about number inventory filters at *Manage number filters*.
  - Choose a directory number (mandatory).

    > **Note:** An inventory number filter can be applied to this field to limit the directory numbers, including a filter that will only show numbers reserved for or belonging to a user you're working with. You may only see numbers reserved for or belonging to this user. See *Reserve numbers for a user*. To find out more about enabling or managing number inventory filters, see *Manage number filters*.

  - Specify a label for the line.
  - Specify a display.

5. Click **Save** to add the phone.

Related topics

- *Manage number filters*

Update a phone

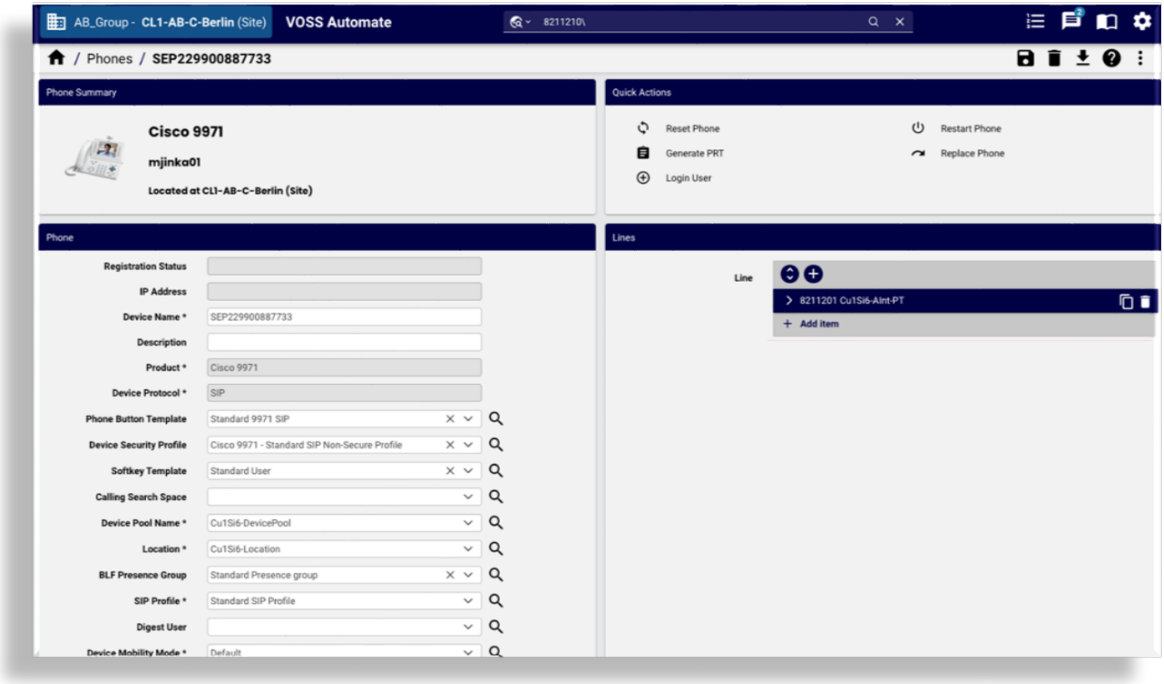
This procedure updates an existing phone.

1. Log in to the Admin portal as a Provider, Customer, or Site admin.

   > **Note:** Only a subset of fields are available to Site admins.

2. Go to the **Cisco Phones** summary list view.
3. Click on the phone you wish to update to open its settings.

Copyright © 2025 VisionOSS Limited. All rights reserved.



4. View existing settings, and update as required. Note the following:
   - Displayed fields are based on the device type and device protocol (for example, SIP or SCCP).
   - Supported features available for each phone type are retrieved from the related Cisco UCM.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Quick Actions	Provides quick access to one or more predefined actions, such as restart, reset, or replace phone, or generate PRT. You can add also access some of these actions via the overflow toolbar menu (vertical ellipsis).
Phone	• Default values are applied for some fields (such as Device Protocol, BAT Phone Template, and Device Security Profile), based on the device (product) type. • **Vendor Config** settings are related to the phone type. • To override the default **Phone Button Template**, either choose another template, or enter a custom value. The new value is applied on the UCM if it allows that phone type. If you don't see a template that you're looking for in the drop-down (for example, for **Phone Button Template**, **Device Security Profile** or **SIP Profile**), edit the template on UCM, and then sync the template into Automate to have it appear in the drop-down. • It is possible to choose an Owner User ID at a higher hierarchy, for example, if the phone is at the site, you can choose an Owner User ID at the customer level and save your changes.
Lines	This panel displays all lines associated with the device and allows you to associate additional lines. When adding a line, the system checks that a line exists, and if it doesn't exist, the line is added. If Number Inventory is enabled, you can select a number from the list of available numbers. 1. At **Pattern**, select a directory number. Line patterns are filtered based on the partition type. 2. At **Monitoring CSS Name**, set the Monitoring Calling Search Space as the CSS that is configured in the Calling Search Space field on the **Lines** page. 3. At the **Busy Trigger** field, enter a busy trigger value, for example, **1**. 4. At the **Max Num Calls** field, enter the maximum number of calls value, for example, **2**.
Speed Dials	On this panel you can configure speed dials for the device. Available speed dials depend on the device's **Phone Button Template**. The order in which Speed Dial entries are added matches the slots that are available on Cisco UCM.
Services	On this panel you can set up IP Phone services. Once you choose the IP phone service, the system retrieves the URL and a custom parameter (if any, for example, ext1 and ext2) from device/Cisco UCM/IpPhoneService, and populates the URL field.
Busy Lamp Fields	In this panel you can configure busy lamps for the device. Available busy lamp fields depend on the device's **Phone Button Template**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Blf Directed Call Parks	This panel allows you to configure Busy Lamp Field directed call parks for the device. Available BLF-directed call parks depend on the device's **Phone Button Template**. Create BLF-directed call parks via **Directed Call Parks** on Cisco UCM before configuring them in this panel. The available BLF-directed call parks match those created for each specific Route Partition Name.
Dual Mode Settings	These settings display only for phones that support Dual Mode, and allow you to configure mobile identity and remote destinations.
Certificate Authority Functions	The settings on this panel are only relevant to a Dual Mode Phone, Spark Remote Device, or CTI Remote Device, and allows you to enter enter the relevant Mobile Identity and Remote Destination (or CTI Remote Destination) parameters for the device. These parameters include Name, Destination Number, Owner User ID, Dual Mode Device Name (or CTI Remote Device), and Answer Too Soon and Too Late Timers. The date-time value must be added manually as: `CCYY:MM:DD:HH:MM`

Note:

- For more information about Certificate Authority Functions, see *Certificate authority functions*.
- When updating the phone, the phone and user remote destination are updated.
- Where a phone activation code has expired and needs to be generated, the user's dummy phone must be deleted and a new dummy phone re-added, following activation steps: *Phone onboarding with Cisco activation codes*.
- For phones supporting the activation codes and the MRA feature will have the `allowMraMode` and `mraServiceDomain` fields available provided a sync has been run that updates the phone types in Automate with the supported feature set.
- If you need to enable Extend and Connect in Automate, perform these steps while creating a CTI Remote Device:
  1. Fill out the **Device Name**. For example, CTIRD<USERID>.
  2. Choose the product as **CTI Remote Device**.
  3. Choose the **Owner User ID** from the drop-down.
  4. Choose the **SUBSCRIBE Calling Search Space** name from the drop-down.
  5. Choose the **Rerouting Calling Search Space** name from the drop-down.

5. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete a phone

This procedure deletes one or more Cisco phones or phone settings.

1. Log in as a Customer or Site administrator.

   Note: If you're logged in as the Customer admin for a specific site, all fields described in this procedure are available to you. If you're logged in as the Site admin, only a subset of fields are available to you.

2. Choose a site.
3. Go to **Cisco Phones**.
4. Choose one of the following methods to delete phones or phone settings:
   - Select the checkbox for the phone you want to delete (one or more), then confirm the deletion.
   - Open the settings for a specific phone and remove its settings. Save your changes.

   Note: Deleting a phone removes the remote destination first so that the Automate cache remains in sync with Cisco UCM.

   Lines are not affected when a phone is deleted.

Certificate authority functions

The table provides details on the available fields for Certificate Authority Functions when adding or configuring phones.

Title	Description
Certificate Status	Shows the current security certificate status of the phone. The field is read-only.
Certificate Operation *	From the drop-down list box, choose one of the following options: No Pending Operation: Displays when no certificate operation is occurring (default setting). Install/Upgrade: Installs a new or upgrades an existing locally significant certificate in the phone. Delete: Deletes the locally significant certificate that exists in the phone. Troubleshoot: Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the Cisco Unified Communications Manager Security Guide. Default: No Pending Operation

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Description
Authentication Mode	Defines the the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • By Authentication String: Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when you fill out the CAPF authentication string on the phone. • By Null String: Installs, upgrades, deletes, or troubleshoots a locally locally significant certificate without user intervention. This option provides no security. Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC): Installs or upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless of whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before choosing this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC): Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless of whether a LSC exists in the in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. The CAPF settings configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window. Default: By Null String

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Description
Authentication String	If you chose the *By Authentication String* option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.
Authentication Server	Enter the URL that the phone uses to validate requests that are made to the phone web server. If you do not provide an authentication URL, the advanced features on the Cisco Unified IP Phone that require authentication will not function. By default, this URL accesses a UCM Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting.
Key Order	`keyOrder` can be updated only if `certificateOperation` field is Install/Upgrade,Delete or Troubleshoot. Default: RSA Only
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. Note The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window. Default: 1024
EC Key Size (Bits)	`ecKeySize` can be updated only if `certificateOperation` field is Install/Upgrade,Delete or Troubleshoot. Default: 384
Operation Completes By	The completion deadline for the operation (CCYY:MM:DD:HH:MM)

View and update phone vendor config settings

Vendor Config settings display on the **Phone** tab/panel if the Field Display Policy (FDP) allows it. The available settings depend on the phone type.

Note: Where admin password credentials may be required in any phone type's vendor config settings, these are masked.

---

1. In the Admin portal, go to the **Cisco Phones** list view.
2. Click on a phone to open its settings.
3. On the **Phones** tab/panel locate and then click on **Vendor Config** to open the configuration screen:

   Enable or disable settings, as required. Ensure you're setting values correctly for Bulk Loaders, the API, or in custom Configuration Templates, where values must be defined as key-value pairs:

   - On Cisco UCM, in some cases the value `0` is "Enabled" and in other cases `0` is "Disabled".
   - It is recommended that settings on Cisco UCM are configured manually on a sample phone to the value you want, before exporting the phone. Then use the example settings as the basis for your

Copyright © 2025 VisionOSS Limited. All rights reserved.

bulk loaders, API, or custom CFTs.

- The required value may change depending on the setting being applied, for example:

  To *enable* the "Web Access" for a phone, configure the following:

  - Key: `webAccess`
  - Value: `0`

  To *disable* "Web Access" for a phone, configure the following:

  - Key: `webAccess`
  - Value: `1`

  To *enable* "Settings Access", configure the following:

  - Key: `settingsAccess`
  - Value: `1`

  To *disable* "Settings Access", configure the following:

  - Key: `settingsAccess`
  - Value: `0`

Generate Problem Reporting Tool (PRT)

Individual phones can have the Problem Reporting Tool (PRT) triggered to generate PRT log collection on the phone and upload it to the log server configured on the Unified CM in the "Customer support upload URL" parameter at the Enterprise, Profile, or Device level.

1. Select the phone from the **Cisco Phones** list view.
2. Click the **Generate Prt Phone** action to generate PRT log collection.

Sync in Cisco phone updates from Cisco UCM

After you make changes to any phone model specific data in Cisco UCM, for example by loading a new BAT file, editing phone button templates, security profiles, and so on, then in order to utilize that data in Automate, you need to do a sync of the UCM.

Include the following models in the data sync (depending on what you changed):

Models	Notes
`device/cucm/PhoneType`	Should always be included. This includes the expansion modules as well as the phone types.
`device/cucm/PhoneButtonTemplate`	Include if button templates were changed.
`device/cucm/PhoneSecurityProfile`	Include if phone security profiles were modified

Perform a full sync or full import to make the changes available in Automate. However, between full syncs, it is best practice to create a sync setup with a model type list that includes the above model types. This

Copyright © 2025 VisionOSS Limited. All rights reserved.

allows you to run an ad-hoc sync with a very limited scope as needed - if changes are made in the UCM that require a sync.

If adding new phone types to the system, you may also need to edit your device groups and entitlement profiles (if used) to have them show as options to the correct users.

Phone onboarding with Cisco activation codes

Automate supports the Cisco UCM capability for device onboarding using activation codes. This provides a simplified method to register a new phone in the system. This is supported from Cisco UCM version 12.5 and later.

This feature allows administrators to create phones without MAC addresses and then share automatically generated activation codes with end users via Self-service or email. The end user can then enter the activation code into the physical device to initiate auto registration.

Once the phone is activated and registered, the correct phone association takes place in Automate.

For more information on the detailed functionality of the Cisco Activation Code Device Onboarding capability, including supported devices, refer to the Cisco documentation.

The setup of the feature has been incorporated into our various user/phone management capabilities:

- Phones
- Users
- Quick Add User
- Smart Add Phone

Note:

- The selected phone type must also be included in the user's entitlement profile.
- When a device is added which supports Activation Codes and the option is chosen, Cisco UCM may be slow to respond with relevant Activation Code. In this instance, Automate will retry fetching the activation code 3 times with a 2 second wait in between. Once the activation code has been received, the retries will stop.

Phone setup and onboarding workflow

The high-level setup steps in Automate for phone onboarding with Cisco activation codes are as follows:

1. Initial setup - enabling phone types for activation code.
2. Per user/device - setup of the phone details and generation of the activation code.
3. Provide the activation code to the user for use to onboard the device.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Complete the initial setup and enable the phone type(s) for activation code use

1. Login as Customer administrator or higher.
2. Navigate to the hierarchy level of the cluster(s) you want to enable.
3. Enable activation code based registration for a target phone type:
   a. Go to **Device Defaults**.
   b. Click the **Model**, e.g. Cisco 7821 on which you want to enable the phone registration activation code feature. Note the device column in the list view to ensure it is the device type on the right UCM cluster.
   c. Select the **Prefer Act Code Over Auto Reg** checkbox.
   d. Click **Save**.

Complete the per user/device setup to prepare the phone for onboarding:

1. Once enabled, you can add the phone, using any of the prescribed user Management methods (see above), making sure to select the **Use Activation Code Onboarding** checkbox. This will remove the device name as a BATXXXXXXXXXXXX device name will be generated when adding the phone.
2. Once the phone is successfully added, an activation code is generated and displayed along with the code expiry time on the relevant **Cisco Phones** settings page.

   Note: The phone activation code must be used to register the phone before the specified expiry date.

3. The activation code is available in the end user's Self-service if the device was associated to a user. Alternatively email the activation code to the end user.
4. The end user registers the phone by entering the activation code into the physical device.
5. To see the list of phones that have been setup for activation codes but not yet activated, you can filter the phones list view for device names starting with, BAT, as once they register they have the appropriate device name prefix (e.g. SEP).

Enhanced INI filtering

If *Enhanced INI Filtering* is enabled, administrators have access to the **Inventory Filter** dropdown list menu for lines on the following forms:

- **Phones**
- **Quick Add Subscriber**
- **Subscribers**

The filter would typically be used to show a filtered, shorter dropdown list of directory numbers.

Note: If the Internal Number Inventory (INI) feature is not enabled, Enhanced INI Filtering will not be applied and all the list of numbers are obtained from the device.

The following options are available in the **Inventory Filter** list:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Default**

  This filter - enabled by default - corresponds with the standard filter of Directory Numbers:

  - used and unused INI numbers *above and at the current hierarchy*.
  - used and unused Associated E164 numbers *above and at the current hierarchy*.
- **Show Unused Numbers with Associated E164's (Site Only)**
  - Shows unused INI numbers with Associated E164 numbers *at the current site only*.
  - Format is: `<INI number> <E164 number>`. Example: `99003 \+279990003`.
- **Show Unused Numbers with Associated E164's**
  - Shows unused INI numbers with Associated E164 numbers *above and at the current hierarchy*.
  - Format is: `<INI number> <E164 number>`. Example: `99003 \+279990003`.
- **Show Used Numbers (Site Only)**
  - Shows used numbers *at the current site only*.
  - Format is: `<INI number> (used)` or `<INI number> (used) <E164 number>`. Example: `99000 (used) \+279990000`.
- **Show Used Numbers**
  - Shows used numbers *above and at the current hierarchy*.
  - Format is: `<INI number> (used)` or `<INI number> (used) <E164 number>`. Example: `99000 (used) \+279990000`.
- **Show Numbers belonging to this Subscriber**
  - The option shows results if a subscriber is selected on the **Quick Add Subscriber** or **Subscriber** form, or is associated with the selected phone on the **Phones** form.
  - Format is: `<INI number> (used)` or `<INI number> (used) <E164 number>`. Example: `99000 (used) \+279990000`.

Configure phone services

Tip: *Use the Action search to navigate Automate*

Overview

This procedure sets up and enables phone services feature.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Pre-requisites

- The phone-based registration web service must be installed before you can set up phone services. Refer to *Install Phone-based Registration (PBR) Web Service*.

Phone services setup workflow

This procedure involves the following steps:

1. *Step 1: Configure a local admin for use by phone services*
2. *Step 2: Enable the PBR instance for CUCM clusters*
3. *Step 3: Create CUCM IP phone service for phones to access phones services*
4. *Step 4: Verify connectivity between VOSS Automate and phones*

Related Topics

- *Introduction to Phone Services*
- *Manage Phone Services*
- *Install Phone-based Registration (PBR) Web Service*

Step 1: Configure a local admin for use by phone services

Configure a local admin user in the system, at the Provider level, to be used by the phone services feature to initiate transactions in VOSS Automate.

It is recommended that this user is used only for phone services, and is not used to log in to the system or for other admin purposes.

The permissions required for this user are included in the access profile **RS_PBR_RestrictedAPIAccess**, which is on the system by default.

You may need to create a role with the relevant settings to assign to the user being created. This user and password is used in the next step.

Note: Consider a credential policy for this user that does not expire the password to avoid needing to change the password and update the various configurations setup in Step 2 for the new password.

Step 2: Enable the PBR instance for CUCM clusters

Note: If you've already configured phone-based registration, some of these steps may already be complete. To access configuration parameters, go to the **PBR Config** page.

- Set up the required PBR configuration instances in Automate.

  You may be required to add the correct model (*data/RS_PBR_Config*) to the access profile and menu layouts for the roles that require access to enable/configure phone services.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- An instance of the model at the Provider level is required (with the CUCM IP value blank if you don't have a CUCM at the Provider level).

  This instance enables the basic phone services capability on the system.
- An instance of the model at the hierarchy level of the CUCM cluster that requires the feature to be supported.

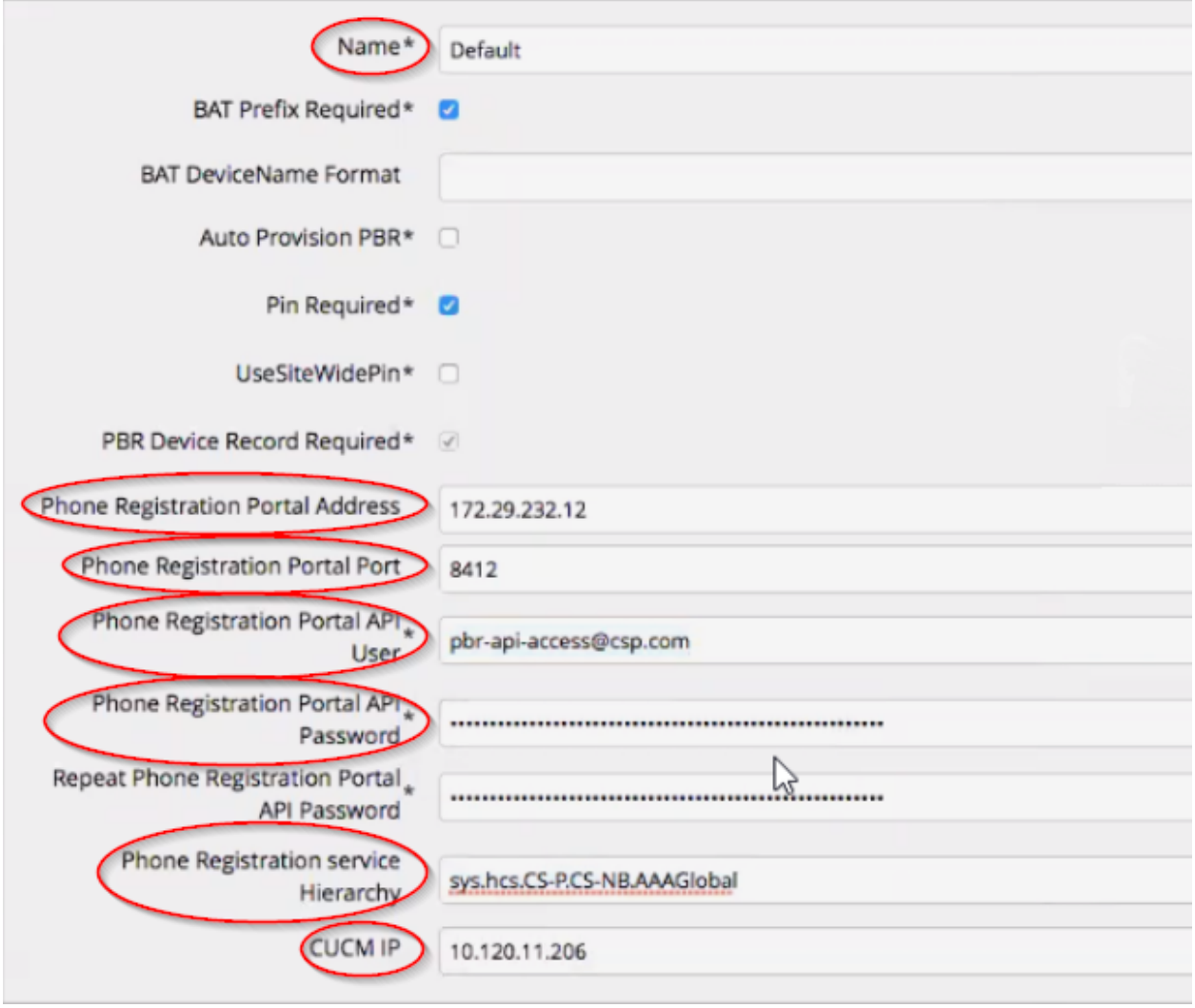
Important: In the case of a multi-cluster setup, multiple instances may be required at the same hierarchy (one instance per CUCM).

The table lists mandatory fields for phone services:

Note: Where an image showing values is included in the documentation for this step, values are examples only. Besides these required values, all other fields are optional for phone services.

Setting	Description
Name	Unique name for this instance.
Phone Registration Portal Address	The IP address of the VOSS Automate Proxy that the phones will communicate with. This needs to be the address visible to the phones (could be across a NAT boundary).
Phone Registration Portal Port	This must be port `8412`.
Phone Registration Portal API User	This user ID is hardcoded for phone services: `pbr-api-access@[providername].com`
Phone Registration Portal API Password	The password for the local admin user you set up.
Phone Registration Service Hierarchy	This field is populated based on the hierarchy breadcrumb when you click the Add button. If it is incorrect, return to the list view and change the breadcrumb to the correct hierarchy: • If the config record is defined at Provider level, then this must be the Provider hierarchy, for example `sys.hcs.CS-P`. • If the config record is defined at the Customer level, then this must be the Customer hierarchy, for example `sys.hcs.CS-P.CS-NB.AAAGlobal`.
CUCM IP	This should be the IP address of the Unified CM Publisher that is accessible to VOSS Automate using HTTP SOAP requests. Optional if this is the initial Provider level record and there is not a Unified CM at that level.

Copyright © 2025 VisionOSS Limited. All rights reserved.



To simplify the setup of multiple instances of this record in a system with two or more clusters, include a configuration template in your menu layout with values for the shared settings (for example, portal address, portal port, API user, and API password). This will pre-populate the form with these values.

Note: Depending on your network setup, in the event of a proxy failure (for example, a data center disaster recovery failover scenario), the phone services hostname/IP address may need to be changed to the proxy in the disaster recovery data center.

Important:

- You must restart the services once you've saved the above configuration in VOSS Automate. To restart services, run the following CLI command on the primary node (if not already done):

  ```
  cluster run application app start phone-based-registration
  ```

  If you're on-boarding and configuring several customers at the same time, the command needs to be run only once, after all configuration is complete.

  Subsequent single customer onboarding will however require that the command is re-run.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Ensure you set the **Services Provisioning** value (under **Enterprise Parameters Configuration - Parameter Name** on the associated CUCM) to **Both**.

Step 3: Create CUCM IP phone service for phones to access phones services

The table describes two methods for setting up the service that controls which devices the service appears on:

Method	Description
Regular service	The service must be subscribed individually to specific phones on which the service must appear: **Enable** checkbox = Selected
Enterprise-wide subscription	The service will appear on all phones in the system: **Enterprise Subscription** checkbox = Selected

Typically, an *enterprise-wide subscription* is simpler as it means not managing the service subscriptions by device.

For more granular control, manage it as a *regular service*, and subscribe as needed.

The IP Phone Service provides the details of the VOSS Automate service, which is how the IP Phones access the feature. The service needs to be set up into the Unified CM for the phones to use it.

Go to the **Phone Services** page.

The table describes settings for the service:

Note: The service can be configured via Automate if the IP Phone Services device model is included in your menus (or via bulk loader). Otherwise it can be configured directly in the CUCM.

Setting	Description
Service Name	VOSS Automate Phone Services (or preferred name that will appear in the Phone's services menu)
Service Description	VOSS Automate Phone Services
Service Category	XML Service
Service Type	Standard IP Phone Service
Service Vendor	VOSS
ServiceURL	Set the URL as described in *ServiceURL Format*, below.

Copyright © 2025 VisionOSS Limited. All rights reserved.

ServiceURL Format

This section describes the format to be used for the ServiceURL.

This is an example ServiceURL only, showing the corporate directory format set to “UN-LN-FN” and the corporate directory scope set to “Customer”. See parameters below, and replace the value following the equals sign (=) with the values you require.

```
http://<VOSS Automate-Address>:8412/phoneservices/<UnifiedCMAddress>/menu
  ?name=#DEVICENAME#
  &corp_dir=true
  &corp_dir_format=UN-LN-FN
  &corp_dir_scope=Customer
  &refresh=true
```

The table describes the parameters in the ServiceURL:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Parameter	Description
`<VOSS Automate-Address>`	The address the phones will use to reach VOSS Automate (typically the primary proxy server - consider any NAT setup in your network). You may consider using/validating a DNS SRV address here for redundancy in the event of a proxy failure.
`<UnifiedCMAddress>`	The address of Unified CM as known to VOSS Automate - consider any NAT setup in your network.
`corp_dir`	Corporate directory. Enabled (true) by default. To disable it, set "corp_dir=false" in the URL. When enabled, the "Corp Dir" menu item is added to the list of services. Corporate directory shows the user with the number of the associated device at the selected hierarchy or lower (see `corp_dir_scope`), and displays a maximum of 50 numbers only. Users are filtered and formatted according to the `corp_dir_format` parameter. Note that the corporate directory excludes "end user" type users who have been marked "Exclude from Directory", as well as "admin" type users.
`corp_dir_format`	Determines the format of the corporate directory. Options are: • "UN-LN-FN" = Username, Lastname, Firstname • "LN-FN-UN" = Lastname, Firstname, Username • "LN-FN" = Lastname, Firstname • "FN-LN" = Firstname, Lastname • "UN" = Username The default is "UN-LN-FN", i.e. Username, Lastname, Firstname
`corp_dir_scope`	Defines which users and numbers display in the corporate directory. Options are Provider, Reseller, Customer, IntermediateNode, Site, LinkedSite. (Default is "Customer") The phone or device profile directory is used as a starting point, and then the search looks up the hierarchy for the `corp_dir_scope` value. For example, if set to "Customer", the corporate directory displays users and numbers at the Customer hierarchy or lower. If the phone or device profile number making the call is located at a higher hierarchy than the `corp_dir_scope` value, then VOSS Automate ignores the `corp_dir_scope` value and includes all users and numbers at the hierarchy of the phone or device profile number.
`refresh`	Default is `refresh=false` Defines whether the service retrieves the latest settings from the underlying Unified CM when the service is used. For example, when opening the call forward option, refresh=true allows the service to retrieve the latest "call forward all setting" from the Unified CM. This is useful if the **CFWD ALL** softkey is also used on the phone. If the softkey is not being used and changes are only in VOSS Automate, then `refresh=false` (default) can be used to speed up the service.

Note: For more details around user types and corporate directory (`corp_dir`), refer to *Add admin user*

Important: When making any change to a value on the IP Phone Services URL, click **Update Subscriptions**

Copyright © 2025 VisionOSS Limited. All rights reserved.

on the **IP Phone Services Configuration** page on the CUCM for the update to take effect.

Step 4: Verify connectivity between VOSS Automate and phones

To enable the phone services feature, the network must support connectivity between the phones and the Automate Proxy server. This may be across a NAT boundary, or configuring a firewall to allow HTTP traffic on port `8412`.

For redundancy, consider the user/validating of a DNS SRV entry for the Automate proxy address. Otherwise, if IP address or static hostname is used, the service and rules may need updating in the event of a disaster recovery (DR) scenario or proxy failure.

Manage Phone Services

Overview

Once phone services is configured, users can manage the following phone services directly from the phone (if configured in VOSS Automate):

- Speed Dials
- Reset PIN (see *Introduction to Phone Services*)
- Call Forward - View Call Forward Settings, Set Call Fwd All(CFA), Set Call Fwd Busy(CFB), Set Call Forward NoAnswer(CFNA)
- Corporate Directory

Important: Phone services is only available for use once it is correctly configured in VOSS Automate as well as in the associated Cisco Unified Communications Manager (CUCM). See *Configure phone services*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Introduction to Phone Services*
- *Configure phone services*

Manage Phone Services from the Telephone User Interface (TUI)

This procedure adds, edits, and deletes a service directly from the Telephone User Interface (TUI).

Note: The services all work in a similar way. These steps describe an example for speed dial.

1. Select **Services > Speed Dial**.
2. Click **Manage**.
3. Click **Add**, **Edit** or **Delete** and follow the prompts.
4. Click **Submit** to initiate the transaction (only relevant to **Add** and **Edit**).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add phone-based registration menus and access profile

Tip: *Use the Action search to navigate Automate*

Overview

The Phone Based Registration (PBR) menus must be added to the Automate menu layouts for Provider and Customer administrators that require access to the feature.

Note: The simplest way to configure the menu layouts and access profiles for PBR is to export the existing menu layouts and access profiles for the appropriate roles, and submit to Automate's GS team to create a customized version that includes current modifications.

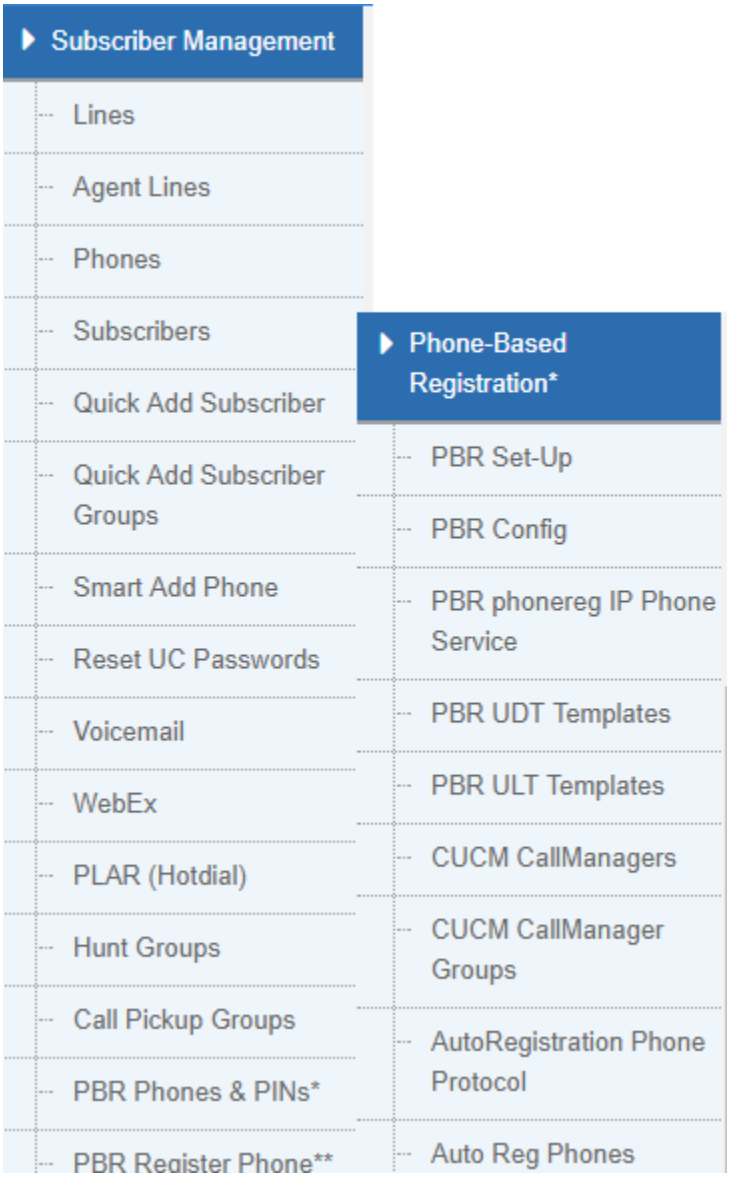
Related topics

- *Introduction to Phone-Based Registration (PBR)*

PBR menu layout and access profiles

The image shows a sample menu layout for PBR.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Add PBR menus to services

The table describes the Phone-Based Registration menus to add under **Services**:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Menu to add	Description
PBR Set-Up	• Title: PBR Set-Up • Type: view/RS_SetupReg_VIEW • Display As Form
PBR Config	• Title: PBR Config • Type: data/RS_PBR_Config • Display as list
PBR phonereg IP Phone Service	• Title: PBR phonereg IP Phone Service • Type: device/cucm/IpPhoneServices
PBR UDT Templates	• Title: PBR UDT Templates • Type: device/cucm/UniversalDeviceTemplate
PBR ULT Templates	• Title: PBR ULT Templates • Type device/cucm/UniversalLineTemplate
CUCM CallManagers	• Title: CUCM CallManagers • Type: device/cucm/CallManager
CUCM CallManager Groups	• Title: CUCM CallManager Groups • Type: device/cucm/CallManagerGroup
AutoRegistration Phone Protocol	• Title: AutoRegistration Phone Protocol • Type: device/cucm/ServiceParameter • Filter: AutoRegistrationPhoneProtocol – Filter By - Name – Filter Type - Equals – Filter String - AutoRegistrationPhoneProtocol – Ignore Case - false
Auto Reg Phones	• Title: Auto Reg Phones • Type: relation/SubscriberPhone • Filter: Auto – Filter By - BAT Phone Template – Filter Type - Equals – Filter String - Auto – Ignore Case - false

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add PBR menus to user management

The table describes the Phone-Based Registration menus to add under **User Management Advanced Functions**:

Menu to add	Description
PBR Phones & PINs	• Type: data/RS_PBR_Device • Title: PBR Phones & PINs
PBR Register Phone	• Title: PBR Register Phone • Type: view/RS_RegPhone_VIEW • Display As: Form

Add PBR Views to Access Profile for Provider Admin

Add the following PBR views to the access profile for Provider administrators (expose all operations):

- view/RS_RegPhone_VIEW
- view/RS_SetupReg_VIEW
- data/RS_PBR_Config
- data/RS_PBR_Device

Create Restricted API Role and Admin User

Overview

The Phone Based Registration (PBR) Web service initiates transactions on behalf of the end user that is registering a phone. This requires a limited role to provide the least privilege to this user.

Related Topics

- *Introduction to Phone-Based Registration (PBR)*

Create a Restricted API Access Role at the Provider Hierarchy

1. Browse to **Role Management**.
2. Click **Roles** and then **Add**.
3. Complete the form as follows:
   a. Name: PBR_RestrictedAPIAccess
   b. Menu Layout: RS_PBR_Restricted_Menu
   c. Access Profile: RS_PBR_RestrictedAPIAccess

Copyright © 2025 VisionOSS Limited. All rights reserved.

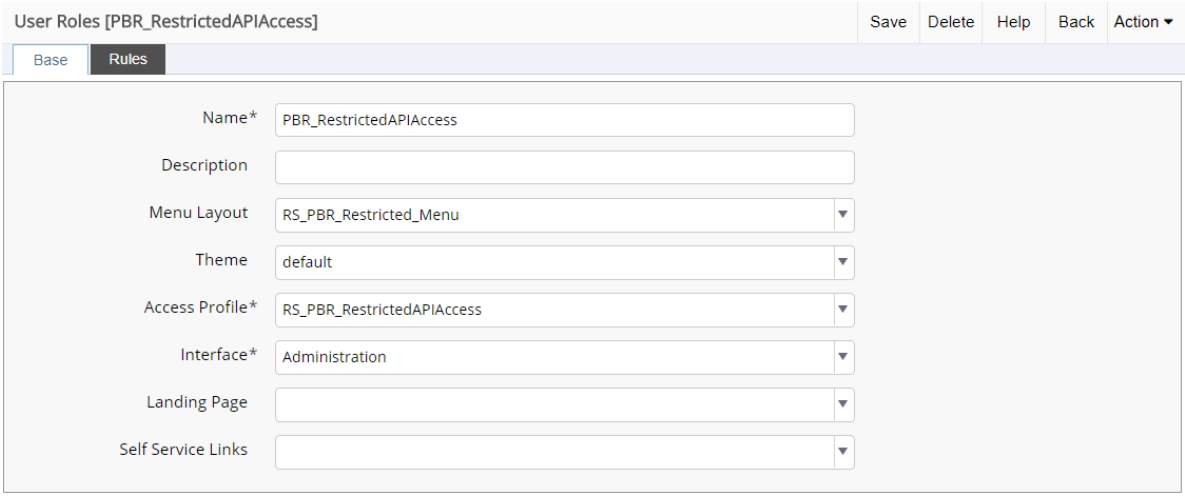


Figure 3: Sample Restricted API Access Role

Create a Restricted API Access User at the Provider Hierarchy

1. Browse to **Admin Users**.
2. Click **Add**.
3. Complete the form and select **PBR_RestrictedAPIAccess** for the role.
4. Note the email address and password.

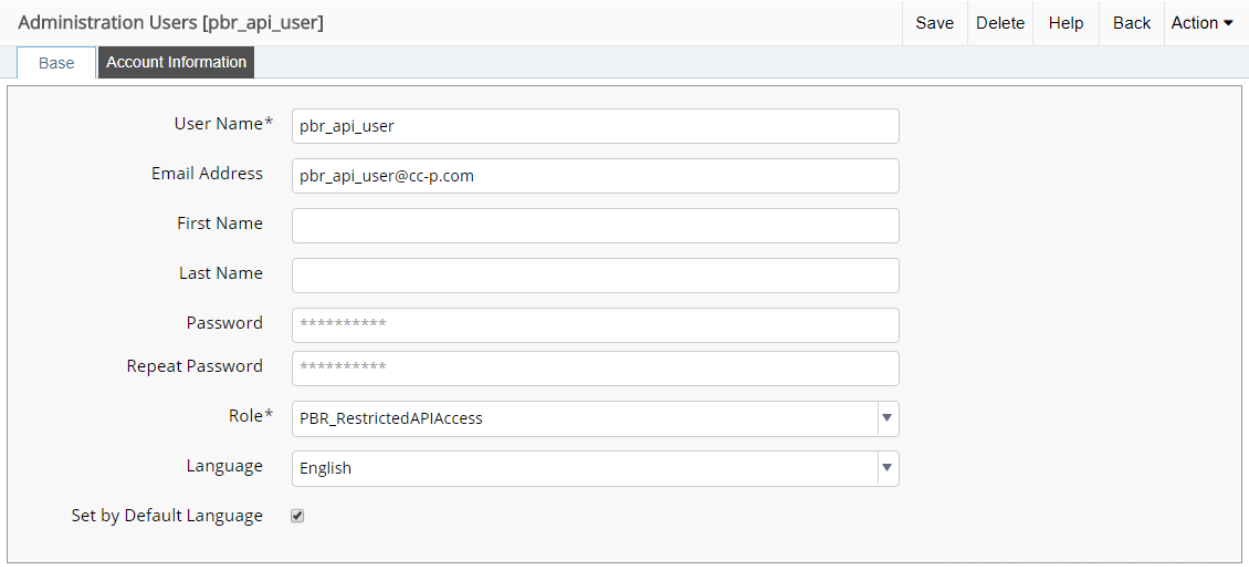


Figure 4: Sample Restricted API Access user

Copyright © 2025 VisionOSS Limited. All rights reserved.

Install Phone-based Registration (PBR) Web Service

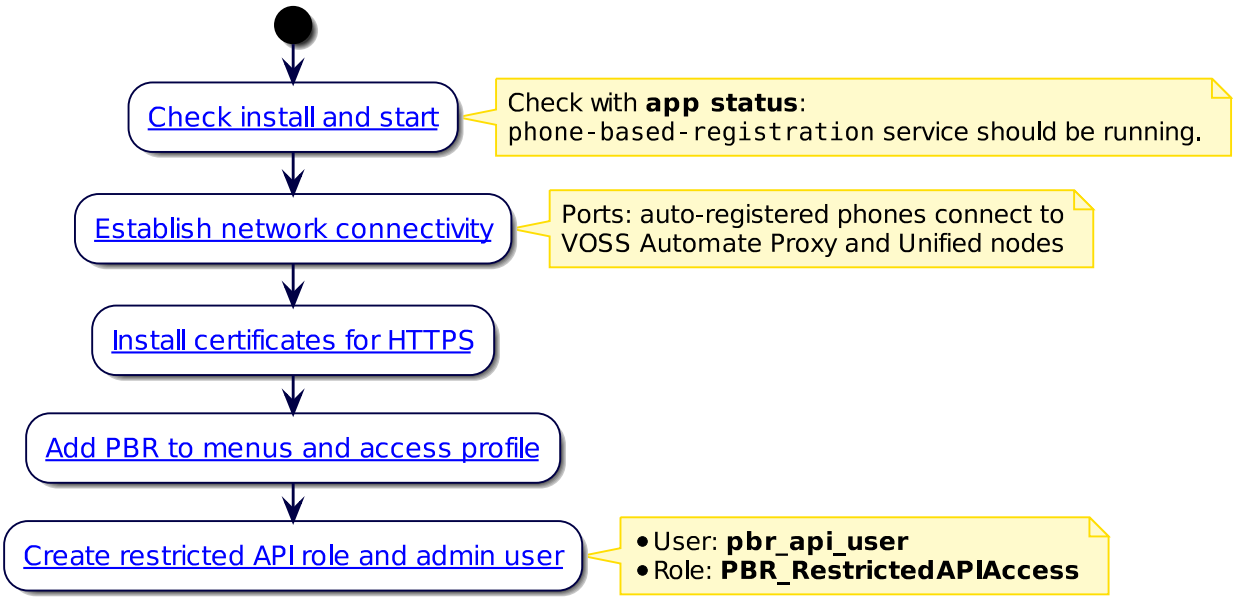
Overview

This section describes how to install phone-based registration (PBR) web service. Two options are described:

- Install PBR Web Service on a Cluster
- Install PBR Web Service on a Standalone System

Note: A full service restart is initiated on initial startup of the phone-based-registration (PBR) web service on each VOSS Automate unified node.

The flowchart sets out the high level steps for the install task:



Related Topics

- *Introduction to Phone-Based Registration (PBR)*
- *Configure Cisco UCM for AutoRegistration and PBR*
- *Add PBR config records*
- *Register a phone for phone-based provisioning*
- *Add phone-based registration menus and access profile*
- *Create Restricted API Role and Admin User*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Prepare for PBR Installation

Before starting installation of PBR, you will need to prepare the following:

- Network connectivity
- Certificates for HTTPS

Network connectivity for PBR

Phone-based registration (PBR) requires that auto-registered phones can connect to the VOSS Automate Proxy Nodes and Unified nodes.

Source Node	Destination Node	Transport	Port	Protocol
Phone	VOSS Automate Proxy Nodes	TCP	443	HTTPS
Phone	VOSS Automate Unified Nodes	TCP	8412	HTTP

Table 1: PBR network ports

Note that either HTTP or HTTPS is used on a per-customer basis. The choice depends on:

- Security requirements, for example, HTTPS only.
- Device support (some older devices do not support HTTPS – refer to the Cisco IP Phone security guide for list of devices that support secure communications.

Certificates for HTTPS

When using HTTPS for connectivity, the VOSS Automate certificate must be installed on CUCMs that make use of the PBR service.

The VOSS Automate Platform certificate must be copied from the VOSS Automate server and uploaded to CUCM.

1. Log in to VOSS Automate using Firefox or Chrome.
2. In the URL, click on the 'Lock' symbol and choose to view the certificate.
3. Find the 'Copy To' or 'Export' option, depending on your browser, and save the certificate file to your PC.
4. Log in to VOSS Automate using the "Cisco Unified OS Administration" login.
5. Browse to **Security > Certificate Management** and upload the certificate with "Certificate Purpose" set to 'tomcat-trust'.
6. Restart the Cisco service as per the instructions.

Note: The CUCM Hostname configured on CUCM under **System > Server** must be able to resolve via DNS otherwise the phones will not authenticate. If the Hostname does not resolve then change the hostname to the IP address instead.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Install PBR Web Service on a Cluster

1. On a *standard* topology, log in to *each node* serially and run `app install phone-based-registration`.

   On a *modular architecture* topology, log in to *each application node* serially and run `app install phone-based-registration`.

2. Verify that the PBR service is running: `app status`.

   The output should contain `v21.1`, for example:

```
phone-based-registration v21.1 (2021-01-11 07:46)
   |-nodeservice           running
```

Install PBR Web Service on a Standalone System

1. Log in to the unified node and run `app install phone-based-registration`.
2. Verify that PBR is running: `app status`.

   The output should contain `v21.1`, for example:

```
phone-based-registration v21.1 (2021-01-11 07:46)
   |-nodeservice           running
```

PBR Web Service - Web Weight Example Output

The PBR web service is assigned the same web weights as the `selfservice` and `voss-deviceapi` service. For example, when running **web weight list** from a web proxy, the output should be similar to the example below:

```
platform@VOSS-WP-1:~$ web weight list
Default service weights

  upstreamservers:
    phonebasedreg:
        phoneservices:
            192.168.100.10:443: 0
            192.168.100.3:443: 1
            192.168.100.4:443: 1
            192.168.100.5:443: 1
            192.168.100.6:443: 1
            192.168.100.9:443: 0
    voss-deviceapi:
        selfservice:
            192.168.100.10:443: 0
            192.168.100.3:443: 1
            192.168.100.4:443: 1
            192.168.100.5:443: 1
            192.168.100.6:443: 1
            192.168.100.9:443: 0
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
        voss-deviceapi:
            192.168.100.10:443: 0
            192.168.100.3:443: 1
            192.168.100.4:443: 1
            192.168.100.5:443: 1
            192.168.100.6:443: 1
            192.168.100.9:443: 0
```

Configure Cisco UCM for AutoRegistration and PBR

Tip: *Use the Action search to navigate Automate*

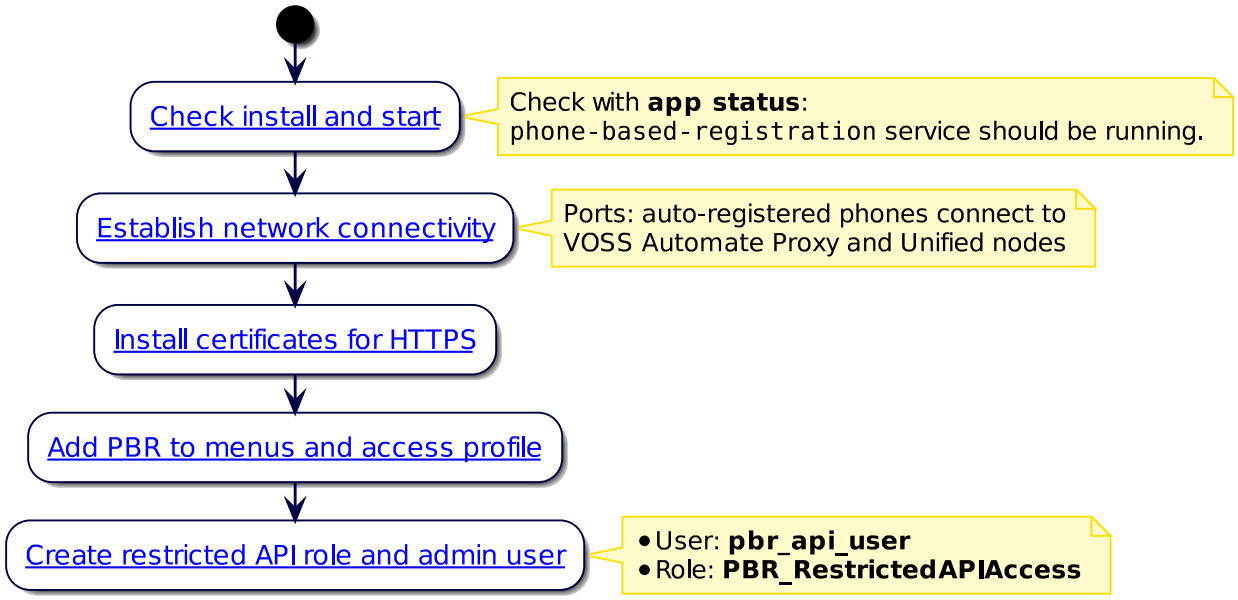
Overview

This section describes phone-based registration (PBR) setup.

Related Topics

- *Introduction to Phone-Based Registration (PBR)*

The flowchart provides the steps for this task:



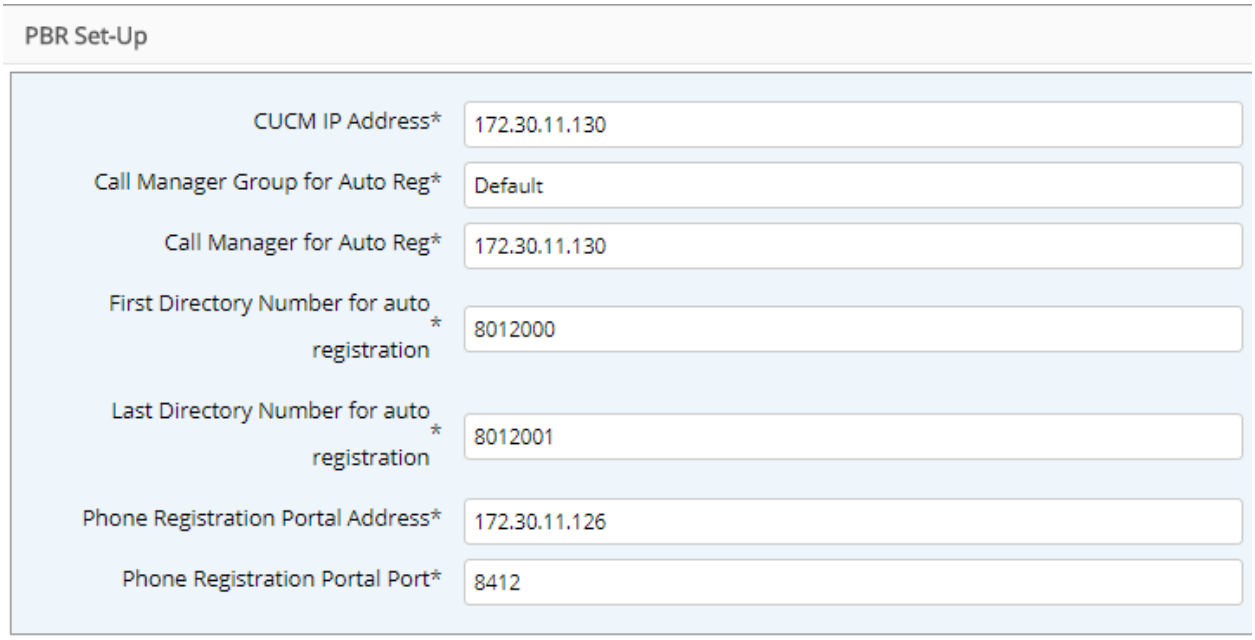
Copyright © 2025 VisionOSS Limited. All rights reserved.

Using PBR setup to configure a UCM

Use the **PBR Setup** menu to automates the configuration of Cisco Unified Communications Manager (UCM) for AutoRegistration and Phone Based Registration.

1. In the Automate Admin portal, go to **PBR Setup**.
2. Configure the following:

Setting	Description
CUCM IP Address	IP Address of the publisher for the UCM cluster.
Call Manager Group for Auto Reg	Name of UCM group for AutoReg.
Call Manager for Auto Reg	Name of the Call Manager for AutoReg (as specified under **CUCM Call Managers**).
First and Last Directory Number for Autoreg	A valid range of DNs to be used for Auto Registration.
PBR Portal Address	The IP Address of Automate cluster UN1
PBR Portal Port	8412



It is recommended that initial configuration of the UCM is performed using the PBR setup workflow described above. In cases where there is existing auto-registration config on the UCM, it may be required to do this manually.

Important: Set the **Services Provisioning** value (under **Enterprise Parameters Configuration - Parameter Name** on the associated UCM) to **Both**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configuration on Cisco UCM

Automate Phone Based Registration (PBR) requires the following functionality to be configured on UCMs that manage phones which may be registered by this feature:

1. Configure the UCM to allow AutoRegistration of new phones.

   This is standard auto registration config for UCM. The PBR Setup in Automate carries out this configuration.

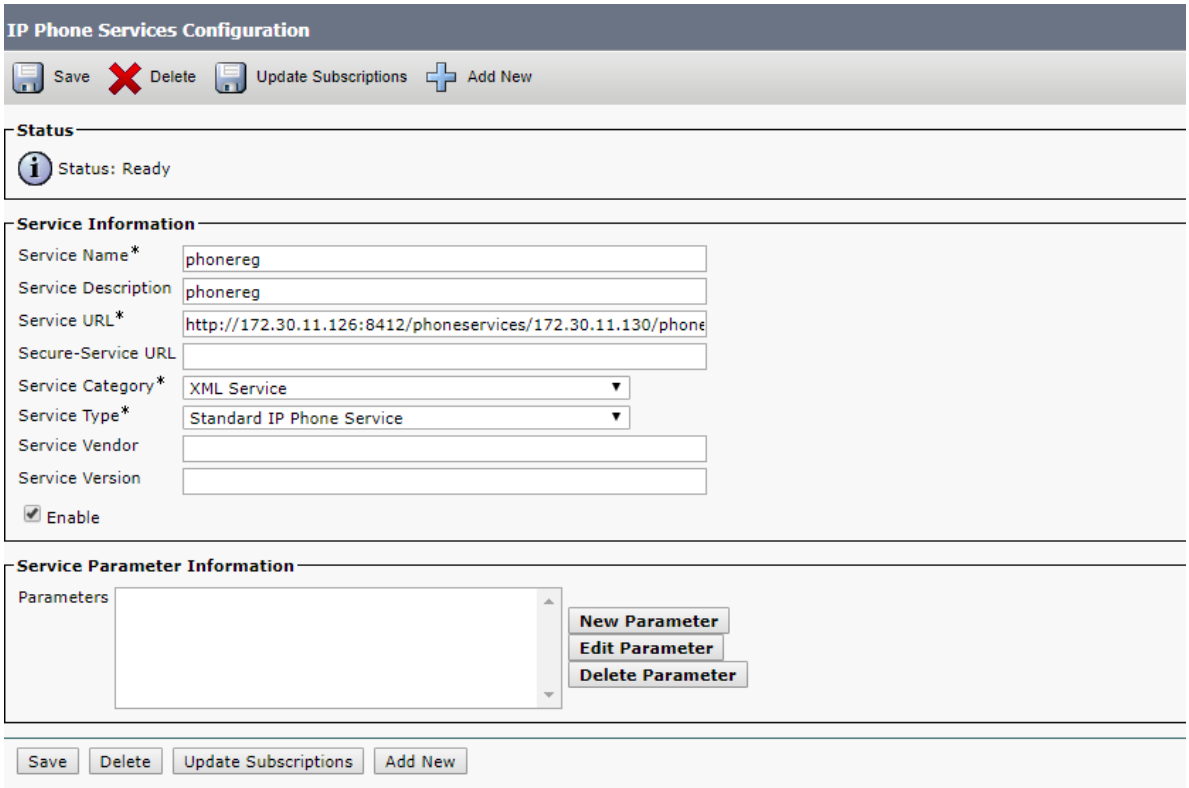
2. When a phone Auto Registers the `phonereg` phone service should be configured for the phone. This is achieved by specifying a Universal Device Template for Auto Reg that user to the `phonereg` phone service.

Screenshots of the relevant configuration on UCM are provided to assist with understanding how the service is implemented and as background for a Cisco expert that may need to fine tune the Unified CM config.

3. Setup the `phonereg` Phone Service:

   Browse to **Device > Device Settings > Phone Services**.

   172.30.11.126



   Service URL:

   Depending on whether HTTPS or HTTP is used the service URL may be different:

   - HTTP (Service URL):

```
http://{VOSS_IP}:{PBR_PORT}/phoneservices/{UnifiedCM_IP}/phonereg/menu?device=
↪#DEVICENAME#
```

   - HTTPS (Secure-Service URL):

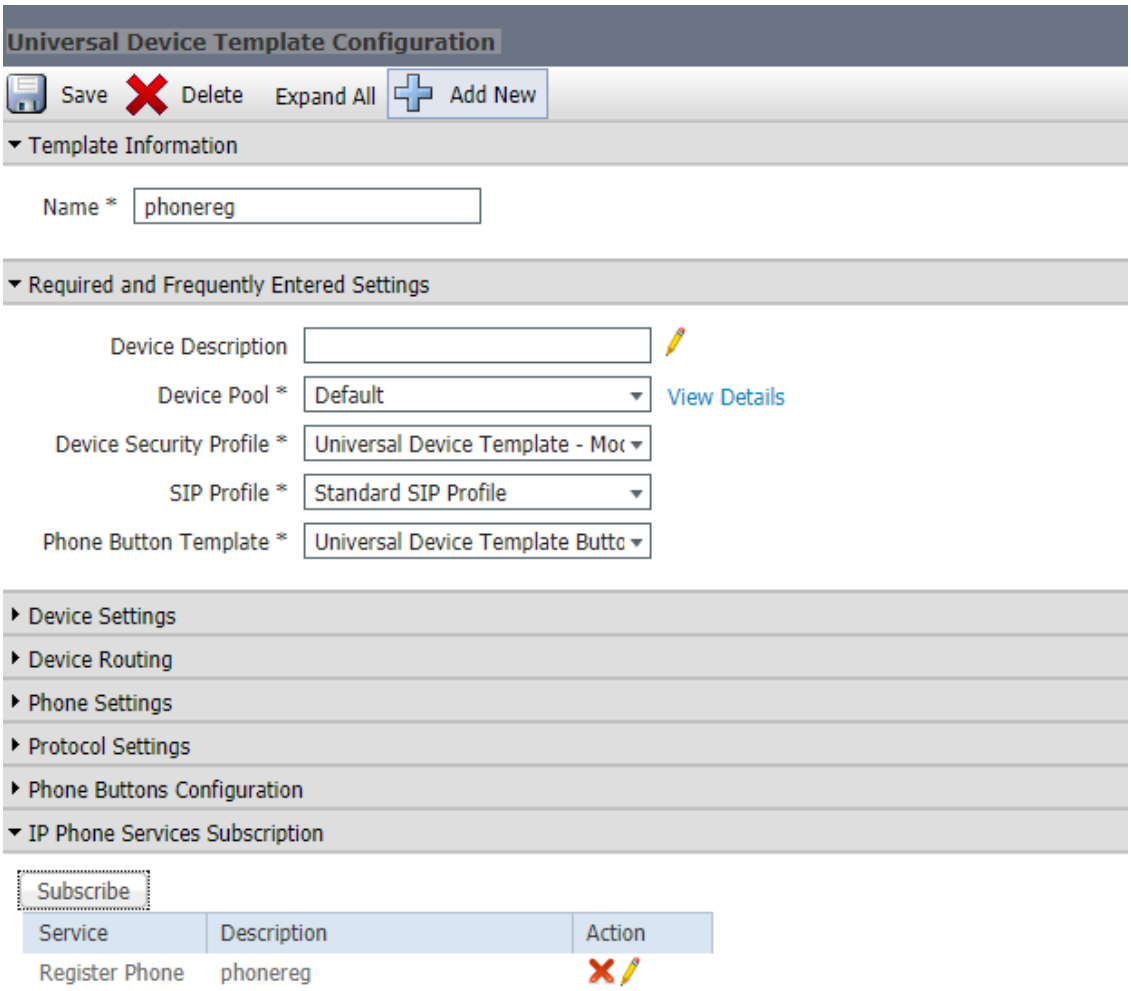
Copyright © 2025 VisionOSS Limited. All rights reserved.

```
https://{VOSS_IP}:443/phoneservices/{UnifiedCM_IP}/phonereg/menu?device=
↪#DEVICENAME#
```

For HTTPS-only, both Secure Services URL and Service URL must be populated with the HTTPS URL.

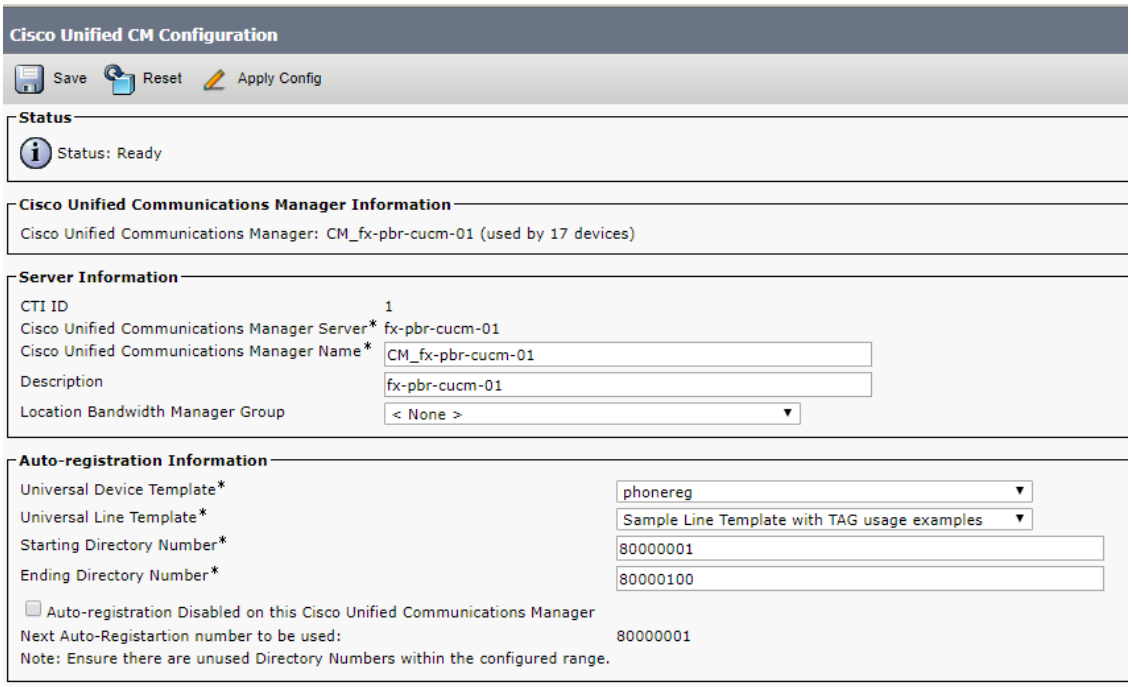
Note: The port must always be specified explicitly.

4. Configure `phonereg` Universal Device Template:
   a. Browse to **User Management > User/Phone Add > Universal Device** Template.
   b. Note the subscription to the `phonereg` Phone Service.



5. UCM for Auto Registration:
   a. Browse to **System > Cisco Unified CM**.
   b. Note the `phonereg` Universal device template.

Copyright © 2025 VisionOSS Limited. All rights reserved.



GDPR and Other Settings

Time periods

Tip: *Use the Action search to navigate Automate*

Overview

A time period specifies a time range that includes a start time and end time. Time periods also specify a repetition interval either as days of the week or a specified date on the yearly calendar. You define time periods and then associate the time periods with time schedules. A particular time period can be associated with multiple time schedules.

Note: Automate provides one **All the time** time period, which is a special, default time period that includes all days and hours, and cannot be deleted.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure time periods

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node where you wish to configure the new time period.
3. Go to **Time Periods**.
4. **Choose an option**:
   - **Add a new time period**? Click **Add**, then go to Step 5.
   - **Edit an existing time period**? Select the time period to be updated by clicking it in the list of time periods, then go to Step 6.
5. To add a new time period, if the **Network Device List** popup window appears, choose the NDL for the time period from the drop-down menu. The window appears when you are on a non-site hierarchy node. If you are at a site hierarchy node, the NDL associated with the site is automatically used.

   Note: The **Network Device List** drop-down menu displays only when adding a time period; it does not display when editing a time period.

6. When adding or editing a time period, add or update a unique name for the time period in the **Name** field. This field is mandatory. Enter a name in the **Time Period Name** field.

   Note: Time period name can comprise up to 50 alphanumeric characters. It can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

   Use concise and descriptive names for your time periods. The hours_or_days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, *office_M_to_F* identifies a time period for the business hours of an office from Monday to Friday.

7. Complete the other fields as appropriate.

Option	Description
Description	Enter a description for the time period.
Time of Day Start	From the drop-down list, choose the time when this time period starts. The available listed start times comprise 15-minute intervals throughout a 24-hour day. Default: No Office Hours Note: To start a time period at midnight, choose the 00:00 value.
Time of Day End	From the drop-down list, choose the time when this time period ends. The available listed end times comprise 15-minute intervals throughout a 24-hour day. Default: No Office Hours Note: To end a time period at midnight, choose the 24:00 value.

8. Choose a repetition period, and complete the required information:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: If choosing to repeat the time period by the week, the **Repeat Every Year** fields are read-only. If choosing to repeat the time period by the year, the **Repeat Every Week** fields are read-only.

Repeat Every Week - For time periods defined by the week

a. From the **Start Day** drop-down menu, choose a day of the week on which this time period starts.

b. From the **End Day** drop-down menu, choose a day of the week on which this time period ends.

Repeat Every Year - For time periods defined by the year

a. From the **Start Month** drop-down menu, choose a month of the year on which this time period starts.

b. Enter a number from 1 to 31 in the **Start Date** field to define the day of the month on which this time period starts.

c. From the **End Month** drop-down menu, choose a month of the year on which this time period ends.

d. Enter a number from 1 to 31 in the **End Date** field to define the day of the month on which this time period ends.

- For weekly time intervals, choose a Start Day on Mon and End Day of Fri for a time period starting on Mondays and ending on Fridays.
- For weekly time intervals, choose Start Day and End Day values of Sat to define a time period that applies only on Saturdays.
- For yearly time intervals, choose Start Month value of Jan and Start Date of 15, and End values of Mar and 15 to choose the days from January 15 to March 15.
- For yearly time intervals, choose Start and End values of Jan and 1 to specify January 1 as the only day during which this time period applies.

9. Click **Save** to save the new or updated time period.

   Next steps: Associate time periods with time schedules. See “Configure Time Schedules”.

Note: You can’t delete time periods if they’re used by any time schedules. Before deleting a time period that is currently in use, perform either or both of these tasks as appropriate:

- Assign a different time period to any time schedule that is using the time period that you want to delete.
- Delete the time schedules that are using the time period that you want to delete.

Time schedules

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

A time schedule includes a group of time periods. Time schedules are assigned to partitions to set up time-of-day call routing. Time schedules determine the partitions where calling devices search when they are attempting to complete a call during a particular time of day. Multiple time schedules can use a single time period.

Configure time schedules

This procedure assigns a time period to a time schedule.

Prerequisites:

- Configure a time period. You can only assign the time period to a time schedule after you have configured a time period.

Note: Automate provides one 'All the time' schedule. The 'All the time' schedule is a special, default time schedule that includes all days and hours, and cannot be deleted.

Perform these steps:

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node where you want to create the new time schedule.
3. Go to **Time Schedules**.
4. **Choose an action**:
   - **Add a new time schedule**? Click the Plus icon (+) to add a new record, then go to Step 5.
   - **Edit an existing time schedule**? Select the time schedule to be updated by clicking it in the list of time schedules. Go to Step 6.
5. If the **Network Device List** popup displays, select the NDL for the time schedule from the drop-down. This dialog displays when you're on a non-site hierarchy. If you're at a site hierarchy, the NDL associated with the site is automatically used.

   Note: The **Network Device List** drop-down displays only when you're adding a time schedule; it doesn't display when editing a time schedule.

   ---

6. Enter a unique name for the new time schedule in the **Name** field, or modify the existing name if required. This field is mandatory.

   Note: The name can comprise up to 50 alphanumeric characters. The name of the time schedule can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

   ---

7. (Optional) Enter a description for the time schedule in the **Description** field.
8. Click the Plus icon (+) to open the **Time Periods** form.
9. From the **Time Period** drop-down, choose a time period for the time schedule.
10. Repeat Steps 8 and 9 to add another time period to the time schedule.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note:

- If multiple time periods are associated with a schedule where the time periods overlap, time periods with Day of Year settings take precedence over time periods with Day of Week settings. Day of Year is applicable when Year Start value is set and the End value is left blank.

  Example: If a Time Period configured for January 1 is configured as No Office Hours and another time period is configured for the same day of the week (for example, Sunday to Saturday) as 08:00 to 17:00, the time period for January 1 is used. In this example, No Office Hours takes precedence.

- Time interval settings take precedence over No Office Hour settings for the same day of the year or day of the week.

  Example: One time period specifies for Saturday as No Office Hours. Another time period specifies Saturday hours of 08:00 to 12:00. In this example, the resulting time interval specifies 08:00 to 12:00 for Saturday.

- If multiple time periods are associated with a schedule where the time periods overlap, time periods with Day of Week settings take precedence over time periods with Range of Days settings. Range of Days applies to when Year Start and End values are set, even if they are configured for the same day.

  Example: If a Time Period configured for Day of Week (for example, Sunday to Saturday) is configured as No Office Hours and another time period is configured for January 1 until December 31 as 08:00 to 17:00, the time period for Day of Week is used. In this example, No Office Hours takes precedence.

11. To save the new time schedule, click **Save**, or to update time schedule, click **Update**.
12. Repeat Steps 3 to 11 to configure another time schedule.

Next steps

You can't delete time schedules that partitions are using. Before deleting a time schedule that is currently in use, perform either or both of the following tasks:

- Assign a different time schedule to any partitions that are using the time schedule that you want to delete.
- Delete the partitions that are using the time schedule that you want to delete.

Warning: Before deleting a time schedule, ensure that you're deleting the correct time schedule. You cannot retrieve deleted time schedules. If you accidentally delete a time schedule, you must rebuild it.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.3.7. Cisco User Self Provisioning

Add a self-provisioning user profile

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Go to **User Profile**.
4. Click **Add**.
5. Enter the user profile information.

Field	Description
Name	Enter the name of the user profile. This field is mandatory.
Universal Line Template	Enter a site-specific ULT. This field is highly recommended.

6. On the **Device Template Desk Phone** tab.
   a. Click the Plus icon (+) to add a new template.
   b. From the **Device Security Profile** drop-down, choose **Model-independent Security Profile** .
   c. From the **Sip Profile** drop-down, choose the required SIP Profile.
   d. Select the **Allow Control of Device From Cti** checkbox.
   e. From the **Calling Search Space** drop-down, choose the appropriate option, for example Cu2Si4-InternalOnly-CSS.
7. On the **Line Template** tab.
   a. Click '+' to add a new template.
   b. From the **Partition** drop-down, choose the appropriate partition, for example Cu2-DirNum-PT.
   c. From the **Calling Search Space** drop-down, choose the appropriate calling search space, for example Cu2Si4-InternalOnly-CSS.
   d. From the **Voice Mail Profile** drop-down, choose the appropriate option, for example Default.
8. Click **Save**.
9. Fill out additional, optional settings, if applicable.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Next Steps

- Set a default user profile for a site.

Add self-provisioning line mask

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Go to the **Self Provisioning Line Mask** page.
4. Click the Plus icon (+) to add a new record, then choose a site.
5. Provide the following information:

Field	Description
Description	A description of the Line Mask.
User Attribute*	Mandatory. Select the user attribute used to generate the user's primary extension. The default is 'telephoneNumber'.
Mask*	Mandatory. Provide a mask to apply to the user attribute. The result is used as the user's primary extension. For example, assume user attribute is telephoneNumber and the mask is 4XXXX. Special characters and blanks are stripped from the user attribute before applying the mask. If the mask is applied to '(919) 867-5309', the user's primary extension would be set to 45309.

6. Click **Save**.

IOS Management - General

IOS device management

Overview

In Automate, you can set up IOS devices such as SIP local gateways and analog gateways. And you can set up command builders to generate the appropriate IOS commands, which allow you to copy to the IOS device CLI.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Command Builders in the Core Feature Guide

IOS device management workflow

This section outlines a possible workflow for setting up Local Break Out (LBO) using a SIP local gateway. This workflow copies IOS commands to the IOS device CLI after each step. Alternatively, you can use the consolidate commands tool to create one set of IOS commands to run all at once.

1. Create customized Command Builders for events. Either add new ones, or clone the default ones and update the clones. See *Set up a command builder* or *Clone a command builder*.
2. Add an IOS device at customer hierarchy level. See *Add an IOS device*.
3. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS commands log*.
4. Add SIP local gateways at customer hierarchy level. See:

   Set up SIP Local Gateway in the Core Feature Guide
5. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS commands log*.
6. Perform manual configuration on the SIP local gateway. See *IOS gateway manual configuration*.
7. Associate SIP local gateways to sites. See:

   Associate / disassociate SIP local gateway to a site in the Core Feature Guide
8. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS commands log*.
9. Create E.164 Associations. See:
   - Associate a Set of E164 Numbers to One Internal Number in the Core Feature Guide
   - Associate a Range of E164 Numbers to a Range of Internal Numbers in the Core Feature Guide
10. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS commands log*.

Add an IOS device

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer hierarchy node where you want to set up the IOS Device.
3. Go to **IOS Devices**.
4. Click the **Plus** icon (+) to add a new record.
5. Mandatory. Fill out a name for the IOS device. Optionally, you can also add a description for the IOS device.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. In the **Network Addresses** pane, configure the SERVICE_PROVIDER_SPACE address space.

Field	Description
Address Space	Address Space Type. SERVICE_PROVIDER_SPACE is the default. This field is required.
IPV4 Address	Enter the IP address of the IOS Device.
Host Name	The **Host Name** field is automatically populated with the IOS Device Name. If the IOS Device Name is not the host name, you can edit this field to provide the host name, or provide an IP address in the **IPV4 Address** field. Note: Either a host name or an IP address is required. If both are provided, the host name is used. If a host name is provided must be resolvable by the IOS Device.
Domain	The domain of the IOS Device.
Description	An optional description for the network address

7. If NAT is used, also configure an APPLICATION_SPACE network address.
8. If a double NAT is deployed, also configure a CUSTOMER_SPACE network address.
9. Optional. Expand **Credentials**, then:
   a. Add credentials for CLI, SNMP_V2, SNMP_V3 credentials types. Click + to add more credentials.
   b. For CLI and SNMP_V3, fill in the user ID and password that you configured when you installed the IOS Device. For SNMP_V2, only the password is required.
   c. For SNMP credentials, choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
   d. Optionally, provide a description for the credential.

   CLI credentials are used to log in to the IOS Device.

   Note: SNMP configuration must be done manually on the IOS Device.

10. Save your changes.

Command builders

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

You can build a repository of IOS commands to be run when certain events occur, such as adding an IOS device. Each set of IOS commands and associated event is known as a *command builder*.

For a list of events with default set of IOS commands and available variables, see *Local Break Out and Analog Gateway Events, IOS Commands, and Variables*.

The default command builders exist at the `sys.hcs` hierarchy level.

You can define customized command builders at any hierarchy node. When an event occurs, command builders nearest (at or above) the hierarchy node of the event are checked first. For instance, if an event occurs at a customer hierarchy level, command builders at the customer level are checked before command builders at the provider or sys.hcs level. Command builders at a higher level are checked only if no builders match at a nearer hierarchy level. If no customized command builders are defined, the default command builders at sys.hcs are checked. Multiple command builders may be run for the same event at the same hierarchy node.

Set up a command builder

This procedure sets up a command builder that contains an IOS commands template for an event.

Note: One event can trigger multiple command builders.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the level where you want to define your command builder.
3. Go to **Command Builder**, then click the Plus icon (+) to add a new record.
4. Configure the following - the table describes the options:

Field	Description
Name	Enter a unique name for the builder. This field is mandatory.
Event Name	Select the event that triggers the builder. This field is mandatory
Description	Enter a description for the builder.
Command Template	Enter the IOS Commands template for the event, one command per line. You can use macros in the IOS Commands template for variable substitution.
Enabled	Clear the **Enabled** check box to create a builder but not have it available to run.
Applicable Device Type	Select the device type that the commands can run on. This field is mandatory.

6. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Clone a command builder

This procedure clones (copies) a command builder that contains an IOS commands template for an event. For instance, use this procedure to modify one of the default command builders to suit your needs.

Note: One event can trigger multiple command builders.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the level where you want to clone an existing Command Builder.
3. Go to **Command Builder**.
4. Select the name of the command builder name you wish to clone.
5. Choose **Action** > **Clone**.
6. Modify the following information as needed:

Field	Description
Name	Enter a unique name for the builder. This field is mandatory.
Event Name	Select the event that triggers the builder. This field is mandatory
Description	Enter a description for the builder.
Command Template	Enter the IOS Commands template for the event, one command per line. You can use macros in the IOS Commands template for variable substitution.
Enabled	Clear the **Enabled** check box to create a builder but not have it available to run.
Applicable Device Type	Select the device type that the commands can run on. This field is mandatory.

7. Click **Save**.

View IOS commands log

Using the IOS Commands log, an administrator can see a list of command sets that were triggered by different events. An administrator can copy the IOS Commands template and paste it into the IOS device CLI to be executed.

By default, the command sets are listed with the most recent at the top.

Note: Deleting a hierarchy node, such as a site, deletes all IOS Command Builders and associated IOS Commands templates configured at the hierarchy node.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the level for which you want to view IOS Commands.
3. Go to the **Commands** page.
4. View the table the command builders that have been triggered.

   The table contains the following information:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Timestamp	The time of the event that triggered the Command Builder.
Device Name	The IOS device associated with the event that fired the Command Builder.
Gateway Name	The SIP Local Gateway or Analog Gateway associated with the event that fired the Command Builder.
Command Builder	The name of the Command Builder that was triggered. To view the IOS Commands template associated with a Command Builder, click the Command Builder name. The Command Builder configuration is displayed, including the IOS Commands template.
Description	The description of the Command Builder that was triggered.
Device Deleted	Select this check box if the associated device has been deleted.
Hierarchy	The hierarchy level of the event that triggered the Command Builder.

Consolidate IOS commands

To copy IOS commands to an IOS device CLI that is generated by multiple events, follow these steps:

Copy IOS commands

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer or site for which you want to consolidate IOS commands.
3. Go to **Consolidate Commands**.
4. Click the Plus icon (+) to add a new record.
5. On the **Consolidate Commands** page, fill out at minimum the mandatory configuration. See *Consolidate commands settings*.
6. Click the required command templates listed in the **Available** list, and click **Select** to move them to the **Selected** list.

   Click **Remove** to unselect a command template.

   Note: You can change the order of the command templates by clicking **Move Up** and **Move Down**. However, the consolidated commands are generated in chronological order regardless of the order of the selected command templates.

7. Click **Save**. The new command consolidation instance appears in the list.
8. Click the command consolidation instance you created.

   In the **Command Template** field, all the commands from the command templates you selected appear in one window. Comments are used to separate and identify the source command templates. You can edit the consolidated commands.

   Any modifications to the Command consolidation, displays the entire list of commands in a single instance. The commands present earlier to the modification cannot be viewed separately as the commands from the earlier events are treated as a single instance.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Next steps

After you have consolidated the IOS commands you want, copy them from the Commands Template field to the IOS device CLI.

Consolidate commands settings

Field	Description
Name *	Enter a unique name for the command consolidation. This field is mandatory.
Description	Enter an optional description for the command consolidation.
IOS Device *	Choose the IOS device from which you want to consolidate commands.
Device Type *	Choose the device types for which you want to consolidate commands. **IOS Device** Choose this to get commands for the IOS device and any SIP Local Gateway or Analog Gateway hosted on that device. **SIP Local Gateway** Choose this to get commands only for the SIP Local Gateway. **Analog Gateway** Choose this to get commands only for the Analog Gateway. You do not get commands for devices that have been deleted. Note: If you select site hierarchy, only specific commands such as IOS Device or SIP Local gateway are displayed. To view both the IOS and Analog gateway commands, choose the customer hierarchy path.

Regenerate IOS commands

This procedure regenerates IOS commands for events that occurred for the selected device, and removes all old IOS commands for the selected device.

Note: Since the variables used in generating IOS commands may change, you may want to regenerate IOS commands with the latest configuration. IOS commands can be regenerated for the following devices:

- IOS Device
- SIP Local gateway
- Analog Gateway

Regenerating commands for an IOS Device also regenerates commands for any SIP Local gateway or Analog Gateway hosted on the IOS Device.

1. Log in as provider, reseller, or customer administrator.
2. Choose one of the following options, depending on the device for which you want to regenerate IOS commands:
   - Go to **IOS Devices** for an IOS device and any gateways it hosts.
   - Go to **SIP Local Gateways** for a SIP local gateway.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Go to **Analog Gateways** for an analog gateway.

3. Click the device for which you want to regenerate commands.
4. Choose **Action > Regenerate IOS Commands**.

   IOS commands for the events that had occurred for the selected device are regenerated. All old IOS commands for the selected device are removed.

Next steps

- View the regenerated commands in the IOS Commands log. See *View IOS commands log*.

Local break out and analog gateway configuration and generated events

Local break out (LBO) and analog gateway configuration and corresponding events

Copyright © 2025 VisionOSS Limited. All rights reserved.

LBO and Analog Gateway Configuration Action	Generated LBO and Analog Gateway Events
Add an IOS Device	HcsAddIOSDeviceEVT
Delete an IOS Device	HcsDeleteIOSDeviceEVT
Add an Analog Device	HcsAddAnalogGatewayEVT
Add an Analog Gateway Endpoint	HcsAddAnalogGatewayEndpointEVT
Add an Analog Gateway Endpoint Mod	HcsAddAnalogGatewayEndpointModEVT
Delete an Analog Gateway	HcsDeleteAnalogGatewayEVT
Delete an Analog Gateway Endpoint	HcsDeleteAnalogGatewayEndpointEVT
Delete an Analog Gateway Endpoint Mod	HcsDeleteAnalogGatewayEndpointModEVT
Add SIP Local Gateway	Provider deployment only HcsAddSipLocalGwEVT HcsAddSipLocalGwDialPeerEVT HcsSipLocalGwAddE164AssociationEVT or HcsSipLocalGwAddMultiE164AssociationEVT (if E164 Associations have been configured at the customer level)
Delete a SIP Local Gateway	Provider deployment only HcsDeleteSipLocalGwEVT HcsDeleteSipLocalGwDialPeerEVT HcsSipLocalGwDelSitePstnEVT HcsSipLocalGwDelSiteAreaCodeEVT HcsSipLocalGwDelE164AssociationEVT or HcsSipLocalGwDelMultiE164AssociationEVT (if E164 Associations have been configured) HcsSipLocalGwDelVoiceMailPilotNumberEVT (if Voice Mail Pilot Number Association has been configured)
Update a SIP Local Gateway	Provider deployment only HcsUpdateSipLocalGw1EVT HcsUpdateSipLocalGw2EVT
Associate a SIP Local Gateway with a Site	Provider deployment only HcsSipLocalGwAddSitePstnEVT HcsSipLocalGwAddSiteAreaCodeEVT HcsSipLocalGwAddE164AssociationEVT or HcsSipLocalGwAddMultiE164AssociationEVT (if E164 Associations have been configured) HcsSipLocalGwAddVoiceMailPilotNumberEVT (if Voice Mail Pilot Number Association with a specified E164 Number has been configured on the site)

Copyright © 2025 VisionOSS Limited. All rights reserved.

LBO and Analog Gateway Configuration Action	Generated LBO and Analog Gateway Events
Disassociate a SIP Local Gateway from a Site	Provider deployment only HcsSipLocalGwDelSitePstnEVT HcsSipLocalGwDelSiteAreaCodeEVT HcsSipLocalGwDelE164AssociationEVT or HcsSipLocalGwDelMultiE164AssociationEVT (if E164 Associations have been configured)
Associate E164 Numbers to a Single DN	Provider deployment only HcsSipLocalGwAddMultiE164AssociationEVT (if a site is associated with SIP Local Gateway)
Associate E164 Numbers to a Range of DNs	Provider deployment only HcsSipLocalGwAddE164AssociationEVT (if a site is associated with SIP Local Gateway)
Disassociate E164 Numbers from a Single DN	Provider deployment only HcsSipLocalGwDelMultiE164AssociationEVT (if a site is associated with SIP Local Gateway)
Disassociate E164 Numbers from a Range of DNs	Provider deployment only HcsSipLocalGwDelE164AssociationEVT (if a site is associated with SIP Local Gateway)
Associate a Voice Mail Pilot Number to a Site	Provider deployment only HcsSipLocalGwAddVoiceMailPilotNumberEVT (if the site is associated with SIP Local Gateway)
Disassociate a Voice Mail Pilot Number from a Site	Provider deployment only HcsSipLocalGwDelVoiceMailPilotNumberEVT (if the site is associated with SIP Local Gateway)

Local break out and analog gateway events, IOS commands, and variables

Local break out (LBO) and analog gateway events:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Notes
HcsAddIOSDeviceEVT An IOS Device is added.	

`conf t`
 	
`voice service VoIP`
 	
`no IP address trusted authenticate`
 	
`y`
 	
`fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback`
`pass-through g711ulaw`
 	
`modem passthrough nse codec g711ulaw`
 	
`voice class codec 1`
 	
`codec preference 1 g729r8 bytes 30`
 	
`codec preference 2 g711ulaw`
 	
`codec preference 3 g711alaw`
 	
`end`
	If you are generating the command for VG350 analog gateway, remove y from the generated commands, and then paste it to the analog gateway console.

Default IOS Commands
HcsDeleteIOSDeviceEVT An IOS Device is deleted.

`conf t`
`no voice service VoIP`
`no voice class codec 1`
`end`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEVT An Analog Gateway is added.	

`conf t`
 	
`stcapp ccm-group 1`
 	
`stcapp`
 	
`stcapp feature access-code`
 	
`stcapp feature speed-dial`
 	
`sccp local {{ pwf.GatewayDAT.networkInterface }}`
 	
`sccp`
 	
`bind interface {{ pwf.GatewayDAT.networkInterface }}`
 	
`sccp ccm group 1`
 	
`{{ macro.HcsAnalogGwCommandForCCMIdentAndAssocMCR }}␣`
`↪ccm-manager`
`config server {{ fn.one macro.`
`↪HcsCucmsAssociatedToNDLRMCR}}`
 	
`ccm-manager sccp local {{ pwf.GatewayDAT.`
`↪networkInterface }}`
 	
`ccm-manager sccp`
 	
`stcapp`
 	
`end`
	pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEndpointEVT An Endpoint is added for the Analog Gateway.	

`conf t`
 	
`voice-port {{ pwf.PORT_NUM }}`
 	
`caller-id enable`
 	
`timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }}`
 	
`cptone {{ pwf.GatewayDAT.cpTone }}`
 	
`signal {{macro.HcsIosCmdAnalogGwSignalMCR}}`
 	
`no shutdown`
 	
`dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
 	
`service stcapp`
 	
`port {{ pwf.PORT_NUM }}`
 	
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.
	pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEndpointModEVT An Endpoint Module is added for the Analog Gateway.	

`conf t`
 	
`voice-port {{ pwf.PORT_NUM }}`
 	
`caller-id enable`
 	
`timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }}`
 	
`cptone {{ pwf.GatewayDAT.cpTone }}`
 	
`signal {{macro.HcsIosCmdAnalogGwSignalMCR}}`
 	
`no shutdown`
 	
`dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
 	
`service stcapp`
 	
`port {{ pwf.PORT_NUM }}`
 	
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.
	pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands
HcsDeleteAnalogGatewayEVT An Analog Gateway is deleted.

`conf t`
 	
`no stcapp`
 	
`no ccm-manager sccp local {{ input.GatewayDAT.networkInterface }}`
 	
`no ccm-manager sccp`
 	
`no sccp`
 	
`no sccp local {{ input.GatewayDAT.networkInterface }}`
 	
`no sccp ccm group 1`
 	
`end`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointEVT An Analog Gateway Endpoint is deleted.	

`conf t`
`voice-port {{ pwf.PORT_NUM }}`
`no caller-id enable`
`no timeouts call-disconnect`
`no cptone`
`no signal`
`shutdown`
`no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
`no port {{ pwf.PORT_NUM }}`
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointModEVT An Analog Gateway Endpoint Module is deleted.	

`conf t`
 	
`voice-port {{ pwf.PORT_NUM }}`
 	
`no caller-id enable`
 	
`no timeouts call-disconnect`
 	
`no cptone`
 	
`no signal`
 	
`shutdown`
 	
`no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
 	
`no port {{ pwf.PORT_NUM }}`
 	
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddSipLocalGwEVT A SIP Local Gateway is added.	

```
conf t
voice class e164-pattern-map 4007
e164 \+T
e164 .T
voice service VoIP
allow-connections sip to sip
sip-ua
retry invite 2
timers trying 150
application
service dsapp
param disc-toggle-time 20
param callHold TRUE
param callWaiting TRUE
param callConference TRUE
param callTransfer TRUE
voice translation-rule 802
voice translation-profile VOIPOUT80
translate called 802
voice translation-rule 812
voice translation-profile VOIPIN81
translate calling 811
translate called 812
no voice hunt invalid-number
no voice hunt unassigned-number


[CTD..]
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddSipLocalGwEVT A SIP Local Gateway is added [CTD]	
[CTD] dial-peer voice 8 VoIP translation-profile incoming VOIPIN81 session protocol sipv2 incoming called e164-pattern-map 4007 fax rate 14400 no vad voice translation-rule 812 rule 97 /^\\+01\\(.*\\)/ /904\\1/ rule 98 /^\\+1\\(.*\\)/ /901\\1/ rule 99 /^\\+\\(.*\\)/ /902\\1/ rule 100 /^\\(.*\\)/ /904\\1/ voice translation-rule 9011 rule 98 /^\\+{{pwf.COUNTRYCODE}}\\(.*\\)/ /\\1/ type ↪any national rule 99 /^\\+\\(.*\\)/ /\\1/ type any international rule 100 /^\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9021 rule 81 /^901\\(.*\\)/ /\\1/ type any national rule 82 /^902\\(.*\\)/ /\\1/ type any international rule 83 /^903\\(.*\\)/ /\\1/ type any unknown rule 84 /^904\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9022 rule 81 /^901\\(.*\\)/ /{{pwf.STDACCESSPREFIX}}\\1/ ↪type any unknown rule 82 /^902\\(.*\\)/ /{{pwf.INTLACCESSPREFIX}}\\1/ ↪type any unknown rule 83 /^903\\(.*\\)/ /\\1/ type any unknown rule 84 /^904\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9111 [CTD...]	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddSipLocalGwEVT A SIP Local Gateway is added [CTD]	

```
[CTD]

rule 1 /^\\(.*\\)/ /\+{{pwf.COUNTRYCODE}}\\1/ type␣
↪national unknown
rule 2 /^\\(.*\\)/ /\+\\1/ type international unknown
voice translation-rule 9012
rule 98 /^\\+{{pwf.COUNTRYCODE}}\\(.*\\)/
/{{pwf.STDACCESSPREFIX}}\\1/ type any unknown
rule 99 /^\\+\\(.*\\)/ /{{pwf.INTLACCESSPREFIX}}\\1/␣
↪type any unknown
rule 100 /^\\(.*\\)/ /\\1/ type any unknown
voice translation-rule 9121
voice translation-rule 9112
rule 1 /^{{pwf.INTLACCESSPREFIX}}\\(.*\\)/ /\+\\1/␣
↪type unknown unknown
rule 2 /^{{pwf.STDACCESSPREFIX}}\\(.*\\)/
/\+{{pwf.COUNTRYCODE}}\\1/ type unknown unknown
voice translation-rule 9122
voice translation-profile POTSOUT9011
translate calling 9011
translate called 9021
voice translation-profile POTSOUT9012
translate calling 9011
translate called 9022
voice translation-profile POTSOUT9021
translate calling 9012
translate called 9021
voice translation-profile POTSOUT9022
translate calling 9012
translate called 9022
voice translation-profile POTSIN9111
translate calling 9111
translate called 9121
voice translation-profile POTSIN9112
translate calling 9111
translate called 9122
voice translation-profile POTSIN9121
translate calling 9112
translate called 9121
voice translation-profile POTSIN9122
translate calling 9112
translate called 9122
end
```

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables	Notes
HcsAddSipLocalGwDialPeerEVT Triggers IOS Commands for each Dial Peer when A SIP Local Gateway is added.		

`conf t`
`dial-peer voice {{pwf.DIALPEER}} VoIP`
`translation-profile outgoing VOIPOUT80`
`{{pwf.PREFERENCE}}`
`voice-class codec 1`
`service dsapp`
`voice-class sip options-keepalive up-interval 120 down-interval 60 retry 2`
`session target {{pwf.PBXIP}}`
`destination e164-pattern-map 4007`
`session protocol sipv2`
`modem passthrough nse codec g711ulaw`
`dtmf-relay rtp-nte`
`fax rate 14400`
`no vad`
`end`
	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW
	pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW
	pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW
	pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer
	pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list
	pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.
		One command set is generated per dial peer.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsDeleteSipLocalGwEVT A SIP Local Gateway is deleted.	

`conf t`
`no voice translation-profile POTSIN9122`
`no voice translation-profile POTSIN9121`
`no voice translation-profile POTSIN9112`
`no voice translation-profile POTSIN9111`
`no voice translation-profile POTSOUT9022`
 	
`no voice translation-profile POTSOUT9021`
 	
`no voice translation-profile POTSOUT9012`
 	
`no voice translation-profile POTSOUT9011`
 	
`no voice translation-rule 9122`
 	
`no voice translation-rule 9112`
 	
`no voice translation-rule 9121`
 	
`no voice translation-rule 9012`
 	
`no voice translation-rule 9111`
 	
`no voice translation-rule 9022`
 	
`no voice translation-rule 9021`
 	
`no voice translation-rule 9011`
 	
`no voice translation-rule 812`
 	
`no voice translation-rule 802`
 	
`no dial-peer voice 8 VoIP`
 	
`no voice class e164-pattern-map 4007`
`application`
`no service dsapp`
`no sip-ua`
`voice service VoIP`
`no allow-connections sip to sip`
`end`
	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW
	pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW
	pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW
	pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer
	pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list
	pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables	Notes
HcsDeleteSipLocalGwDialPeerEVT Triggers IOS Commands for each Dial Peer when A SIP Local Gateway is deleted.		

`conf t`
`no dial-peer voice {{pwf.DIALPEER}} VoIP`
 	
`end`
	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW
	pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW
	pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW
	pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer
	pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list
	pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.
		One command set is generated per dial peer.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables	Notes
HcsUpdateSipLocalGw1EVT Triggers IOS Commands when A SIP Local Gateway is updated.		

`conf t`
 	
`no dial-peer voice {{pwf.DIALPEER}} VoIP`
 	
`end`
	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW
	pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW
	pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW
	pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer
	pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list
	pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.
		Removes configuration related to previous dial peer. One set of commands per dial peer. Note: If "Enable Command Builder" is updated from False to True, IOS commands will be regenerated for the SIP Local Gateway.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables	Notes
HcsUpdateSipLocalGw2EVT Triggers IOS Commands when A SIP Local Gateway is updated.		

`conf t`
`dial-peer voice {{pwf.DIALPEER}} VoIP`
`translation-profile outgoing VOIPOUT80`
`{{pwf.PREFERENCE}}`
`voice-class codec 1`
`service dsapp`
`voice-class sip options-keepalive up-interval 120 down-interval 60 retry 2`
`session target {{pwf.PBXIP}}`
`destination e164-pattern-map 4007`
`session protocol sipv2`
`modem passthrough nse codec g711ulaw`
`dtmf-relay rtp-nte`
`fax rate 14400`
`no vad`
`end`
	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW
	pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW
	pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW
	pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer
	pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list
	pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.
		Adds configuration related to new dial peer. One set of commands per dial peer. Event is triggered only if the SIP Trunk information has been updated.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables	Notes
HcsSipLocalGwAddSiteAreaCodeEVT Triggers IOS commands for Area Code when a SIP Local Gateway is associated with a Site.		

`conf t`
 	
`voice translation-rule 9021`
 	
`rule {{pwf.RULENUMBER}} /^901{{pwf.NATCODE}}\\(.*\\)//{{pwf.NATCODEFORLOCALDIALING}}\\1/ type any subscriber`
 	
`voice translation-rule 9022`
 	
`rule {{pwf.RULENUMBER}} /^901{{pwf.NATCODE}}\\ (.*\\)//{{pwf.NATCODEFORLOCALDIALING}}\\1/ type any unknown`
 	
`end`
	{{pwf.RULENUMBER}} and {{pwf.NATCODE}} are sequence numbers and area codes that is substituted by workflow during runtime {{pwf.NATCODEFOR LOCALDIALING}} is the Area Code if the administrator selected the "Area Code Used for Local Dialing" option when deploying the site dial plan. If this option was not selected, this variable has no value.	The workflow for this event generates IOS Commands for each Area Code defined for the associated Site.

(Provider deployment)

Default IOS Commands	Available Variables	Notes
HcsSipLocalGwDelSiteAreaCodeEVT Triggers IOS commands for Area Code when a SIP Local Gateway is disassociated from Site.		

`conf t`
 	
`no voice translation-rule 9021`
 	
`no rule {{pwf.RULENUMBER}}`
 	
`end`
 	
`conf t`
 	
`no voice translation-rule 9022`
 	
`no rule {{pwf.RULENUMBER}}`
 	
`end`
	{{pwf.RULENUMBER}} is substituted as sequence number by workflow during run time	The workflow for this event generates IOS Commands for each Area Code defined for the disassociated Site. If Area Codes are shared across multiple sites and associated with the same gateway, the commands are generated only when the gateway is disassociated from the last site that shares the Area Code.

Copyright © 2025 VisionOSS Limited. All rights reserved.

(Provider deployment)

Default IOS Commands	Available Variables
HcsSipLocalGwAddSitePstnEVT Triggers IOS commands for PSTN when a SIP Local Gateway is associated with a Site.	

`conf t`
`voice translation-rule 9111`
`rule 3 /^\\(.*\\)/ /{{pwf.PSTNACCESSPREFIX}}\\\\1/ type`
`subscriber unknown`
 	
`rule 4 /^\\(.*\\)/ /{{pwf.PSTNACCESSPREFIX}}\\\\1/ type unknown`
`unknown`
`voice translation-rule 9112`
`rule 3 /^\\(.*\\)/ /{{pwf.PSTNACCESSPREFIX}}\\\\1/ type unknown`
`unknown`
`end`
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site

(Provider deployment)

Default IOS Commands	Notes
HcsSipLocalGwDelSitePstnEVT Triggers IOS commands for PSTN when a SIP Local Gateway is disassociated from Site.	

`conf t`
 	
`no voice translation-rule 9111`
 	
`no rule 3`
 	
`no rule 4`
 	
`no voice translation-rule 9112`
 	
`no rule 3`
 	
`end`
	By default, these commands are not generated to avoid deleting the voice translation rule for PSTN if the gateway is shared by multiple sites. If you need to delete the translation rules for PSTN when SIP Local Gateway is disassociated from site, clone the command builder template and set the Enabled flag.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsSipLocalGwAddE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to 1 DN) is made.	

`conf t`
 	
`voice translation-rule 9011`
 	
`rule {{ pwf.RULENUMBER }} /^{{pwf.DNESCAPE }}{{ pwf.DNPREFIX }}`
`\\\\ ({{ pwf.RGMASK }} \\\\ )/ /{{ pwf.DDIPREFIX }} \\\\ 1/ type`
`any national`
 	
`voice translation-rule 9012`
 	
`rule {{ pwf.RULENUMBER }} /^{{pwf.DNESCAPE }}{{ pwf.DNPREFIX }}`
`\\\\ ({{ pwf.RGMASK }} \\\\ )/ /{{ pwf.STDACCESSPREFIX }}{{`
`pwf.DDIPREFIX }} \\\\ 1/ type any unknown`
 	
`voice translation-rule 802`
 	
`rule {{ pwf.RULENUMBER }} /^{{pwf.DNESCAPE }}{{ pwf.DNPREFIX }}`
`\\\\ ({{ pwf.RGMASK }} \\\\ )/ /\+{{ pwf.COUNTRYCODE }}{{`
`pwf.DDIPREFIX }} \\\\ 1/`
 	
`voice translation-rule 9121`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.DDIPREFIX }} \\\\ ({{`
`pwf.RGMASK }} \\\\ )/ /{{ pwf.DNPREFIX }} \\\\ 1/ type national`
`unknown`
 	
`voice translation-rule 9122`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.STDACCESSPREFIX }}{{`
`pwf.DDIPREFIX }} \\\\ ({{ pwf.RGMASK }} \\\\ )/ /{{ pwf.DNPREFIX`
`}} \\\\ 1/ type unknown unknown`
 	
`voice translation-rule 712`
 	
`[CTD..]`
	pwf.DNPREFIX - Contains the directory number prefix (DN without the mask digits)
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsSipLocalGwAddE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to 1 DN) is made.	

`[CTD..]`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.PSTNACCESSPREFIX }}`
`↪{{`
`pwf.STDACCESSPREFIX }}{{ pwf.DDIPREFIX }} \\\\ ({{␣`
`↪pwf.RGMASK }}`
`\\\\ )/ /{{ pwf.DNPREFIX }} \\\\ 1/`
 	
`end`
	pwf.RULENUMBER - Contains the appropriate rule index for associate/disassociate

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsSipLocalGwDelE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to 1 DN) is deleted.	

`conf t`
`voice translation-rule 9011`
`no rule {{ pwf.RULENUMBER }}`
 	
`end`
 	
`conf t`
 	
`voice translation-rule 9012`
 	
`no rule {{ pwf.RULENUMBER }}`
 	
`end`
 	
`conf t`
 	
`voice translation-rule 802`
 	
`no rule {{ pwf.RULENUMBER }}`
 	
`end`
 	
`conf t`
 	
`voice translation-rule 9121`
 	
`no rule {{ pwf.RULENUMBER }}`
 	
`end`
 	
`conf t`
 	
`voice translation-rule 9122`
 	
`no rule {{ pwf.RULENUMBER }}`
 	
`end`
 	
`conf t`
 	
`voice translation-rule 712`
`no rule {{ pwf.RULENUMBER }}`
`end`
	pwf.DNPREFIX - Contains the directory number prefix (DN without the mask digits)
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for associate/disassociate

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsSipLocalGwAddMultiE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to N DN) is made.	

`conf t`
 	
`voice translation-rule 9011`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.DNESCAPE }}{{ pwf.DN }}/ /{{ pwf.DDIPRIMARY }}/ type any national`
 	
`voice translation-rule 9012`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.DNESCAPE }}{{ pwf.DN }}/ /{{ pwf.STDACCESSPREFIX }}{{ pwf.DDIPRIMARY }}/ type any unknown`
 	
`voice translation-rule 802`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.DNESCAPE }}{{ pwf.DN }}/ /\+{{ pwf.COUNTRYCODE }}{{ pwf.DDIPRIMARY }}/`
 	
`voice translation-rule 9121`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.DDIPREFIX }}{{ pwf.RGMASK }}/ /{{ pwf.DN }}/ type national unknown`
 	
`voice translation-rule 9122`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.STDACCESSPREFIX }}{{ pwf.DDIPREFIX }}{{ pwf.RGMASK }}/ /{{ pwf.DN }}/ type unknown unknown`
 	
`voice translation-rule 712`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.PSTNACCESSPREFIX }}{{ pwf.STDACCESSPREFIX }}{{ pwf.DDIPREFIX }}{{ pwf.RGMASK }}/ /{{ pwf.DN }}/`
 	
`end`
	pwf.DN - Contains the directory number
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPRIMARY - Contains the primary E.164 associate with the N:1 association (DDI without + prefix and country code) Note: this still contains the national code (area code)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for associate/disassociate

Copyright © 2025 VisionOSS Limited. All rights reserved.

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsSipLocalGwDelMultiE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to N DN) is deleted.	

`conf t`
`voice translation-rule 9011`
`no rule {{ pwf.RULENUMBER }}`
`end`
`conf t`
`voice translation-rule 9012`
`no rule {{ pwf.RULENUMBER }}`
`end`
`conf t`
`voice translation-rule 802`
`no rule {{ pwf.RULENUMBER }}`
`end`
`conf t`
`voice translation-rule 9121`
`no rule {{ pwf.RULENUMBER }}`
`end`
`conf t`
`voice translation-rule 9122`
`no rule {{ pwf.RULENUMBER }}`
`end`
`conf t`
`voice translation-rule 712`
`no rule {{ pwf.RULENUMBER }}`
`end`
	pwf.DN - Contains the directory number
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPRIMARY - Contains the primary E.164 associate with the N:1 association (DDI without + prefix and country code) Note: this still contains the national code (area code)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for associate/disassociate

Copyright © 2025 VisionOSS Limited. All rights reserved.

(Provider deployment)

Default IOS Commands	Available Variables
HscSipLocalGwAddVoiceMailPilotNumberEVT Associate a Voice Mail Pilot Number with a Site	

`conf t`
 	
`voice translation-rule 9121`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.DDIPREFIX }}\\\\({{ pwf.RGMASK }}\\\\)/ /{{ pwf.DNPREFIX }}\\\\1/ type national unknown`
 	
`voice translation-rule 9122`
 	
`rule {{ pwf.RULENUMBER }} /^{{ pwf.STDACCESSPREFIX }}{{ pwf.DDIPREFIX }}\\\\({{ pwf.RGMASK }}\\\\)/ /{{ pwf.DNPREFIX }}\\\\1/ type unknown unknown`
 	
`end`
	pwf.DNPREFIX - Contains the voice mail pilot number prefix (without the mask digits)
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for voice mail pilot association

(Provider deployment)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HscSipLocalGwDelVoiceMailPilotNumberEVT Disassociate a Voice Mail Pilot Number from a Site	

`conf t`
`voice translation-rule 9121`
`no rule {{ pwf.RULENUMBER }}`
`end`
`conf t`
`voice translation-rule 9122`
`no rule {{ pwf.RULENUMBER }}`
`end`
	pwf.DNPREFIX - Contains the voice mail pilot number prefix (without the mask digits)
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for voice mail pilot association

MGCP analog gateway events and IOS commands

MGCP analog gateway events:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEVT Adds an Analog MGCP Gateway.	

`conf t`
`hostname {{pwf.GatewayDAT.domainName}}`
`ccm-manager config server {{ fn.one macro.`
`↪HcsCucmsAssociatedToNDLRMCR}}`
`ccm-manager config`
`mgcp call-agent {{ fn.one macro.`
`↪HcsCucmsAssociatedToNDLRMCR}} 2427 service-type␣`
`↪mgcp version 1.0`
`ccm-manager mgcp`
`! ccm-manager redundant-host`
`ccm-manager switchback Graceful`
`ccm-manager fallback-mgcp`
`mgcp bind control source-int {{ pwf.GatewayDAT.`
`↪networkInterface }}`
`mgcp bind media source-int {{ pwf.GatewayDAT.`
`↪networkInterface }}`
`mgcp dtmf-relay voip codec all mode out-of-band`
`mgcp modem passthrough voip mode nse`
`mgcp package-capability sst-package`
`no mgcp package-capability sst-package`
`end`
	pwf.GatewayDAT.networkInterface - returns the Network Interface based on the configuration in the Gateway.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEndpointEVT Adds an Endpoint for the Analog MGCP Gateway.	

`conf t`
`voice-port {{ pwf.PORT_NUM }}`
`timeouts call-disconnect {{ fn.as_string pwf.`
`↪GatewayDAT.disconnectTimeout }}`
`cptone {{ pwf.GatewayDAT.cpTone }}`
`signal {{macro.HcsIosCmdAnalogGwSignalMCR}}`
`ring frequency 25`
`description {{ fn.sub_string macro.`
`↪HcsAnalogGatewayIOSCmdDesc, 0, 63 }}`
`timing hookflash-in 250 80`
`no shutdown`
`exit`
`dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
`service mgcpapp`
`port {{ pwf.PORT_NUM }}`
`end`
	pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.
	pwf.DIAL_PEER_NO - returns the dial peer number that is used to generate the dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsAddAnalogMGCPGatewayEndpointModEVT Adds an Endpoint Module for the Analog MGCP gateway.	

`conf t`
`voice-port {{ pwf.PORT_NUM }}`
`timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }}`
`cptone {{ pwf.GatewayDAT.cpTone }}`
`signal {{macro.HcsIosCmdAnalogGwSignalMCR}}`
`ring frequency 25`
`description {{ fn.sub_string macro.HcsAnalogGatewayIOSCmdDesc, 0, 63 }}`
`timing hookflash-in 250 80`
`no shutdown`
`exit`
`dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
`service mgcpapp`
`port {{ pwf.PORT_NUM }}`
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.
	pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEVT Deletes an Analog MGCP Gateway.	

`conf t`
`no mgcp call-agent {{ fn.one macro.`
`↪HcsCucmsAssociatedToNDLRMCR}} 2427 service-type␣`
`↪mgcp version 1.0`
`no ccm-manager config server {{ fn.one macro.`
`↪HcsCucmsAssociatedToNDLRMCR}}`
`mgcp`
`no ccm-manager mgcp`
`! no ccm-manager redundant-host`
`no ccm-manager switchback Graceful`
`no ccm-manager fallback-mgcp`
`no mgcp bind control source-int {{ pwf.GatewayDAT.`
`↪networkInterface }}`
`no mgcp bind media source-int {{ pwf.GatewayDAT.`
`↪networkInterface }}`
`no mgcp dtmf-relay voip codec all mode out-of-band`
`no mgcp modem passthrough voip mode nse no ccm-`
`↪manager music-on-hold`
`no ccm-manager config`
`no mgcp package-capability rtp-package`
`no  mgcp package-capability sst-package`
`no  mgcp default-package mt-package`
`no mgcp timer receive-rtcp`
`no  mgcp sdp simple`
`no mgcp fax t38 inhibit`
`no mgcp`
`end`
	pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointEVT Deletes an Endpoint for the Analog MGCP Gateway.	

`conf t`
`voice-port {{ pwf.PORT_NUM }}`
`no timeouts call-disconnect`
`default cptone`
`default timing hookflash-in`
`default description`
`no signal`
`default ring frequency`
`shutdown`
`exit`
`no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsDeleteAnalogMGCPGatewayEndpointModEVT Deletes an Endpoint Module for the Analog MGCP Gateway.	

`conf t`
`voice-port {{ pwf.PORT_NUM }}`
`no timeouts call-disconnect`
`default cptone`
`default timing hookflash-in`
`default description`
`no signal`
`default ring frequency`
`shutdown`
`exit`
`no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots`
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default IOS Commands	Available Variables
HcsUpdateAnalogGatewayEVT Updates the Analog MGCP Gateway.	

`conf t`
`hostname {{pwf.GatewayDAT.domainName}}`
`no mgcp bind control source-int {{ pwf.previousGatewayDAT.networkInterface }}`
`mgcp bind control source-int {{ pwf.GatewayDAT.networkInterface }}`
`no mgcp bind media source-int {{ pwf.previousGatewayDAT.networkInterface }}`
`mgcp bind media source-int {{ pwf.GatewayDAT.networkInterface }}`
`end`
	pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.

Default IOS Commands	Available Variables
HcsUpdateAnalogGatewayEndpointEVT Updates the Endpoint for the Analog MGCP Gateway.	

`conf t`
`voice-port {{ pwf.PORT_NUM }}`
`no signal`
`signal {{macro.HcsIosCmdAnalogGwSignalMCR}}`
`no timeouts call-disconnect`
`timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }}`
`no cptone`
`cptone {{ pwf.GatewayDAT.cpTone }}`
`no shutdown`
`end`
	pwf.PORT_NUM - This is the FXS port number of the analog gateway device.
	pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.
	pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.

Translation rule numbering

The following information can be helpful to decode the number of translation rules included in IOS command builders.

- The first digit indicates if the rule is for SRST, VoIP, or TDM: 7 for SRST, 8 for VoIP, and 9 for PSTN.
- The second digit indicates if it is for incoming or outgoing call: 1 for incoming and 0 for outgoing
- The third digit indicates if it is for calling or called number: 1 for calling and 2 for called
- The fourth digit indicates if NOA is used: 1 is for NOA and 2 for no NOA and defines on the TDM trunk to the PSTN.

Examples:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Translation-rule 9011 - for handling calling number of an outgoing call to the PSTN where NOA is used.
- Translation-rule 9022 - for handling called number of an outgoing call to the PSTN where NOA is not used.
- Translation-rule 9111 - for handling calling number of an incoming call from the PSTN where NOA is used.

Analog gateways

Tip: *Use the Action search to navigate Automate*

Overview

A Cisco analog gateway connects fax machines, analog phones, and modems in the SCCP/MGCP protocol. Any IOS device that has FXS ports configured as SCCP/MGCP endpoints on Cisco Unified Communications Manager is considered an SCCP/MGCP analog gateway.

An analog device contains analog phones, which are endpoints in Cisco Unified Communications Manager.

The table displays success and failure scenarios showing the expected behavior of an Analog gateway when adding a new gateway and when modifying or deleting an existing gateway:

Successful Scenario	Failure Scenario
Adding an Analog device with a phone line.	Removing the phone line from the endpoint.
Adding an Analog gateway without using enable command builder.	Adding a phone line after adding the command builder.
Removing the command builder after adding an analog gateway with command builder.	Adding an analog gateway without a phone line after adding a phone line to an endpoint. Note: Ensure to add the Directory Names to both endpoints.

Add an analog gateway

This procedure adds an analog gateway.

Tip: *Use the Action search to navigate Automate*

Pre-requisites

- Add an IOS device in Automate at the Customer level hierarchy. See *Add an IOS device*.
- If applicable, ensure that the site-level dial plan is applied on the site where the gateway is being added.

Note: Automate supports SCCP and MGCP protocols. It does not support BRI endpoints. Do not add slots or modules or subunits for BRI.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add an analog gateway:

1. Log in as provider, reseller, or customer administrator.
2. Go to **Analog Gateways**.
3. Click the Plus (+) icon, then select the relevant hierarchy.
4. Configure the analog gateway:
   - On the **Gateway** tab, complete, at minimum, the mandatory *Gateway settings*.
   - On the **Gateway Units** tab, click the Plus icon (+) to expand **Modules**, then complete, at minimum, the mandatory *Gateway Units - Modules settings*.
   - On the **Endpoints** tab, click the Plus icon (+) to expand the SCCP or MGSP endpoints, then complete, at minimum, the following mandatory settings:
     - *Endpoints settings (SCCP)*
     - *Endpoints settings (MGCP)*

     Note: Gateway endpoints display in the following order on the **Endpoints** tab:

     Slot > Subunit > Port Number, for example:

     ```
     0-0-0
     0-0-1
     2-0-0
     2-0-1
     2-0-2
     ```

   - On the **Config** tab, click the Plus icon (+) to expand the **Product Specific Configuration Layout**, then complete the required *Config: Product-specific configuration layout settings*.
5. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Gateway settings

Field	Description
IOS Device *	Choose the required IOS Device from the drop-down list. For example: IOS 11. This is a mandatory field. Note: The IOS device identifies the devices that are not associated with any Analog Gateways.
Product *	Choose the product from the drop-down list. For example: VG202, where VG represents Voice Gateway and 202 represents port. It has 2 ports, 0 and 1. This is a mandatory field. Note: The analog gateway supports the following models (FXS ports): • VG202: 2 ports • VG204: 4 ports • VG224: 24 ports • VG310: 24 ports • VG320: 48 ports • VG350: 144/160 ports • VG400: 8 ports max • VG410: 48 ports max • VG420: 144 ports max • VG450: 144 ports max
Protocol *	Choose the protocol from the drop-down list. The available protocols are **SCCP** and **MGCP**. This is a mandatory field.
Gateway Name *	Enter the MAC address of the analog gateway. For example: SKIGW0102030405, where SKI represents SCCP, GW represents gateway, and the last 10 digits represents the MAC address of the gateway. This is a mandatory field for the SCCP protocol.
Domain Name	Enter a fully qualified domain name. For example: E7C1VG310.hcsent17.com. This is a mandatory field for the MGCP protocol.
Call Manager Group *	Mandatory. Choose the call manager group from the drop-down. For example: **Default**. Note: Call Manager Group is default based on the site default device pool.
Enable Command Builder	Leave the check box clear to generate IOS commands, when Analog Gateway is added, deleted, or modified.

Note: To view generated commands from Command Builder, see *View IOS commands log*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Gateway Network Interface *	Enter a Gateway Network Interface. For example: **FastEthernet0/0**, **FastEthernet0/1**, **GigabitEthernet0/0**, **GigabitEthernet0/1** or ****GigabitEthernet0/2**. This is a mandatory field. Note: Check the network interface at the Physical Device, then choose the appropriate Network Interface and Port as applicable. The Network Interface is used in Command Generation. Choose **FastEthernet** for all 2x series and **GigabitEthernet** for all 3x series.
Call Disconnect Timeout *	Enter the time unit for Call Disconnect Timeout. For example: **2**. This is a mandatory field. Note: The time unit always is in seconds. Do not enter any negative timer values.
CP Tone *	Choose the call progress tone (country code) from the drop-down list. For example: **in** (for India). This is a mandatory field. Note: CP Tone is an FXS configuration parameter that supports each analog device in the gateway.
Signal *	Choose a signal from the drop-down list. For example: **loop-start** or **ground-start**. This is a mandatory field. Note: Signal is an FXS configuration parameter that supports each analog device in the gateway.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Gateway Units - Modules settings

Field	Description
Slot *	Choose the required value from the drop-down list. For example: 0. This is a mandatory field Note: • Add only those Units (Modules) and Subunits that are listed in the drop-down list, without duplicate the units and subunit numbers. • If duplicating entry is made for a slot, then the new slot overwrites the older configuration. You may lose previously configured endpoints. • For VG310 model, do not choose any module for slot 1.
Module *	Choose the available module from the drop-down list. For example: NM-4VWIC-MBRD. Note: Only modules that are available for the slot appear in the list.
Subunits *	Click + to expand Subunits. This is a mandatory field.
Subunit Position *	Choose the subunit position from the drop-down list. For example: 0. Note: Subunit position 1 on the VG310 gateway has no available hardware by design, so choosing a value of 1 in this drop-down will not allow you to continue. Please choose a different subunit position to continue setting up your gateway.
Subunit *	Choose the subunit from the drop-down list. For example: VIC3-2FXS-E/DID-SCCP.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Endpoints settings (SCCP)

Option	Description
Gateway Name	GUI read-only field is populated from the analog gateway for the SCCP protocol. This is a mandatory field.
Slot *	GUI read-only field is populated from the gateway units. This is a mandatory field.
Subunit Position *	GUI read-only field is populated from the gateway units. This is a mandatory field.
Port Number *	GUI read-only field is populated from the gateway units. This is a mandatory field.
Product Type *	Choose the product type from the drop-down list. For example: Analog Phone. This is a mandatory field.
Device Protocol *	Choose the device protocol from the drop-down list. This is a mandatory field.
Device Name *	GUI read-only field is populated from the analog gateway. This is a mandatory field.
Description	When the endpoint is added, the default description is in the format: *Endpoint for slot/subunit/port n/n/n gateway @domain* that can be updated if required. This is an optional field and accepts a string value.
Device Pool *	Choose the device pool from the drop-down list. For example: Cu2Si2-DevicePool. This is a mandatory field.
Phone Button Template *	Choose the phone button template from the drop-down list. For example: Standard Analog. This has a specific phone button template for the analog gateway. This is a mandatory field.
Common Phone Profile *	Choose the common phone profile from the drop-down list. For example: Standard Common Phone Profile. It includes the attributes (services or features) that are associated with a particular user. This is a mandatory field.
Calling Search Space	From the drop-down list, choose the appropriate calling search space. The calling search space specifies a collection of partitions that are searched to determine how a collected (originating) number should be routed.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.
Location *	Choose a location from the drop-down list. For example: Cu2Si2-Location. This is a mandatory field.
AAR Group	Specify the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth.
Owner	Choose from the drop-down list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Always Use Prime Line for Voice Message	Choose the required options from the drop-down list. For example: On, Off or Default. This is a mandatory field. This specifies whether the device will always use the prime line for voice messages.
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.
Transmit UTF-8 for Calling Party Name	Keep the check box clear.
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. Note: If the Called Party Transformation CSS is configured as <None>, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	Select the check box.
Allow Control Of Device From CTI	Select the check box.
Logged Into Hunt Group	Select the check box.
Calling Party Transformation CSS (Caller ID For Calls From This Phone)	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Note: If the Calling Party Transformation CSS is configured as <None>, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Use Device Pool Calling Party Transformation CSS (Caller ID for Calls From This Phone)	Select the check box.
Calling Party Transformation CSS (Device Mobility Related Information)	

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)	Select the check box.
BLF Presence Group *	Choose the presence group for busy lamp field buttons from the drop-down list. For example: Standard Presence group is the default value. This is a mandatory field.
Device Security Profile *	Choose options from the drop-down list. For example: Analog Phone - Standard SCCP Non-Secure Profile. This is mandatory field.
MLPP Domain	If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device pool of this device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	Choose options from the drop-down list. For example: On, Off, or Default. This is a mandatory field.
MLPP Preemption	Choose options from the drop-down list. For example: Disabled, Forceful, Default. This is a mandatory field. Note: If there are any changes to be performed to analog phone line then do not refer line settings. For example: Changing CSS is done under User Management.
Line	Click + to expand **Line**.
Pattern *	Choose the route pattern from the drop-down list. For example: 08231006
Enduser	Click + to expand **Enduser**.
User ID	Choose the available user ID from the drop-down list. For example: User 1
Product Specific Configuration Layout	Click + to expand **Product Specific Configuration Layout**.
Key	Enter the Key for the product specific configuration layout. For example: stcapRegCap.
Value	Enter the Key for the product specific configuration layout. For example: 0.

Note: For more optional field information, see *Cisco phones*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Endpoints settings (MGCP)

You can configure multiple endpoints for an MGCP gateway.

Option	Description
Domain Name	GUI read-only field is populated from the analog gateway for the MGCP protocol. This is a mandatory field.
Slot *	GUI read-only field is populated from the gateway units. This is a mandatory field.
Subunit Position *	GUI read-only field is populated from the gateway units. This is a mandatory field.
Port Number *	GUI read-only field is populated from the gateway units. This is a mandatory field.
Product Type *	Choose the product type from the drop- down list. For example: Analog Phone. This is a mandatory field.
Device Protocol *	Choose the device protocol from the drop-down list. For example: SCCP. This is a mandatory field.
Protocol Side *	This is a read-only field except when creating a device. This is a mandatory field.
Class *	This is a read-only field except when creating a device. This is a mandatory field.
Device Name *	GUI read-only field is populated from the analog gateway. This is a mandatory field.
Description	When the endpoint is added, the default description is in the format: *Endpoint for slot/subunit/port n/n/n gateway @domain*. Update it with an optional description for the device. This is an optional field and accepts a string value.
Device Pool	Choose the device pool from the drop-down list. For example: Cu2Si2-DevicePool. This is a mandatory field.
Calling Search Space	Choose the space name from the drop-down list. This is an optional field.
Common Device Configuration	Specify the Configuration name of the device. This is an optional field.
Network Locale	Choose the location from the drop-down list. This is an optional field.
Location *	Choose a location from the drop-down list. For example: Cu2Si2-Location. This is a mandatory field.
Media Resource Group List	Choose a media resource to allocate for a device. This is an optional field.
AAR calling search space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) from the drop-down list. This is an optional field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Use Trusted Relay Point	Choose one of the following values: • Off - Choose this value to disable the use of a Trusted Relay Point (TRP) with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On - Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • Default - If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
AAR Group	Specify the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth.
Geolocation	Specify the location name. This is an optional field.
Transmit UTF-8 for Calling Perty Name MLPP Preemption	Keep the check box cleared.
Port Number *	Configure the ports for the **MGCP Endpoint**. This is a mandatory field.
Trunk *	This field value auto-populates depending on the value set for the Port Number. This is a mandatory field.
Trunk Direction *	The field value auto-populates depending on the value set for the Number. This is a mandatory field.
Trunk Level *	The field value auto-populates depending on the value set for the Number. This is a mandatory field.
Attendant DN	Specify this field for group start and loop start. This is a mandatory field.
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls.
Num Digits *	Enter the number of significant digits to collect between 0 to 32.
Expected Digits *	Enter the number of digits that are expected on the inbound side of the trunk. You can leave zero as the default value, if you are unsure.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
SMDI Port Number (0 - 4096) *	Enter the first SMDI port number of the T1 span. If you set this parameter to a nonxero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue beyond this span.
Unattended Port	Select this check box to indicate an unattended port on this device.
Line	Click + to expand **Line**.
Label	Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line and phone combination.
E164 Mask	Indicate a phone number (or mask) that is used to send Caller ID information when a call is placed from the line. You can enter a maximum of 24 numbers, the international escape character + and 'X' characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.
Dirn, Pattern *	Choose the route pattern from the drop-down list. For example: 08231006.
Dirn, Route Partition	Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the Directory Number field is unique within the partition that you choose. If you do not want to restrict access to the directory number, choose <None> for the partition.
Enduser	Click + to expand **Enduser**.
User ID	Choose the available user ID from drop-down list. For example: User 1.
Index	This field is the line position on the device. If left blank, an integer is automatically assigned.
Trunk Selection Order *	Choose the order from the drop-down list to display the call routing logic for the route pattern.

Config: Product-specific configuration layout settings

Field	Description
Key	Enter the Key for the product-specific configuration Layout. For example stcappRegCap.
Value	Enter the Key for the product-specific configuration layout. For example: 0.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a port to an analog gateway

Tip: *Use the Action search to navigate Automate*

You can add a new port to a gateway located at site level, without prior knowledge of existing ports. This is useful on the higher density gateways, and in cases where a port is bulk loaded.

Note: The following ports are supported:

- VG2XX and VG3XX models (FXS ports) are supported, providing a range of port capacities, from 2 - 160 ports.
- VG400 (8 ports max) and VG450 (144 ports max) models (FXS ports)

1. In the Automate Admin Portal, go to **Add port to Analog Gateway**.
2. Choose a site.
3. Configure the following:
   - At **Gateway Domain**, add a URI, and add a description for the analog gateway.
   - Choose owner user ID, and INI inventory filter.
   - At **Directory Number**, specify the directory number to use for the new line.

     Note: When selecting a Directory Number (DN) to add to a new port:

     – The next available DN from site level INI is pre-populated.

     – The **Directory Number** drop-down can be used to select alternative Directory Numbers.

     – If a bulk loader or form drop-down does not have the Directory Number field populated, the next number from site level INI is used. If this is not available, the next available number from customer level INI is used.

   - At **Calling Search Space**, fill out the Line CSS (if this is a new line).
   - Optionally, use one or more of the custom fields (Custom String or Custom Boolean) to configure additional fields, for example, to add a display name.
4. Click **Save**.

   VOSS Automate checks for the first free port space on the gateway, and adds the port to the gateway.

   Once the transaction completes, a log entry shows the port number added.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP gateway port

Tip: *Use the Action search to navigate Automate*

Manage gateway ports

This procedure displays, updates, and deletes existing gateway ports, and adds new gateway ports.

1. Go to **SIP Gateway Port**.
2. Choose a site.
3. View the list of existing gateway ports.
4. Choose an option:
   - To delete an existing port, select the checkbox for the relevant ports, and click **Delete**.
   - To update an existing port, click the port name in the list. Update as required. Save your changes.
   - To add a new port, go to step 5.
5. To add a new port, click **Add**. Fill out the form with the new port details:
   - At **LBO Gateway Name**, choose the gateway where you will add the new port.
   - At **Port Number** enter a port number (free text field).
   - Choose a port type, either *T1* or *E1*, and optionally, add a description.

     Note: If you've chosen a *T1* port:
     - Choose a **Framing** option, either *sf* (super frame) or *esf* (extended super frame).
     - Choose a **Line Coding** option, either *b8zs* or *ami*.

     If you've chosen `E1` port:
     - Choose a **Framing** option, either *crc4* or *no-crc4*.
     - **Line Coding** defaults to *hdb3*, which is the only option for this port type.

   - At **Clock Source**, choose either *line* or *internal*.
   - Choose **Protocol Side**, either *Network* or *User*.
   - Choose a **ISDN Switch Type**.
   - Choose **ISDN B-Channel Number Order**, either *ascending* or *descending*.
   - Define whether to set calling/called party number NOA for outgoing calls.
6. Save your changes.

   A workflow pushes the data, and triggers the Command Builder. The commands for setting up the port are available via the **Commands** page. You can paste these commands into the gateway. Commands for updates and deletes can also be found in the **Commands** log.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick add SIP gateway

Overview

Quick Add SIP Gateway allows you to configure a new SIP gateway at the site level, with minimum details. Saving the form triggers a background process that uses the information you provide, along with configuration templates, and automatically creates the required elements at the correct hierarchies:

At customer level	Saving a Quick Add SIP Gateway configuration creates and adds the following elements at the customer level: • The IOS device • The SIP trunk • The SIP LBO gateway
At site level	Saving a Quick Add SIP Gateway configuration performs these actions at the site level: • The gateway is associated to the site • The E1/T1 Ports are added (optional)

Note:

- Quick Add SIP Gateway does not support incremental configuration of the gateway. Activities such as adding additional ports must be done via the appropriate menus.
- While the Quick Add SIP Gateway tool automates the creation and configuration of elements required for the SIP gateway at the customer and site level, you can manually create these elements, if required. For example, to associate an unused or old gateway that was previously associated with a site, to a new site.

  In this case, you would need to add these elements at customer and site hierarchies, as follows:

  - At customer level:
    - Add the IOS device
    - Add the SIP trunk
    - Add the SIP LBO gateway
  - At the site level:
    - Associate the gateway to the site
    - Add the E1/T1 ports (optional)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add SIP gateway and associated components

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, choose the site.
2. Go to **Quick Add SIP Gateway**.
3. On the **IOS Device** tab, configure IOS gateway details:
   - Mandatory. Enter a **IOS Device Name** or select an existing IOS device from the drop-down.
   - Optional. Add a description for the IOS device.
   - At **Network Addresses** you must create two network addresses:
     - To create the first network address, at **Address Space**, choose **SERVICE_PROVIDER_SPACE**, then enter the associated **IPv4 Address**.

       Note: This is used to specify the IP address of the IOS device, if one is created.

     - Create the second network address (as seen from the Unified CM) for the SIP Trunk to use. In this case, at **Address Space**, choose **APPLICATION_SPACE**.

       Important: The second network is address is critical as it is used to specify the IP address of the SIP trunk.

4. On the **SIP Trunk** tab, choose a SIP trunk template.

   Note:
   - The SIP trunk templates assembles data (such as IPv4) from the details you specified in the **Network Addresses** section of the **IOS Device** tab in the previous step.
   - The **Configuration Templates** list displays available templates. Type *siptrunk* in the **Name** column to filter the list. Existing sample SIP trunk templates can be cloned, modified, and saved under a new name.

5. On the **SIP Gateway** tab, complete the relevant fields, for example:

SIP Gateway Name	Mandatory.
Run On Every Node	Enabled by default. Defines whether the Unified CM hosts the trunk everywhere.
Enable Command Builder	Enabled by default.

   Note: **Country** is a read-only field that displays the location of the SIP gateway. The value in this field (the country) is the same as the site to which the SIP gateway will be associated.

6. Optional. On the **Ports** tab, add an E1 or T1 port to the gateway:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Enter the required T1 or E1 **Port Number**, and a description.

  Note: Port numbers should be formatted as follows: `x/x/x` (unit/subunit/port)

- Choose a **Port Template**. The template drives the values defined for E1 and T1.

  Note: Existing sample port templates can be cloned, modified, and saved under a new name.

7. Click **Save**.

   Once the transaction completes:

   - The IOS Device, SIP Trunk, SIP LBO Gateway are created at the customer level
   - The SIP LBO Gateway is associated to the site
   - The optional E1 and T1 ports are created at the site level

Related topics

- *Add an IOS device*

SIP local gateway

Tip: *Use the Action search to navigate Automate*

Add a SIP local gateway

This procedure adds a SIP local gateway.

Pre-requisites

- Configure an IOS Device at the customer hierarchy node.
- Configure an NDL containing the CUCM for the customer.
- Configure a SIP trunk at the customer hierarchy node.

A SIP Local Gateway is a logical gateway running on a physical IOS device.

Add SIP local gateway

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer for which you are setting up the SIP Local Gateway.
3. Go to **SIP Local Gateways**, then click the Plus icon (+) to add a new record.
4. Configure settings for at least the mandatory fields. See *SIP local gateway settings*.
5. Click **Save**.

   View transaction progress and details in the Transaction Logs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The SIP Local Gateway appears in the **SIP Local Gateway** list view.
- The HcsAddSipLocalGwEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
- The HcsAddSipLocalGwDialPeerEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each dial peer.

Related topics

- Transaction Logging and Audit in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP local gateway settings

Field	Description
Name *	Mandatory. Fill out a name for the SIP Local Gateway.
Description	Enter a description for the SIP Local Gateway.
IOS Device *	Mandatory. Choose the IOS Device on which the SIP Local Gateway is located. Note: An IOS Device can have only one SIP Local Gateway. Once selected, the IOS Device cannot be changed.
Country *	Mandatory. Choose the country where the SIP Local Gateway is. The country selected must be the same country as the Site to which the SIP local gateway will be associated.
CUCM Publisher *	Mandatory. Choose the CUCM Publisher. All CUCM Publishers that are in the customer's NDL are displayed. The chosen CUCM Publisher must be the same as the CUCM Publisher in the NDL for the Site to which the SIP local gateway will be associated.
SIP Trunk *	Mandatory. Choose the SIP Trunk from those available on the CUCM Publisher. Note: Only SIP Trunks configured at the customer hierarchy are available. If the customer uses a shared CUCM, then SIP Trunks must be manually configured at the customer level in VOSS Automate to be selectable here.
Gateway Address	Read-only. The Gateway Address, derived from the selected SIP Trunk. Note: If a SIP Trunk has multiple destination addresses, only the first one is used.
Gateway Port	Read-only. Gateway Port, is derived from the selected SIP Trunk.
Run on Every Node	Read-only. Defines whether call processing is distributed across all CUCM subscriber nodes. The value comes from the selected SIP Trunk.
Dial Peer Info	If the **Run on Every Node** is cleared then the Call Manager Group members are displayed in priority order. If the **Run on Every Node** checkbox is selected, then all CUCM nodes in the cluster are displayed, but without priority.
Enable Command Builder *	Select this check box to have Command Builder generate commands when SIP Local Gateway is added, deleted, or modified. Default = Selected. If this is checked and the Override below is also checked, then E164-to-DN disassociation will fail if it exceeds the default limit. This setting should therefore be un-selected for disassociation to succeed in this case.
Override Voice Translation Limit ** Warning may invalidate Command Builder Configuration**	Select this checkbox to override Voice Translation Limit if E164 associations exceed 80. Default = Cleared. Note that once checked and saved, then un-checking will not reset the limit to 80. Contact VOSS support or a high level admin to reset it to 80.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Update SIP local gateway

This procedure updates a SIP local gateway. You can also perform this task if you have updated the SIP Trunk associated with the SIP Local Gateway.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer whose SIP Local Gateway you are updating.
3. Go to **SIP Local Gateways**.
4. Click the SIP Local Gateway to update.
5. On the **SIP Local Gateways** page, only the following values can be modified:

   Note: The SIP trunk can be updated on the CUCM **SIP Trunks** page.

Field	Description
Name	Enter a name for the SIP Local Gateway. This field is mandatory.
Description	Enter a description for the SIP Local Gateway.
Enable Command Builder	Select this check box to have Command Builder generate commands when SIP Local Gateway is added, deleted, or modified.

6. Click **Save**.

   View transaction progress and details in the Transaction Logs.

   - If you changed the SIP Local Gateway name, the Gateway Name for generated commands is updated in the IOS Commands log.
   - If the **Run on Every Node** checkbox is selected for SIP Trunk, the HcsUpdateSipLocalGw1EVT and HcsUpdateSipLocalGw1EVT events are generated.

     If the **Enable Command Builder** checkbox is selected, the IOS Command Builder generates the default IOS commands associated with the events.

Related topics

- Transaction Logging and Audit in the Core Feature Guide.

Delete SIP local gateway

1. Log in as provider, reseller, or customer administrator.
2. Go to IOS **SIP Local Gateways**.
3. Select the SIP Local Gateway that you want to delete, then click the **Delete** icon on the details page.

   View transaction progress and details in the Transaction Logs. See *Transaction logging and audit*

   - The SIP Local Gateway is removed from the **SIP Local Gateway** list view.
   - The HcsDeleteSipLocalGwEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The HcsDeleteSipLocalGwDialPeerEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each dial peer.
- If the SIP Local Gateway is associated with any sites, the events for disassociating a SIP Local Gateway from a Site are generated for each associated site. See “Disassociate a SIP Local Gateway from a Site” for details.

Related topics

- Transaction Logging and Audit in the Core Feature Guide.

Associate or disassociate SIP local gateway to a site

provider

Tip: *Use the Action search to navigate Automate*

Overview

Associating a SIP local gateway to a site triggers registered IOS Builder events and triggers registered dial plan schema group custom workflows. Only SIP local gateways that share a common Cisco UCM cluster as specified in the site NDL and have the same country as the site can be associated with a site hierarchy node.

Note:

- Sites with the same area code(s)

  In this scenario, there are two possibilities:

  - All sites share the same TDM trunks to the provider – this is supported with the default IOS Command Builder templates
  - Each site has its own TDM trunk to the provider – this is not supported with the default IOS Command Builder templates
- Sites with different area codes

  In this scenario, it is unlikely the sites will be sharing the same TDM trunks. However even if they do share the same TDM trunks, it is not currently supported without having to manually modify the default IOS Command Builder templates. If the admin does deploy a shared LBO gateway to two or more sites with different area codes using the default IOS Command Builder templates, calls from one of these sites to a number that is in the same area code as another site sharing the same trunk will be treated as a local/subscriber call.

  A site with its own trunk is also not supported without modifying the default IOS Command Builder templates.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Associate a SIP local gateway to a site

This procedure associates a SIP local gateway with a site.

Prerequisites:

- The SIP local gateway and the target site must be in the same country.
- The SIP local gateway and the target site must have the same CUCM Publisher.
- The target site must have a site dial plan deployed.

Note:

- A SIP local gateway can be associated with multiple sites given the prerequisite conditions are met.
- A site can be associated with multiple SIP local gateways given the prerequisite conditions are met.
- If a SIP local gateway is deleted, all existing site associations are disassociated.
- If a site is deleted via the **Delete Site** page and at least "Remove Dial Plan Items" is selected, all SIP local gateway associations for that site are disassociated.
- If a site dial plan is deleted, all SIP local gateway associations are disassociated.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy to the site for which you want to associate a SIP local gateway.

   If you do not have the path set to a site, you are prompted to select the site.
3. Go to **Associate SIP Local Gateway**.
4. Click the Plus icon (+) to add a record.
5. Select the SIP local gateway you want to associate with the site from the menu.

   Only SIP local gateways that have the same country and CUCM Publisher configuration as the site are available to be selected.
6. Click **Save**. View transaction progress and details in the Transaction Logs. See *Transaction logging and audit*
   - The SIP local gateway appears in the **Associate SIP Local Gateway** list view.
   - The HcsSipLocalGwAddSitePstnEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - For each Area Code defined on the target site's dial plan, the HcsSipLocalGwAddSiteAreaCodeEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the site has an existing E.164 to DN Association (N to N), either the HcsSipLocalGwAddE164AssociationEVT (for N to N) or the HcsSipLocalGwAddMultiE164AssociationEVT event (for N to 1) is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the site has an existing Voice Mail Pilot Number Association, the HcsSipLocalGwAddVoiceMailPilotNumberEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- If the Dial Plan Schema Group that is associated with the customer dial plan has the associateLboGateway custom workflow provisioned, the associateLboGateway custom workflow is executed.
- The Site association to the SIP local gateway creates a Route Group with the SIP Trunk created and associated to the SIP local gateway.

Disassociate a SIP local gateway from a site

This procedure disassociates a SIP local gateway from a site.

Note: Prior to Automate, IOS commands generated at a site were lost when the site was deleted.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Go to **Associate SIP Local Gateway**.
3. Select the checkbox adjacent to the SIP local gateway you want to disassociate, then click **Delete**.
   - The SIP local gateway association is removed from the **Associate SIP Local Gateway** list view.
   - The HcsSipLocalGwDelSitePstnEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - For each Area Code defined on the site's dial plan, the HcsSipLocalGwDelSiteAreaCodeEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event. If Area Codes are shared across multiple sites and associated with the same gateway, the commands are generated only when the gateway is disassociated from the last site that shares the Area Code.
   - If the site has an existing E.164 to DN Association, either the HcsSipLocalGwDelE164AssociationEVT (for N to N) or HcsSipLocalGwDelMultiE164AssociationEVT (for N to 1) event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the site has an existing Voice Mail Pilot Number Association, the HcsSipLocalGwDelVoiceMailPilotNumberEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the Dial Plan Schema Group that is associated with the customer dial plan has the unassociateLboGateway custom workflow provisioned, the unassociateLboGateway custom workflow is executed.

Note: When a SIP local gateway is disassociated from a site because the site is deleted, IOS commands are copied from the site to the customer level before the site is deleted. Use the Action search to go to the IOS **Commands** page to view copied IOS commands.

Copyright © 2025 VisionOSS Limited. All rights reserved.

IOS gateway manual configuration

This procedure adds a PRI trunk to connect to the PSTN.

Automate does not generate any controller, interface, or dial peer commands for the gateway. This has to be manually added after the command builder has generated the gateway configuration.

Perform these steps:

1. Configure PRI on a channelized E1 or T1 controller with the following commands:
   a. controller <T1 or E1><slot/port>

      where slot/port is the controller location in the gateway

   b. framing <esf | sf or crc4 | non crc4>

      esf/sf for T1 and crc4/non crc4 for E1

   c. linecode <b8zs | ami or bdb3 | ami>

      b8zs/ami for T1 and hdb3/ami for E1

   d. clock source <internal/line>
   e. pri-group timeslots <1-24 | 1-31>

      Use all channel on the trunk 1-24 for T1 and 1-31 for E1

2. Configure Serial Interface with the following commands:
   a. interface serial <slot/port>:<23 | 15>

      slot/port similar to the above for controller and use 23 for T1 and 15 for E1

   b. no ip address
   c. encapsulation hdlc
   d. isdn protocol-emulate <network | user>
   e. isdn switch-type <switch-type>

      See IOS documentation for supported switch types.

   f. isdn incoming-voice voice
   g. isdn bchan-number-order <ascending | descending>
   h. no cdp enable

3. Configure POTS dial peer with the following commands:
   a. dial-peer voice 95 pots
   b. translation-profile incoming <91XX>

      For incoming call:

      - use 9111 when both called and calling number have NOA
      - use 9121 when called number does not have NOA but Calling number has NOA
      - use 9112 when calling number does not have NOA but Called number has NOA
      - use 9122 when both called and calling number do not have NOA

   c. translation-profile outgoing <90XX>

      For outgoing call:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- use 9111 when both called and calling number have NOA
- use 9121 when called number does not have NOA but Calling number has NOA
- use 9112 when calling number does not have NOA but Called number has NOA
- use 9122 when both called and calling number do not have NOA

d. destination-pattern 90[1-9]T

e. incoming called-number .

f. no digit-strip

g. direct-inward-dial

h. port <slot/port>:<23 | 15>

   Similar to what is configured for serial interface

i. no register e164

Example IOS gateway manual configuration

```
controller T1 0/0/0
framing esf
linecode b8zs
clock source line
pri-group timeslots 1-24

interface serial 0/0/0:23
no ip address
encapsulation hdlc
isdn protocol-emulate user
isdn switch-type  primary-net5
isdn incoming-voice voice
isdn bchan-number-order descending
no cdp enable

dial-peer voice 95 pots
translation-profile incoming 9111
translation-profile outgoing 9011
destination-pattern 90[1-9]T
incoming called-number .
no digit-strip
direct-inward-dial
port 0/0/0:23
no register e164
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP Gateways

Translation and Transformation

Cisco UCM translation patterns

Tip: *Use the Action search to navigate Automate*

Overview

The Cisco Unified Communications Manager (UCM) default dial plan translation patterns are deployed as part of the default dial plan translation patterns that ship with the Automate template package.

This section describes how to update these default dial plan translation patterns. For example, you may want to make your default national number translation patterns more restrictive. Or you may want to deploy additional, customer-specific translation patterns (with custom blocking plans that aren't defined in the standard country dial plan schema, for instance).

Caution: Provider deployments. The Cisco HCS default dial plan includes most common translation patterns and route patterns, which are typically added automatically when provisioning a customer dial plan, site dial plan, and voice mail service.

Ensure you have a full understanding of the Cisco HCS dial plan before using Automate to update translation patterns and route patterns. For details, see the "Provider HCS Dial Plan Management Support Guide".

Configure Cisco UCM translation patterns

This procedure updates the UCM translation patterns that are provisioned by the dial plan schema and adds new translation patterns from Automate that are not part of the standard dial plan package.

Note: For more information on UCM translation patterns, see the "Cisco Unified Communications Manager Administration Guide, Release 10.0(1)".

1. Log in as Provider, Reseller, or Customer administrator.
2. Choose the hierarchy where you want to add or edit the translation pattern.
3. Go to **Translation Patterns**.
4. Choose an option:
   - Add a new translation pattern? Click the Plus icon (+) to add a new record, then go to Step 5.
   - Edit an existing translation pattern? Click on the pattern to be updated and go to Step 6.
5. On the **Pattern Definition tab**, from the **CUCM** drop-down, choose the hostname, domain name, or IP address of the Cisco UCM to which you want to add the translation pattern.

   Note: This drop-down displays only when you're adding a translation pattern. When adding a translation pattern at a hierarchy above the site level, the drop-down displays UCMs located at the

Copyright © 2025 VisionOSS Limited. All rights reserved.

hierarchy node where you're adding the translation pattern, and all UCMs in hierarchies above this hierarchy node.

When adding a translation pattern at a site, the UCM in the **CUCM** drop-down list is the UCM in the site's Network Device List (NDL). If the site does not have an NDL, or the NDL at the site does not have a UCM, then the drop-down list is empty and a translation pattern can't be added to the site.

6. On the **Pattern Definition tab**:
   - Mandatory. In the **Translation Pattern** field, fill out a unique name for the translation pattern, (or update the name if you're editing the translation pattern).

     Note: The name must be unique, and can include numbers and wildcards. Spaces aren't allowed. For example, enter 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +.

   - Mandatory. In the **Partition** field, fill out a unique name for the route partition (or update the name if you're editing the translation pattern).
   - In the **Description** field, fill out an optional description for the translation pattern and route partition.

     Note: The description can include up to 50 characters in any language, but it can't include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

7. Fill out at least the mandatory fields on each tab/panel of the **Translations Patterns** page.

   Tip: Use the Corresponding UCM attribute information provided in the tables to manually verify in the UCM GUI that fields have been mapped correctly.

   - *Pattern Definition Tab*
   - *Calling Party Transformations Tab*
   - *Connected Party Transformations Tab*
   - *Called Party Transformations Tab*
8. Save your changes.

Translation patterns settings

This page adds and edits UCM translation patterns.

Tip: *Use the Action search to navigate Automate*

You can select the following tabs on this page:

- *Pattern Definition Tab*
- *Calling Party Transformations Tab*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *Connected Party Transformations Tab*
- *Called Party Transformations Tab*

Pattern Definition Tab

Option	Description
MLPP Precedence *	From the drop-down menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this translation pattern: • Executive Override - Highest precedence setting for MLPP calls. • Flash Override - Second highest precedence setting for MLPP calls. • Flash - Third highest precedence setting for MLPP calls. • Immediate - Fourth highest precedence setting for MLPP calls. • Priority - Fifth highest precedence setting for MLPP calls. • Routine - Lowest precedence setting for MLPP calls. • Default - Does not override the incoming precedence level but rather lets it pass unchanged. Default: Default Corresponding UCM attribute: MLPP Precedence.
Route Class *	From the drop-down menu, choose a route class setting for this translation pattern: • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data The route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. The Default setting uses the existing route class of the incoming call. You can use non-default route class settings to translate an inbound T1 CAS route class digit into a Cisco UCM route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration. If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class. Default: Default Corresponding UCM attribute: Route Class.
Calling Search Space	From the drop-down menu, choose the calling search space for which you are adding a translation pattern, if necessary. Default: None Corresponding UCM attribute: Calling Search Space.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call, select the Use Originator's Calling Search Space check box. If the originating device is a phone, the originator's calling search space is a result of device calling search space and line calling search space. Whenever a translation pattern chain is encountered, for subsequent lookups Calling Search Space is selected depending upon the value of this check box at current translation pattern. If you select the Use Originator's Calling Search Space check box at current translation pattern, then originator's Calling Search Space is used and not the Calling Search Space for the previous lookup. If you clear the Use Originator's Calling Search Space check box at current translation pattern, then Calling Search Space configured at current translation pattern is used. Default: Clear Corresponding UCM attribute: Use Originator's Calling Search Space.
Block this pattern	Indicates whether you want this translation pattern to be used for routing calls (such 8[2-9]XX) or for blocking calls. Default: Clear (meaning translation pattern is used for routing calls). Corresponding UCM attribute: Block this pattern.
Block Reason	If you click Block this pattern radio button above, you must choose the reason that you want this translation pattern to block calls. From the drop-down menu, choose one of: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded Default: No Error Corresponding UCM attribute: <entry box next to Block this pattern>.
Provide Outside Dial Tone	Outside dial tone indicates that UCM routes the calls off the local network. Select this check box for each translation pattern that you consider to be off network. Default: Selected Corresponding UCM attribute: Provide Outside Dial Tone.
Urgent Priority	If the dial plan contains overlapping patterns, UCM does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Select this check box to interrupt interdigit timing when UCM must route a call immediately. Default: Clear Corresponding UCM attribute: Urgent Priority.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Do Not Wait for Interdigit Timeout on Subsequent Hopes	When you select this check box along with the Urgent Priority check box and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), UCM does not start the interdigit timer after it matches any of the subsequent patterns. Note: UCM does not start the interdigit timer even if subsequent patterns are of variable length or if overlapping patterns exist for subsequent matches. Whenever you select the Do Not Wait For Interdigit Timeout On Subsequent Hops check box that is associated with a translation pattern in a translation pattern chain, UCM does not start the interdigit timer after it matches any of the subsequent patterns. Note: UCM does not start interdigit timer even if subsequent translation patterns in a chain have Do Not Wait For Interdigit Timeout On Subsequent Hops check box cleared. Default: Clear Corresponding UCM attribute: Do Not Wait for Interdigit Timeout On Subsequent Hops.
Route Next Hop By Calling Party Number	Select this check box to enable routing based on the calling party number, which is required for call screening based on caller ID information to work between clusters. Default: Clear Corresponding UCM attribute: Route Next Hop By Calling Party Number.

Calling Party Transformations Tab

Option	Description
Use Calling Party's External Phone Number Mask	Select the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. Default: Default Corresponding UCM attribute: Use Calling Party's External Phone Number Mask.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is cleared, no calling party transformation takes place. Default: None Corresponding UCM attribute: Calling Party Transform Mask.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding UCM attribute: Prefix Digits (Outgoing Calls).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Line ID Presentation *	UCM uses calling line ID presentation/restriction (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party phone number on the called party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change calling line ID presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling number. • Restricted - Choose if you want Unified CM to block the display of the calling number. For more information about this field, see topics related to calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Note: Use this parameter and the Connected Line ID Presentation parameter, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to configure call display restrictions. Together, these settings allow you to selectively present or restrict calling and/or connected line display information for each call. See topics related to device profile configuration settings and phone settings for information about the Ignore Presentation Indicators (internal calls only) field, and for more information about call display restrictions, see topics related to call display restrictions in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Line ID Presentation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Name Presentation *	Unified CM uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party name on the called party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change calling name presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling name information. • Restricted - Choose if you want Unified CM to block the display of the calling name information. For more information about this field, see calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Name Presentation.
Calling Party Number Type *	Choose the format for the number type in calling party directory numbers. Unified CM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of: • Unified CM - the Unified CM sets the directory number type. • Unknown - The dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user, using the shortened user name. Default: Cisco UCM Corresponding UCM attribute: Calling Party Number Type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Party Numbering Plan *	Choose the format for the numbering plan in calling party directory numbers. Unified CM sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of: • Unified CM - Use when the Unified CM sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown. Default: Unified CM Corresponding Unified CM Attribute: Calling Party Numbering Plan.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Connected Party Transformations Tab

Option	Description
Connected Line ID Presentation *	Unified CM uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party phone number on the calling party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change the connected line ID presentation. • Allowed - Choose if you want to display the connected party phone number. • Restricted - Choose if you want Unified CM to block the display of the connected party phone number. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Line ID Presentation.
Connected Name Presentation *	(CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party name on the calling party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change the connected name presentation. • Allowed - Choose if you want to display the connected party name. • Restricted - Choose if you want Unified CM to block the display of the connected party name. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Name Presentation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Called Party Transformations Tab

Option	Description
Discard Digits	Choose the discard digits instructions that you want to be associated with this translation pattern. See topics related to discard digits instructions in the Cisco Unified Communications Manager System Guide for more information. Default: None Corresponding Unified CM Attribute: Discard Digits.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed. Default: None Corresponding Unified CM Attribute: Called Party Transform Mask.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#);the international escape character +; and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).
Called Party Number Type *	Choose the format for the number type in called party directory numbers. Unified CM sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CMUnified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of: • Unified CM - Use when the Unified CM sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user, using a shortened user number Default: Cisco UCM Corresponding UCM attribute: Called Party Number Type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Called Party Numbering Plan *	Choose the format for the numbering plan in called party directory numbers. Unified CM sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of: • Unified CM - Use when the Unified CM sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown. Default: Unified CM Corresponding Unified CM Attribute: Called Party Numbering Plan.

Calling search spaces

Tip: *Use the Action search to navigate Automate*

Overview

A Calling Search Space (CSS) comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

Add and edit calling search spaces

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Go to **Calling Search Spaces**.
3. Choose the relevant hierarchy.
4. Choose an option:
   - To add a new calling search space, click **Add**, then go to step 5.
   - To edit an existing calling search space, click on the line item in the table. Go to step 6.
5. In the popup, select from the pull-down the network device list (NDL) to which you are adding the calling search space, and click **OK**.

   Note: The NDL popup will only appear when you are adding a new calling search space. If you are updating an existing calling search space, go to Step 6.

Copyright © 2025 VisionOSS Limited. All rights reserved.

If you are adding the calling search space to a Site hierarchy node, the NDL popup will not appear. You will go right to the Calling Search Spaces add page using the NDL associated to the site.

6. From the **Calling Search Spaces** page, modify the following fields as required.

Option	Description
Name (Mandatory)	Enter a name in the field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each calling search space name is unique to the system. Note Use concise and descriptive names for your calling search spaces. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a calling search space. For example, CiscoDallasMetroCS identifies a calling search space for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas. Default value: None
Description	Enter a description in the field. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (), or angle brackets (<>). Default value: None
Route Partitions	Click the Add (+) button to add a partition to the calling search space. Repeat as necessary to add multiple partitions to the calling search space.
Partition Name	Click the drop-down list and select a partition to add to the calling search space. Click **Add (+)** to add another partition to the Route Partitions list. Repeat as necessary to add multiple partitions to the list. Click the **Remove (-)** button to remove a partition from the list. Click the up and down arrow buttons to change the order of a partition in the list.
Partition Index	Enter the priority number for this partition in the calling search space. The smaller the integer, the higher the priority.

The following table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length.

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86
. . .	. . .
10 characters	46
15 characters	32

Copyright © 2025 VisionOSS Limited. All rights reserved.

7. Click **Save**. The calling search space appears in the list.
   - To modify any of these properties, click the item in the list, make your changes, and click **Save**.
   - To delete a calling search space, check the box to the left of the Name column in the group list, and click **Delete**.

Note: When selecting an existing CSS with a partition associated and cloning this instance for modification, the new CSS will by default show the partition populated with this associated partition.

Calling party transformation patterns

Tip: *Use the Action search to navigate Automate*

Overview

Parameters on the **Calling Party Transformation Patterns** page provide appropriate caller information using the Calling Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

You use calling party transformation patterns with the calling party normalization feature.

Configure calling party transformation patterns

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Go to **Calling Party Transformation Patterns**.
3. Set the hierarchy path to the relevant level.
4. Choose an option:
   - To add a new calling party transformation pattern, click **Add**, then go to step 5.
   - To edit an existing calling party transformation pattern, click on the line item in the table. Go to step 6.
5. In the popup, select from the drop-down the network device list (NDL) to which you are adding the calling party transformation pattern, and click **OK**.

   Note: The NDL popup will only appear when you are adding a new calling party transformation pattern. If you are updating an existing pattern, go to Step 6.

   If you are adding the calling party transformation pattern to a Site hierarchy node, the NDL popup will not appear. You will go right to the Calling Party Transformation Pattern add tabs using the NDL associated to the site.
6. From the **Pattern Definition** tab, modify the following fields as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Pattern (Mandatory)	Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and +, which represents the international escape character +. Note Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. Default value: None
Partition	If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box. Note Configure transformation patterns in different non-null partitions rather than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, Cisco Unified Communications Manager ignores the patterns in null partitions. Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description of the transformation pattern.
Numbering Plan	Choose a numbering plan.
Route Filter	If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.
MLPP Preemption Disabled	Check this box to make the numbers in a transformation pattern non-preemptable.

7. From the **Calling Party Transformations** tab, modify the following fields as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Use Calling Party's External Phone Number Mask	Choose On from the drop-down list if you want the full external phone number to be used for calling line identification (CLID) on outgoing calls. Choose Off or Default if you do not want to use the full external phone number for CLID on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
Digit Discards	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the Digit Discards field is blank, the Prefix Digits field is blank, the Calling Party Transformation Mask field is blank, and Use Calling Party's External Phone Number Mask is set to Off or Default, no calling party transformation takes place.
Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. Note The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this route pattern. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Party Number Type	Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non national type numbering plan. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user by using a shortened user number.
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

8. Click **Save**. The calling party transformation pattern appears in the list.
   - If you need to modify any of these properties, click the item in the list, make your changes, and click **Save**.
   - To delete a calling party transformation pattern, select the checkbox adjacent to the **Name** column in the group list, then click **Delete**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure called party transformation patterns

Tip: *Use the Action search to navigate Automate*

Overview

Parameters on the **Called Party Transformation Patterns** page provide appropriate caller information by using the Called Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

Configure called party transformation patterns

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Go to **Called Party Transformation Patterns**.
3. Set the hierarchy path to the relevant level.
4. Choose an option:
   - **Add a new called party transformation pattern**? Click **Add**, then go to step 5.
   - **Edit an existing called party transformation pattern**? Click on the line item in the table. Go to step 6.
5. In the popup, select from the drop-down the network device list (NDL) to which you are adding the called party transformation pattern, and click **OK**.

   Note: The NDL popup will only appear when you are adding a new called party transformation pattern. If you are updating an existing pattern, go to Step 6.

   If you are adding the called party transformation pattern to a Site hierarchy node, the NDL popup will not appear. You will go right to the Called Party Transformation Pattern add tabs using the NDL associated to the site.
6. From the Pattern Definition tab, modify the following fields as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Pattern (Mandatory)	Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. Valid characters include the uppercase letters A, B, C, and D and +, which represents the international escape character +. Note Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. Default value: None
Partition	If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the transformation pattern, choose <None> for the partition. Note Transformation patterns should be configured in different non- NULL partitions than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, the patterns in NULL partitions get ignored. Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description of the transformation pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).
Numbering Plan	Choose a numbering plan.
Route Filter	If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.
MLPP Preemption Disabled	Check this box to make the numbers in a transformation pattern non-preemptable.

7. From the **Called Party Transformations** tab, modify the following fields as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Digit Discards	Choose the discard digit instructions that you want to be associated with this called party transformation pattern.
Called Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#),the international escape character +, and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user, by using a shortened user number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

8. Click **Save**. The called party transformation pattern appears in the list.
   - To modify any of these properties, click the item in the list, make your changes, and click **Save**.
   - To delete a called party transformation pattern, select the checkbox adjacent to the **Name** column in the group list, and click **Delete**.

Cisco UCCX Management

Configure UCCX server

Tip: *Use the Action search to navigate Automate*

Overview

Reseller level and higher administrators can view and manage Cisco Unified Contact Center Express (UCCX) servers, typically from the **Apps Management** menu.

Note:

- Network Device Lists (NDLs) must always be updated to include the UCCX server, even when a single server is used per customer.
- Multiple UCCX servers can be configured for a single customer. In this case, the relevant NDLs be updated with the UCCX server references.
- Cisco Unified Communications Manager (CUCM) server and UCCX server integration should be performed as pre-configuration for this feature to work correctly.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Contact Center*

Add a UCCX server

This procedure adds a UCCX server.

1. Log in as Provider administrator or higher.
2. Choose the relevant hierarchy.

   Note: The UCCX server must be created at the same hierarchy as the CUCM. This is because the application user for the UCCX server is selected from a drop-down that is populated with application users from the CUCM at the same hierarchy.

   If the UCCX is at a hierarchy above or below the CUCM, there are no application users to choose from.

2. Go to the (UCCX) **Servers** page.
3. Click **Add**.
4. Fill out the server details.
   - The current supported **Versions** are 11.x and 12.x.
   - Set the **Application User ID** values of the server. These are CUCM users to be used for agent device association. Typically this would be the RMCM application user (CCX Resource Manager, CUCM Telephony user), but could also include others for call recording and so on.

Run a pull data sync from the UCCX server

Once the UCCX server is added you can run a pull data sync from the server to Automate via the **Sync** page for the UCCX server.

Automate also automatically creates two default Data Sync instances to manage and schedule data synchronization between the device and Automate. These can be seen from the **Data Sync** list view:

SyncUccx-<host>	Use this sync to schedule or manually sync data between the server and Automate.
PurgeUCcx-<host>	Disabled by default to avoid accidental purges. To enable it, change the Sync Type to “Purge Local Resources” from “Pull from Device”, and clear **Disabled Operations**.

Data sync instances are removed automatically when the server is deleted. The purge sync will also be executed on server deletion, thereby removing any configuration from Automate.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Introduction to Webex Contact Center

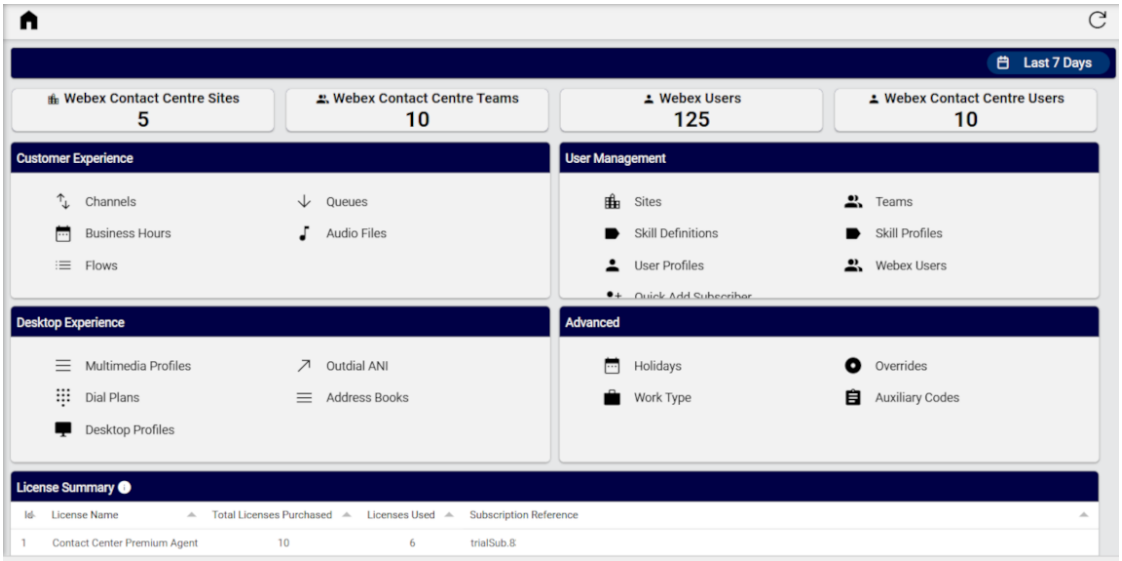
Tip: *Use the Action search to navigate Automate*

Important: The **Webex Organization** setting, **Contact Center Customer**, must be enabled in order to manage a Webex Contact Center in Automate.

If a Cisco Webex service is added to Automate from **Webex Organization** and the setting **Contact Center Customer** is enabled, Automate provides a range of features to manage a Webex Contact Center. In particular, this includes:

- Agent and associated configuration management
  - Agents, Users, Agent Profiles, Teams, Sites
  - Skills, skill profiles
  - Holidays, business hours
  - Address book
  - Contact Service Queue, Entry points, overrides
  - Auxiliary codes
  - Multimedia Profiles
- Integration into Webex User management in Automate
  - Quick Add User

Automate also provides role-based access, menus, and dashboards to view and manage the Webex Contact Center



For continuity, the grouping of functionality on the menus and dashboards follows the format and naming as seen on the Webex Control Hub interface.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Webex Contact Center sync*
- *Webex Contact Center customer experience*
- *Webex Contact Center user management*
- *Webex Contact Center Desktop Experience*
- *Webex Contact Center Advanced*
- *Introduction to Cisco Webex App*

Contact Center

Cisco

Tip: *Use the Action search to navigate Automate*

Overview

Automate provides Day 2 management support for Cisco Unified Contact Center Express (UCCX), and allows administrators to manage and configure agents from a single pane of glass.

A data sync in Automate allows Contact Center device models in Automate to sync to the UCCX server:

- UCCX server management:
  - *Configure UCCX server*
- Day 2 integration:
  - Add a UCCX device to a hierarchy, add entitlement profiles, then configure users as Contact Center agents. Additional management can be performed in Automate, including overbuild. See *Dial plan elements moved to the site hierarchy*
  - *Add a Contact Center agent using Quick Add User*
  - *Add a user* (Contact Center)
- Direct management:
  - *Agents* (`device/uccx/Agent`)
  - *Skills* (associated with competency levels)
  - *Teams* (`device/uccx/Team`)
  - Contact Center Resource Groups (`device/uccx/ResourceGroup`)
  - Contact Center Service Queues (`device/uccx/ContactServiceQueue`)
- Associate agent devices association with CUCM users:

  Admins can specify the agent's controlled device via:
  - Quick Add User
  - Users

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Direct Agent management

  The agent device is associated with the list of CUCM application users specified as part of the UCCX server configuration. The association is kept sync when phones and extension mobility profiles are deleted or replaced.

- Automate management interfaces for UCCX:
  - Manage agent profiles (See *Agent Profiles*)
  - Re-skilling (see: *Re-skill agents*)

    Bulk manage (add, remove) agent skills and competencies via side-by-side transfer boxes for the following:

    * Agents
    * Teams
    * Resource groups

Agents

You can view a list of Contact Center agents that have been synced in, or agents added when adding users at a customer or site, via the **Agents** page.

Note: Agents synced from UCCX but not yet moved to a site may be listed as located at the customer hierarchy.

To add a new Contact Center agent, from the list view click the Plus (+) icon, then on the **Agents** / **New Record** page, choose an agent by their user ID from the **User ID** drop-down.

To view or update an existing Contact Center agent, click on an agent in the list to view the agent's devices and tagged lines or to update the agent. You can manage the following agent properties:

Field	Description
Alias	The agent alias on the device. Note that there are restrictions on allowable characters in the alias.
Type	The agent type, either Agent or Supervisor.
Team	Agents who are not assigned to a specific team are assigned to the Default team.
Resource Group	Optional. Choose a resource group.
Automatic Available	Enabled by default. Defines whether the agent is automatically in an 'available' or 'ready' state after finishing a call and disconnecting.
Skills	Optional. Click the Plus icon to add skills.
Controlled Device	Click the Plus icon to add a device type, either Phone or Extension Mobility. When choosing Phone, you will need to choose the phone name.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Teams

On the **Teams** page you can view a list of Contact Center agent team names, their primary and secondary supervisors, team members, and team availability. From the list view you can add and manage Contact Service Queues.

Note:

- When adding a new team at the Customer level, the NDL must have a reference set up to UCCX, via **Network Device Lists**.
- Agents displayed in the **Available** list are agents that are currently not assigned to any other team, and may be assigned to the team you're working with. An agent can only be assigned to one team at a time.

Contact Center Resource Groups

Contact Center resource groups comprise one or more agent profiles. If you're creating resource groups directly in Automate, you will need to create the resource groups before creating the agent profiles. When creating the agent profiles, you reference the resource group where you want to add the agent profile. Contact service queues can be configured to use resource groups.

To view and manage resource groups for Contact Center agents, go to the **Resource Groups** page.

Skills

Automate allows you to define skills and to assign competency levels to agents with these skills when associating a skill with an agent, agent profile, or skill group in a Contact Service Queue.

To view and manage skills for Contact Center agents, go to the **Skills** page.

Contact Center Service Queues

Incoming contact center calls are placed in a queue and sent to a specific agent based on the queue configuration.

To view and manage contact service queues, go to the **Contact Service Queues** page.

In the **Contact Service Queues** list view you can view, add, and update contact service queues. For example, you can associate a contact service queue with a resource group or skills.

Automate supports the following queue types:

- Chat
- Email
- Voice

If voice, chat, and email Contact Service Queues exist on UCCX, their data is included when a Contact Center server is imported to Automate, and you can manage the queues in Automate.

Note: When choosing queue type `EMAIL`, you will need to fill out details for the following mandatory fields:

- Email Username (`accountUserId`)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Email Password (`accountPassword`)

Agent profiles

Each agent profile specifies:

- Team
- Resource group (agent profiles can be grouped together as resource groups)
- Skill

Note:

- Before creating the agent profile, you will need to define the team, resource group, and skill you wish to associate with the agent profile.
- If you're creating an agent using Quick Add User, you must first create the agent profile.

To view and manage agent profiles, go to the **Agent Profiles**.

Re-skill agents

Re-skilling Contact Center agents involves editing an agent's skills to either add new skills or remove existing skills previously assigned to the agent. You can re-skill one or more agents at a time.

Note: Re-skill is available for agents, teams, and resource groups in the Admin Portal. In the Business Admin Portal, only agent re-skill is supported.

This procedure re-skills agents. To re-skill teams or resource groups, select the relevant menu item via **Contact Center**.

To re-skill agents:

1. In the Admin Portal, select the relevant customer from the organization picker.
2. Go to the **Re-skill Agents** page.
3. On the **Re-skill Agents** page, choose the agents you wish to re-skill (one or more). Select agents in the **Available** field then click the right-pointing arrow to move the agent (or agents) to the **Selected** field, then:
   - To add new skills, click the Plus (+) icon at **Add Skills**, choose a skill, and select a competency level. Repeat this step to add additional skills.
   - To remove existing skills, click the Plus (+) icon at **Remove Skills**, and select the relevant skill from the **Skill** drop-down. Repeat this step to remove additional skills.
4. Click **Save**.
5. On the **Agents** page, click on an agent you re-skilled to verify that their new skills are added and their removed skills no longer display.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Example setup workflow for Contact Center

This section describes an example workflow for configuring Contact Center:

1. On the UC apps, configure CUCM and UCCX server integration (this is done directly on the UC apps).
2. At the relevant Customer level in the hierarchy, add a new UCCX server.
   a. Use UCCX admin user credentials.
   b. Select the list of CUCM application users to be used for agent device association.
3. Update the Network Device List (NDL):
   a. Reference the relevant CUCM and UCCX servers in the NDL.
   b. Set this NDL for each site where agents will be managed.
4. Sync the existing configuration from the UCCX server, either directly from the UCCX server page, or via the **Data Sync** menu.
5. Create agent profiles. To do this, go to **Agent Profiles**.
6. Create a new - either add the agent directly via the **Agents** page, or use Quick Add User.

Provision a Contact Center agent

This procedure provisions a user as a Contact Center agent.

Pre-requisites:

- The user you wish to provision as a Contact Center agent must be assigned an entitlement profile that has Contact Center service enabled.

Perform these steps:

1. In the Admin Portal, go to **Users**.
2. From the **Users** list, click on the user to be provisioned as a Contact Center agent.
3. On the user's management page, select the **Contact Center** tab.

   Note: This tab is visible only if the user is assigned an entitlement profile with Contact Center service enabled.

4. Provision the user as a Contact Center agent.

Webex Contact Center sync

Overview

The default Webex Contact Center sync (`SyncSparkCXDataSync`) that is used to sync Webex Contact Center data and is available from the Data Sync list applies:

- **Model Type List**: `SparkCXDataAllMTL`
- **Synchronization Order**: `SparkCXDataSyncOrder`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default synced models

The following Webex Contact Center device model instances are synced:

```
device/spark/CXAddressBook
device/spark/CXAudioFile
device/spark/CXWorkType
device/spark/CXAuxiliaryCode
device/spark/CXOverrides
device/spark/CXBusinessHours
device/spark/CXContactServiceQueue
device/spark/CXDialPlan
device/spark/CXEntryPoint
device/spark/CXFlow
device/spark/CXHolidayList
device/spark/CXMultimediaProfile
device/spark/CXOutdialANI
device/spark/CXSite
device/spark/CXSkill
device/spark/CXSkillProfile
device/spark/CXTeam
device/spark/CXUser
device/spark/CXDesktopProfile
device/spark/CXUserProfile
```

Exclusion list

This list type contains an *exclusion list*, that is, all device model instances that are *not* are synced.

```
device/spark/ActivateDevice
device/spark/Announcements
device/spark/AutoAttendants
device/spark/CallParkExtensions
device/spark/CallParkGroup
device/spark/CallPickup
device/spark/Device
device/spark/DeviceConfig
device/spark/DialPlans
device/spark/Floor
device/spark/Group
device/spark/HuntGroup
device/spark/License
device/spark/Location
device/spark/LocationCallingDetails
device/spark/LocationFloor
device/spark/Number
device/spark/Organization
device/spark/Place
device/spark/Role
device/spark/Room
device/spark/RouteGroups
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
device/spark/Schedules
device/spark/SupportedDevices
device/spark/Team
device/spark/Trunks
device/spark/User
device/spark/UserConfig
device/spark/WholesaleCustomer
device/spark/WholesaleSubscriber
device/spark/WorkspaceCallSettings
device/spark/WorkspaceLocation
device/spark/WorkspaceLocationFloor
```

Sync existing Cisco Webex Contact Center data

Execute **SyncSparkCX[Customer]** via the **Data Sync** page to run a sync.

Synced data is reflected in the transaction log entries, for example:

```
"Execute Data Sync",
"Import Spark",
"Update Local Spark Cx Address Book",
"Update Local Spark Cx Audio File",
"Update Local Spark Cx Auxiliary Code",
"Update Local Spark Cx Business Hours",
"Update Local Spark Cx Contact Service Queue",
"Update Local Spark Cx Desktop Profile",
"Update Local Spark Cx Dial Number",
"Update Local Spark Cx Dial Plan",
"Update Local Spark Cx Entry Point",
"Update Local Spark Cx Flow",
"Update Local Spark Cx Outdial Ani",
"Update Local Spark Cx Overrides",
"Update Local Spark Cx Site",
"Update Local Spark Cx Skill Profile",
"Update Local Spark Cx Team",
"Update Local Spark Cx User",
"Update Local Spark Cx User Profile",
"Move Spark Cx Address Book",
"Move Spark Cx Desktop Profile",
"Move Spark Cx Team",
"Move Spark Cx User",
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Webex Contact Center customer experience

Tip: *Use the Action search to navigate Automate*

Overview

This collection of features provides a single view of customer-specific functionality and reflects the layout in the Webex Control Hub.

Channels

Channels can be managed in Automate.

- An Inbound or Outbound **Entry Point Type** is selected for a channel:
  - Inbound: initial landing place for a customer contact.
  - Outbound: the outdial point provisioned for outdial customer calls.
- An endpoint **Timezone** can be selected for the channel.
- A **Channel Type**: Telephony, Email, Chat or Social Channel is selected for the channel.

Queues

Queues can be managed in Automate.

A **Queue Type** (Inbound, Outbound) and **Channel Type** (Telephony, Email, Chat or Social Channel) is selected for a queue.

For outbound queue types, the channel types defaults to TELEPHONY and the Queue Routing Type is the agent who has been available for the longest time in all teams assigned to the queue.

Business Hours

Business hours can be managed in Automate and are used to define one or more shifts containing for example regular work hours, peak hours, off-peak hours and required for the operation of a specific contact center.

These are defined by working hours, a selected holiday list and overrides to working hours.

For the management of holidays and overrides, see: *Webex Contact Center Advanced*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Audio prompts

Audio prompts can only be imported but not created or edited in Automate.

These are audio files containing for example predefined chat responses and music on hold.

Flows

Call flows can only be imported but not created or edited in Automate.

The flows are designed on the Webex Control Hub Flow Designer and allow for the routing of real-time calls through the system, how agents are assigned to calls and what occurs at each stage of the process. This is done by the configuration of activities and events.

Webex Contact Center user management

Tip: *Use the Action search to navigate Automate*

Overview

The User Management section collects a number of elements associated with a contact center user.

Sites

Sites can be managed in Automate. These are the physical location of the contact center.

As a part of the management, a **Multimedia Profile Name** can be associated to the new site. See: *Webex Contact Center Desktop Experience*.

Skill definitions

Skill definitions can be managed in Automate.

These definitions group skill values, thresholds and a selected **Skill Type**, making it possible to assign skill requirements such as language fluency or product expertise to incoming calls so these are assigned to agents with a matching skills.

These definition are then also selected to be a part of a **Skill Profile**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Skill profiles

Skill profiles can be managed in Automate and comprise of a set of skills, each with an assigned value, that you can assign to a team or agent.

Skill definitions are assigned to a profile. For example, you can assign a high level of proficiency (**Proficiency Value**) in English to one skill profile and a lower level in another profile.

A skill profile can then be assigned to a Contact Center user - see: *Cisco Webex App users*.

Teams

Teams can be managed in Automate and can be assigned for specific functions. Agent Based (for a specific number of agents) and Capacity Based (no number assigned) team types are available.

A team can also be active or inactive and be assigned to a defined Site and Contact Center user - see: *Cisco Webex App users*.

User profiles

User profiles can be managed in Automate and consist of a **Profile Type** (determines the determine the privilege level) with features accessible to a Contact Center user.

Module Settings allow for the specification of permissions to the Contact Center modules, while similar access settings are available for user profiles, entry points, sites, queues, teams and folders.

The profile can then be assigned to a Contact Center user - see: *Cisco Webex App users*.

Webex Contact Center Desktop Experience

Overview

The settings in this category allow you to set up or manage the agent desktop experience. Settings include multimedia inactivity timeouts and system settings.

Multimedia profiles

A multimedia profile for the user, that includes enable and timeout settings for all types of media.

Outdial ANI

The Outdial Automatic Number Identification (ANI) is only synced from the Webex Control Hub and instances can then be selected in Automate. The number allows an agent to select a phone number as the caller ID for an outdial call.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial plans

The dial plan is only synced from the Webex Control Hub and instances can then be selected in Automate. The dial plan allows you to define validation criteria for the Dial Number (DN) that an agent uses to sign in to the Agent Desktop, as well as the DN used to dial out. DNs are validated against the syntax rules that are defined in one or more dial plans.

Address books

Address books can be managed in Automate. These contain entries with phone numbers that agents can use, and are associated with a selected **Parent Type** and Contact Center **Site** - as available from the **Sites** list under the **User Management** group - see: *Webex Contact Center user management*.

Desktop profiles

Desktop profiles can be managed in Automate. These are a group of permissions and desktop behaviors that can be assigned to an agents.

The following permissions and settings are available:

- Queue Transfer
- Agent Consult and Transfer
- Wrap-up and Idle Codes
- Wrap-up Timeout Values
- Agent Auto Available
- Dialing Capabilities
- Dial Number Capabilities
- Access to the agent personal statistics
- Auto Answer

Idle/Wrap-Up Codes

Idle and wrap-up codes can be managed in Automate. These contain entries that agents have available in their **Desktop Profiles** and use to indicate their unavailability or status of the customer contacts.

The codes are also associated with available **Work Types** that are synced from the Webex Control Hub or managed in Automate. See: *Webex Contact Center Advanced*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Webex Contact Center Advanced

Holiday List

Define holiday lists for your organization and associate to working hours. Use holidays to define the non working days based on business requirements.

Overrides

Define overrides for your organization and associate it to working hours. Use an override to define exceptions to shifts or working hours, based on your business requirements.

Associate an override to a working hours schedule to map the duration that can be exempt from the defined business hours, such as emergency hours.

Work Type

Work types group idle and wrap-up codes in auxiliary reports.

Agent Lines

Add an Agent Line (Phone or Device Profile)

Prerequisites:

In order to have an application user available, add a Contact Center server and service:

1. Under **Services > Contact Center > Servers** (default): add a server.

   Two SIP Trunks are needed, a CVP and CUBEE on the server.

2. Under **Services > Contact Center > Service** (default): add a service using the above server. This step will create the application users needed when adding an Agent Line.

Perform these steps:

1. In the Admin Portal, go to **Agent Lines**.

   Note: Use the toolbar Action search to go to the page.

2. On the **Agent Lines** form, click **Add** to add a new agent line.
3. Complete the mandatory fields, consider the following:
   - Device Type*
     - Phone, or
     - Device Profile (Extension Mobility)
   - Profile User* (Device Profile device types only)

     Drop-down displays only users who have an extension mobility profile.
4. Click **Save** to add the agent line.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Search in Automate*

Tag CTI port as Contact Center agent line

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, go to **Agent Lines**.
2. Set the relevant hierarchy path (Provider, Reseller, Customer, Site).
3. Click the Plus icon (+) to add a new CTI port.
4. At **Device Type**, select **Phone**.
5. At **Device Name**, select a port from the list of device names.
6. At **Line**, select the line.
7. At **Application User**, select **pguser**.
8. Save your changes.
9. Repeat this procedure for both LCP and RCP ports.

Introduction to Contact Center Service

Tip: *Use the Action search to navigate Automate*

- Only one instance of Contact Center Server can be created for a Cisco Unified Communications Manager (CUCM) cluster.
- Only one instance of Contact Center Service can be created for Contact Center Server.
- For CUSP, only one trunk of type CUSP needs to be added via the Contact Center **Services** page.
- For deleting a server, ensure that the service is deleted first.

Note: Ensure that before you begin deleting Contact Center Server you have deleted all the agent lines for that Contact Center Server.

Configure Contact Center server using Cisco UCM

Tip: *Use the Action search to navigate Automate*

Contact Center provisioning configures Cisco Unified Communications Manager (Cisco UCM) to communicate with Contact Center.

- To enable UCM to communicate with Contact Center when transferring a call from agent to agent and routing a call back to the Customer Voice Portal (CVP), go to the **Servers** page for Contact Center.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To allow internal service calls to be routed to the CUBE (ENT) for Contact Center to process, go to the **Service** page for Contact Center.

Configuration overview

1. Once you have Automate configured and have added a Provider, add a Customer (under Provider or Reseller), then log in as a Provider Admin.
2. Contact Center configuration is only supported for dedicated Unified Communications Applications for a Customer. When adding a Provider, clear Shared UC Apps.
3. After successfully adding a Customer, choose the Customer hierarchy at the above context level and then add the UCMs to that customer, via the Cisco UCM **Servers** page.
4. Complete a UCM import before proceeding further.
5. Automate supports multiple UCM clusters at a Customer hierarchy. You can decide which cluster to use for Contact Center and IP telephony.
6. SIP Trunk Security Profiles must be created manually in each UCM and synced to Automate.
7. For the Contact Center customers, Built-in-Bridge must be enabled for the phones. By default, it is disabled at system level.
8. SIP trunk profiles must be created manually in each CUCM and synced to Automate.

Built-in-bridge

provider

Tip: *Use the Action search to navigate Automate*

Overview

Built-in-Bridge (BIB) is disabled by default for the phones at the system level as it is not used by all customers by default. It is used only by customers with Contact Center.

The provider has to perform the following procedures to enable BIB for the customers having contact center:

- *Configure the Built-in-bridge*
- *Enable or disable the Built-in-Bridge*

Note: Create a new field display policy at the customer level and add Built-in Bridge to the list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure the Built-in-bridge

1. Log in to the Automate Admin portal as provider administrator.
2. Go to **Field Display Policies**.
3. Set the hierarchy to the relevant Customer.
4. Select **SubscriberPhoneMenuItemProvider**.
5. Choose **Action > Clone**.
6. In the **Name** field, enter **SubscriberPhoneMenuItemProvider**.
7. From the **Target Model Type** drop-down, choose **relation/SubscriberPhone**.
8. Click '+' next to **Groups** to expand the Groups section, and in the **Title** field enter **Phone**.
9. From the **Available** list, choose **builtInBridgeStatus** and click **Select**.
10. Click **Save**.

Enable or disable the Built-in-Bridge

Prerequisites:

- *Configure the Built-in-bridge*

To enable or disable BIB:

1. Log in to the Automate Admin Portal as provider administrator.
2. Set the hierarchy to the appropriate Customer.
3. Go to the **Phones** page, then select the relevant phone.
4. On the **Phone** tab:
   - From the **Built in Bridge** drop-down in the **Vendor Config** section, choose **On** to enable BIB.
   - From the **Built in Bridge** drop-down in the **Vendor Config** section, choose **Off** to disable BIB.
5. Click **Save**.

Add a Contact Center server

Tip: *Use the Action search to navigate Automate*

1. Log in as provider administrator at the customer hierarchy.
2. Go to the **Servers** page for Contact Center.
3. Click the Plus icon (+) to add a new Contact Center server.
4. Configure the new Contact Center server, then save your changes. The table describes Contact Center server settings:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Contact Center Server Name	Unique server name. This field is mandatory.
Description	Server description.
Cisco Unified Communications Manager	The Cluster you want to use for Contact Center Server. This field is mandatory.
Transfer Conference Pattern	Transfer conference pattern used when transferring calls between agents. This field is mandatory.
Network VRU	Pattern used to route calls to a CVP. This field is mandatory.
SIP Trunks	This field is mandatory. See fields below:
Trunk Destination Type	CVP or CUBE (ENT) or CUSP SIP Trunk. This field is mandatory. Note: Both CVP and CUBE (ENT) trunks must be added for this Contact Center Server to be added successfully.
Trunk Destination Address	The destination address of the CVP or CUBE (ENT) or CUSP SIP Trunk. This field is mandatory. Multiple destination addresses & ports can be added for each trunk type.
Trunk Destination Port	The destination port of the CVP or CUBE (ENT) or CUSP SIP Trunk, if no value provided system takes 5060 as default.
Trunk Security Profile	The SIP trunk Security Profile that needs to be used by each trunk. This field is mandatory.
SIP Profile	The SIP trunk profile that needs to be used by each trunk. This field is mandatory.

For 500/1000/4000/12K/SCC - You must provide information for a CVP and a CUBE (ENT) SIP Trunk. For Small Contact Center, both the CVP and CUBE (ENT) trunks should have the same IP address with a different Trunk Security Profile selected in the **Trunk Security Profile** drop-down for each trunk.

For CUSP - You must provide information for a CUSP SIP Trunk. Only one trunk type can be added.

Note: For CUSP, use only one SIP trunk. For CVP or CUBE (ENT), use two SIP trunks.

1. Device Pool will create automatically as a part of Contact Center server with the name “Cu<CUSTOMER_ID>-CC<CC_SERVER_ID>-DP” with the default Call Manager Group & Region.
2. Call Manager Group & Region can be changed in the Cisco Unified Communications Manager as desired.
3. Two application users creates with names pguser & pguser2 - both are created with default password “cisco”.

Note:

- The pguser & pguser2 names may be changed to tie with the Customer ID in future releases.
- For all the phone line CSS of a site, add Cu<CUSTOMER_ID>-CC<CC_SERVER_ID>-Xfer4CCServer-PT to the Class of Service member list as a partition with the next available index.
- The admin needs to add Default Region as related regions for each site region created for a site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Reset the trunk by clicking the **Reset** button in the Trunk page after updating the SIP profile.

Edit or delete Contact Center servers

Tip: *Use the Action search to navigate Automate*

Edit a Contact Center server

1. Log in to Automate as provider or reseller admin.
2. Choose the Customer hierarchy level.
3. Go to the **Servers** page for Contact Center.
4. Click the Contact Center server that you want to edit and modify the required fields.

   Note: The Contact Center server name is read-only and can't be changed.

5. Save your changes.

Delete a Contact Center server

Prerequisites:

- Delete the Contact Center service and parameters associated with Contact Center server.

Perform these steps:

1. Log in to Automate as provider or reseller admin.
2. Choose the Customer hierarchy level.
3. Go to the **Servers** page for Contact Center.
4. Select the checkbox adjacent to the name of the Contact Server/s you wish to delete.
5. Click **Delete**, then click **Yes** to confirm.

Add a Contact Center service

Tip: *Use the Action search to navigate Automate*

Note:

- Only ONE instance of Contact Center Server can be created for a Cisco Unified Communications Manager (CUCM) cluster.
- Only ONE instance of Contact Center Service can be created for a Contact Center Server.
- For CUSP only ONE trunk of type CUSP needs to be added.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To delete a server, ensure the service is deleted first.

Pre-requisites:

- Customer & Site Dial Plan is required to add a Contact Center Service.

Perform these steps:

1. Log in as provider administrator at the customer hierarchy.
2. Go to the **Services** page for Contact Center.
3. Click **Add** to add a new Contact Center Service.
4. Configure the Contact Center service.
5. Save your changes.

Edit or delete Contact Center services

Tip: *Use the Action search to navigate Automate*

Edit Contact Center services

1. Log in to Automate as provider or reseller administrator.
2. Choose the customer hierarchy level.
3. Go to the **Services** page for Contact Center.
4. Click the Contact Center service that you want to edit, and modify the required fields.

   Note: Contact Center service name is read-only and can't be modified.

5. Save your changes.

Delete Contact Center services

1. Log in to Automate as provider or reseller administrator.
2. Choose the customer hierarchy level.
3. Go to the **Services** page for Contact Center.
4. Select the checkbox adjacent to the name of any Contact Center service you wish to delete, then click the **Delete** icon.
5. Click **Yes** to confirm the deletion.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure CTI Port

This procedure adds and configures a CTI port.

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, go to the **Phones** page, then click the Plus icon (+) to open the **Phones**/**New Record** page.
2. Set the hierarchy level (Provider, Reseller, Customer, Site).
3. On the **Phone** tab:
   - At **Device Name**, enter a unique name for the Local CTI Port pool name. For example, use the following format for the device name (LCPxxxxFyyyy):
     - LCP identifies the CTI Port as a local device.
     - xxxx is the peripheral ID for the Unified Communications Manager PIM.
     - yyyy is the local CTI Port.At the **Product** drop-down, choose **CTI Port**.
   - Enter a description for the Local CTI Port.
   - At **Device Pool Name**, choose the appropriate device pool.
4. On the **Lines** tab:
   - Click the Plus icon (+) at **Line** to add a new line.
   - At **Pattern**, choose a unique directory number for the CTI port.
   - Leave default values unchanged.
5. Go to the **Phones** page, then, click the Plus icon (+) to create a new CTI port.
6. Set the hierarchy level (Provider, Reseller, Customer, Site).8
7. On the **Phone** tab:
   - At the **Product** drop-down, choose **CTI Port**.
   - At **Device Name**, enter a unique name for the Local CTI Port pool name. For example, use the following format for the device name (RCPxxxxFyyyy):
     - RCP identifies the CTI Port as a Network device.
     - xxxx is the peripheral ID for the Unified Communications Manager PIM.
     - yyyy is the Network CTI Port.
   - At **Description**, enter a description for the Local CTI Port.
   - At **Device Pool Name**, choose the appropriate device pool.
8. On the **Lines** tab:
   - Click the Plus icon (+) to add an entry for a new line.
   - From the **Pattern** drop-down, choose a unique directory number for the CTI port.
   - Leave default values unchanged.
9. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Basic Settings

Call Manager Groups

Tip: *Use the Action search to navigate Automate*

Overview

A Call Manager Group (Cisco UCM group), contains a list of up to three UCM servers (users). These servers are prioritized. The server marked with the lowest number (zero) serves as the primary UCM user for that group, and the other members of the group serve as secondary and tertiary (backup) UCMs.

Each device pool has one UCM group that is assigned to it. When a device registers, it attempts to connect to the primary UCM user in the group assigned to its device pool. If the primary UCM is unavailable, the device tries to connect to the next UCM listed in the group, and so on.

A single UCM user is usually assigned as primary for one UCM group, and as secondary / tertiary (if applicable) on other UCM groups.

The table describes the value of UCM groups for your system:

Benefit	Description
Redundancy	This feature enables you to designate a primary and backup UCM user servers for each group.
Call processing load balancing	This feature enables you to distribute the control of devices across multiple UCM users.

For systems with a UCM that includes multiple servers (users), you are likely to achieve better load distribution and redundancy.

Manage Call Manager Groups

This procedure adds a new UCM group, and edits and deletes an existing UCM group.

Prerequisites:

- Configure all UCM servers (users) that you want to assign as members of the Call Manager group.

Note: After configuring the Call Manager group, you can use it to configure device pools. Devices obtain their UCM group list setting from the device pool to which they are assigned.

Perform these steps:

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.

   Note: For Shared Architecture deployment, ensure you sign in only as either Provider or Reseller admin as only these admins can add UCMs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. If you are adding a new instance, ensure the hierarchy path is set to the target node for the new instance.
3. Go to **Call Manager Groups**.
4. Choose an option:
   - To add a new UCM group, click the Plus icon (+), then go to step 5.
   - To edit an existing UCM group, click on the relevant option in the list to open its settings, then go to step 5.
5. Configure the UCM group:

Field	Description
Name (Mandatory)	Fill out the UCM group name.
Auto-registration Cisco Unified Communications Manager Group	Select this checkbox if you want this UCM group to be the default UCM group when auto-registration is enabled. Leave unchecked (disabled) if you don't want devices to auto-register with this UCM group. Tip Each UCM cluster can have only one default auto-registration group. If you choose a different UCM group as the default auto-registration group, that is, you select the Auto-registration Cisco Unified Unified Communications Manager Group* checkbox for a different UCM group, the previously chosen auto-registration group no longer serves as the default for the cluster; the Auto-registration Cisco Unified Communications Manager* checkbox displays for the previously chosen group (the original default), and the checkbox gets disabled for the group that now serves as the default.
Unified CM Group Items (Mandatory)	Click the Plus icon (+) to add a UCM to the group. Repeat to add multiple UCM's to the group. You can delete UCMs added to to the Call Manager (UCM) group or re-order UCMs in the group.
Priority (Mandatory)	Enter the priority number for this UCM in the group. The smaller the integer, the higher the priority.
Selected Cisco Unified Communications Managers	This field displays the UCMs in the Cisco UCM group.

6. Click **Save**.

   New UCM groups now appear in the list view of Call Manager Groups. You can delete Call Manager Groups from the list if required.

Note: To verify that the UCM is deployed in Shared Mode:

- Go to UCM **Servers**.
- On the **Publisher** tab, verify that the Multi-Tenant field is set to *Shared*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Cisco UCM group selection in the Core Feature Guide.
- Set up Cisco UCM servers in the Core Feature Guide.

Cisco UCM group counts

Tip: *Use the Action search to navigate Automate*

1. Log in as a Provider administrator, then go to the **CUCM Group Counts** page.
2. From the **CUCM** drop-down, choose a CUCM instance to show the CUCM Group counts for.
3. The **CUCM Group counts** field shows all CUCM groups and the count of devices in the format: *<group_name>*[*<count>*].

   If a CUCM Group has no device pool, in other words it has no devices, the group shows as *<group_name>[0 no device pools]*.

An administrator can use the CUCM Group Count data to inspect CUCM Group utilization at a customer, or to choose a Default CUCM Group that will be assigned to a customer's Site Defaults Doc.

Note: Group Counts values are Phone counts per Device Pool per CUCM Group.

Locations

Tip: *Use the Action search to navigate Automate*

Overview

Locations are used to implement call admission control in a centralized call-processing system. Call admission control enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between the locations.

Important: Locations are different to sites. Locations are used by CUCM to manage call admission control. Sites are used by VOSS Automate to logically group resources.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add locations on CUCM

This procedure adds CUCM locations.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to a customer or site level.
3. If prompted, select the NDL that contains the CUCM on which you are configuring the location.
4. Choose an option:
   - Logged in as Provider or Reseller admin? Go to (CUCM) **Locations**.
   - Logged in as Customer admin? Go to (Advanced) **Locations**.
5. Click the Plus icon (+) to add a new record.
6. On the **Location Information** tab, fill out the name of the location.
7. Select the **Intra-Location** tab, and complete at minimum, the mandatory *Intra-Location settings*.
8. Select the **Between Locations** tab, and complete at minimum, the mandatory *Between Locations settings*.
9. Select the **RSVP Settings** tab, and complete at minimum, the mandatory *RSVP Settings*.
10. Click **Save**.

Intra-Location settings

Field	Description
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Valid values are 0 to 2147483647, where 0 means unlimited bandwidth. This field is mandatory. Note: To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on this link.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Valid values are 1 Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. Setting the value to 1 means you cannot make video calls within this location. This field is mandatory.
Immersive Video Bandwidth	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. Setting the value to 1 means you cannot make immersive video calls within this location. This field is mandatory.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Between Locations settings

Field	Description
Location	Select a location from the list. This field is mandatory.
Weight	Enter the relative priority of this link in forming the Effective Path between any pair of Locations. The Effective Path has the least cumulative Weight of all possible paths. Valid values are 0-100. This field is mandatory.
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Valid values are 0 to 2147483647, where 0 means unlimited bandwidth. You can also select Unlimited Bandwidth. This field is mandatory.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. You can also select Unlimited Bandwidth or None. Setting the value to **None** means you cannot make video calls between this location and other locations. This field is mandatory.
Immersive Video Bandwidth	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link between this location and other locations. For video calls, the immersive video bandwidth does not include overhead. Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. You can also select **Unlimited Bandwidth** or **None**. Setting the value to **None** means you cannot make immersive video calls between this location and other locations. This field is mandatory.

Copyright © 2025 VisionOSS Limited. All rights reserved.

RSVP Settings

Field	Description
Location	To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane. This field is mandatory.
RSVP Setting	To choose an RSVP policy setting between the current location and the location that is chosen in the Location pane at left, choose an RSVP setting from the drop-down list. This field is mandatory. Choose from the following available settings: • **Use System Default** - The RSVP policy for the location pair matches the clusterwide RSVP policy. See topics related to clusterwide default RSVP policy in the Cisco Unified Communications Manager System Guide for details: – **No Reservation** - No RSVP reservations can get made between any two locations. – **Optional (Video Desired)** - A call can proceed as a best-effort audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified Communications Manager if reservation succeeds. – **Mandatory** - Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream too. – **Mandatory (Video Desired)** - A video call can proceed as an audio-only call if a reservation for the video stream cannot be reserved.

Date time groups

Tip: *Use the Action search to navigate Automate*

Overview

Date Time Groups define time zones for the various devices that are connected to Cisco UCM. Each device exists as a member of only one device pool, and each device pool has only one assigned Date Time Group.

UCM automatically configures a default Date Time Group, called `CMLocal`, which syncs to the active date and time of the operating system on the server where UCM is installed. You can change the settings for `CMLocal`, as required. Normally, adjust server Date and Time to the local time zone date and time.

Tip: For a worldwide distribution of Cisco Unified IP phones, create one named Date Time Group for each of the time zones in which you deploy endpoints.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add date time groups

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to a customer or site level.
3. If prompted, select the NDL that contains the Cisco Unified CM on which you are configuring the Date Time Group.
4. Go to **Date Time Groups**.
5. Click the Plus icon (+) to add a new record, then, provide configuration details:

Field	Description
Group Name	Enter the name that you want to assign to the new Date Time Group. This field is mandatory.
Time Zone	Choose the time zone for the group that you are adding. This field is mandatory.
Separator	Choose the separator character to use between the date fields. This field is mandatory.
Date Format	Choose the date format for the date that displays on the Cisco Unified IP Phones. This field is mandatory.
Time Format	Choose a 12-hour or 24-hour time format. This field is mandatory.
Selected Phone NTP References	To ensure that a phone that is running SIP gets its date and time configuration from an NTP server, select the phone NTP references for the Date Time Group.

6. Click **Save**.

Cisco UCM group selection

Tip: *Use the Action search to navigate Automate*

Overview

Provider level administrators can manage the default Cisco UCM (Unified Communications Manager) group setting in a customer's Site Defaults:

- The least utilized group can be calculated, in other words the group with the least number of phones can automatically be determined.

  In this case, the administrator can set the Default CUCM Group in the customer's Site Defaults to automatically be the least utilized group so that CUCM Groups are optimally assigned whenever a site is created.

- The current device utilization of customer CUCM Groups can be inspected. Device utilization is calculated by inspection of the Device Pools that belong to a CUCM Group of a CUCM cluster and the number of Phones in these Device Pools.

  The administrator can therefore inspect the CUCM Group counts and then choose a Default CUCM Group to be the Default CUCM Group in the customer's Site Defaults.

Copyright © 2025 VisionOSS Limited. All rights reserved.

High level administrators carry out these tasks via **CUCM Group Counts**. Use the Action search to locate the page.

Select a Cisco UCM group

1. Log in as a Provider administrator, then go to **CUCM Group Selection**.
2. The list of existing CUCM Group Selection configurations at the Provider hierarchy are listed.

   Click the Plus icon (+) to create a configuration. A hierarchy pop-up will show to choose the customer hierarchy at which the configuration should apply.
3. Choose a name for the configuration. The default name is the hierarchy name.
4. Choose an algorithm to apply to the CUCM Group Selection:
   - If **Use Default** is selected, the Site Defaults doc is updated if necessary so that the Default CUCM Group is applied.

     Note: The CUCM Group called Default is always used when adding a site unless the "Least utilized" algorithm has been selected. Default will also be the fallback CUCM Group in the event that all CUCM Groups have been excluded from the selection.

   - If Least utilized CUCM Group is selected from the Algorithm drop-down, options are available to include and exclude specific CUCM groups from the algorithm.
     - If no groups are included or excluded, *all* groups available at the customer hierarchy are considered by the algorithm.
     - If groups are added to the CUCM Groups to Include, only these groups are considered by the algorithm.
     - If groups are added to the CUCM Groups to Exclude, these groups are not considered by the algorithm, *unless* they have also been added to the Groups to Include.

     The table summarizes the options and outcomes:

Group Selection	Algorithm	Include List	Exclude List	Result	Comment
No	Use Default	N/A	N/A	Default	Falls back to Default always
Yes	Use Default	None	None	Default	
Yes	Least utilized	None	None	Least utilized	
Yes	Least utilized	Yes	None	Least utilized	From the groups in the included list.
Yes	Least utilized	None	Yes	Least utilized	Least utilized from all groups except in the exclude list.
Yes	Least utilized	Yes	Yes	Least utilized	From the groups in the included list. Note that the exclude list will be ignored in this case.

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. Click **Save** to save the configuration for the customer hierarchy.

   When a new site is created, the Default CUCM Group in the Site Defaults Doc is updated to reflect the configuration, so that any sites that are now created under this customer hierarchy will apply the calculated CUCM group.

   Note: An administrator can override this calculated CUCM group by manually updating the Site Defaults Doc.

Device pools

Tip: *Use the Action search to navigate Automate*

Overview

Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains system, device, and location-related information.

After adding a new device pool, you can use it to configure devices, such as Cisco Unified IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, and CTI route points.

Add or manage device pools

1. Log in to the Admin Portal as Provider, Reseller, or Customer administrator.
2. Go to **Device Pools**.
3. Choose an option:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add new device pool	• Click **Add**. • Choose the network device list (NDL) where you want to add the new device pool. **Note:** You won't need to choose a NDL if you're adding the device pool at a site. In this case, you will use the NDL associated with the site. • Click **OK**. • On the **Device Pool Settings** tab, at **Device Pool Name**, fill out the device pool name as **RSMSimPhone_DP**. • From the **Cisco Unified CM Group** drop-down, choose **RSMSimPhone**. • On the **Roaming Sensitive Settings** tab, from the **Date/Time Group** drop-down, choose the appropriate date/time group. • From the **Region** drop-down, choose **AR_RSMSimPhone**. • From the **SRST Reference** drop-down, choose **Disable**.
Edit a device pool	• Click on the relevant device pool in the list. • Go to step 4.
Delete a device pool	• In the list view, select the checkbox adjacent to the **Name** column for the device pool you want to remove. • Click **Delete**.

4. To configure or update device pool properties, click through the tabs on the page and fill out at least the mandatory fields:
   - Device Pool Settings tab
   - Local Route Group Settings tab
   - Roaming Sensitive Settings tab
   - Device Mobility Related Information tab
   - Geolocation Configuration** tab
   - Incoming Calling Party Settings tab
   - Incoming Called Party Settings tab
   - Caller ID for Calls from This Phone tab
   - Connected Party Settings tab
   - Redirecting Party Settings tab

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. Click **Save**. The route partition appears in the device pool list.

Associate a local route group to a device pool

This procedure associates a local route group with an existing device pool for each site.

This allows calls from a device that is tied to a device pool to go out on a specific route group based on the call type. For example, you can associate multiple local route groups such as Emergency Route Group, Primary Local Route Group (for site A), Secondary Local Route Group (for site A), Primary Local Route Group (for site B), and Secondary Local Route Group (for site B).

Local Route groups allow you to specify different route groups for each site (site A and site B) for the respective device pool. Also, you can define a separate call routing option for emergency calls when you associate the Emergency Route Group with a different route group. Hence you can easily define separate call routing options for emergency calls and PSTN calls.

1. Log in as Provider, Reseller, or Customer administrator.

   Warning: When associating a local route group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to associate a local route group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.

2. Go to **Device Pools**.
3. Click the device pool to be associated.
4. From the **Cisco Unified CM Group** drop-down menu, select a specific Cisco Unified Communications Manager group or leave the Cisco Unified CM Group as Default.
5. Configure setting in the **Local Route Group Settings** tab/panel:
   a. In the grid, from the **Local Route Group** drop-down menu, select the local route group.
   b. In the grid, from the **Route Group** drop-down menu, select the route group or gateway.
6. Save the new local route association.

Device pools configuration settings

Device Pool Settings

The table describes the device pool settings and values on the Device Pool Settings tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Device Pool Name *	Enter the name of the new device pool that you are creating. You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces. Default value: None
Cisco Unified CM Group *	Choose the Cisco Unified Communications Manager group to assign to devices in this device pool. A Unified CM group specifies a prioritized list of up to three Unified CMs. The first Unified CM in the list serves as the primary one for that group. The other members of the group serve as backup Unified CMs for redundancy.
Calling Search Space for Auto-registration	Choose the calling search space to assign to devices in this device pool that auto-register with Unified CM. The calling search space specifies partitions that devices can search when attempting to complete a call.
Adjunct CSS	From the drop-down list, choose an existing Calling Search Space (CSS) to use for the devices in this device profile as an adjunct CSS for the Extension Mobility Cross Cluster (EMCC) feature. To configure a new CSS or modify an existing CSS, choose **Call Routing > Class of Control > Calling Search Space** in Unified CM Administration. When configuring the EMCC feature, the administrator must configure a device pool for each remote cluster. If the remote cluster is located in a different country, the adjunct CSS must embrace the partition with which the emergency patterns of that country associate. This configuration facilitates country-specific emergency call routing. Default value: None
Reverted Call Focus Priority	Choose a clusterwide priority setting for reverted calls that the hold reversion feature invokes. This setting specifies which call type, incoming calls or reverted calls, have priority for user actions, such as going off hook. • **Default**-If you choose this option, incoming calls have priority. • **Highest**-If you choose this option, reverted calls have priority. The **Not Selected** setting specifies the reverted call focus priority setting for the default device pool at installation. At installation, incoming calls have priority. You cannot choose this setting in Unified CM. Note: This setting applies specifically to hold reverted calls; it does not apply to parked reverted calls.
Intercompany Media Services Enrolled Group	Choose an **Intercompany Media Services Enrolled Group** from the drop-down list.

Local Route Group Settings

The table describes the device pool settings and values on the Local Route Group Settings tab/panel:

Option	Description
Local Route Group	From the drop-down, choose the name of the local route group to associate with this device pool.
Route Group	From the drop-down, choose the value for the local route group to associate with this device pool.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Roaming Sensitive Settings

The table describes the device pool settings and values on the Roaming Sensitive Settings tab/panel:

Option	Description
Date/Time Group *	Choose the date/time group to assign to devices in this device pool. The date/time group specifies the time zone and the display formats for date and time. Default value: None
Region *	Choose the Unified CM region to assign to devices in this device pool. The Unified CM region settings specify voice codec that can be used for calls within a region and between other regions. Default value: None
Media Resource Group List	From the drop-down list, choose a media resource group list. A media resource group list specifies a prioritized list of media resource groups. An application selects the required media resource (for example, a music on hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order defined in a media resource group list. Default value: None
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability. It works by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list, choose the appropriate location for this device pool. A location setting of **None** or **Hub_None** means that the locations feature does not track the bandwidth that the devices in this pool consume. A location setting of **Phantom** specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. Default value: None
Network Locale	From the drop-down list, choose the locale that is associated with phones and gateways. The network locale contains a definition of the tones and cadences that the phones and gateways in the device pool in a specific geographic area use. Make sure that you select a network locale that all of the phones and gateways that use this device pool can support. Note: If the user does not choose a network locale, the locale that is specified in the Unified CM clusterwide parameters as Default Network Locale applies. Note: Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. When a device is associated with a network locale that it does not support in the firmware, the device fails to come up. Default value: None

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
SRST Reference *	From the drop-down list, choose a survivable remote site telephony (SRST) reference to assign to devices in this device pool. Choose from these options: • **Disable** - When you choose this option, devices in this device pool do not have SRST reference gateways that are available to them. • **Use Default Gateway** - When you choose this option, devices in this device pool use the default gateway for SRST. • **Existing SRST references** - When you choose an SRST reference from the drop-down list, devices in this device pool use this SRST reference gateway. Default value: None
Connection Monitor Duration	This setting defines the time that the Cisco Unified IP Phone monitors its connection to Unified CM before it un-registers from SRST and re-registers to Unified CM. To use the configuration for the enterprise parameter, you can enter “1” or leave the field blank. The default value for the enterprise parameter equals 120 seconds. Tip: When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter.
Single Button Barge	This setting determines whether the devices or phone users in this device pool have single-button access for barge and cBarge. From the drop-down list, choose from these options: • **Off** - When you choose this option, the devices in this device pool have the Single Button Barge/cBarge feature disabled. • **Barge** - When you choose this option, the devices in this device pool have the Single Button Barge feature enabled. • **CBarge** - When you choose this option, the devices in this device pool have the Single Button cBarge feature enabled. • **Default** - When you choose this option, the devices in this device pool use the service parameter setting for the Single Button Barge/cBarge feature. Default value: Default
Join Access Lines	This setting determines whether the Join Access Lines feature is enabled for the devices or phone users in this device pool. From the drop-down list, choose from these options: • **Off** - When you choose this option, the devices in this device pool have the Join Access Lines feature disabled. • **On** - When you choose this option, the devices in this device pool have the Join Access Lines feature enabled. • **Default** - When you choose this option, the devices in this device pool use the service parameter setting for the Join Access Lines feature. Default value: Default
Physical Location	Select the physical location for this device pool. The system uses physical location with the device mobility feature to identify the parameters that relate to a specific geographical location. Default value: None

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Device Mobility Group	Device mobility groups represent the highest level geographic entities in your network and are used to support the device mobility feature. Default value: None
Wireless LAN Profile Group	Choose a wireless LAN profile group from the drop-down list. Note: You can specify the Wireless LAN Profile Group at the Device Pool level or the individual phone level.

Device Mobility Related Information

The table describes the device pool settings and values on the Device Mobility Related Information tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Device Mobility Calling Search Space	Choose the appropriate calling search space to be used as the device calling search space when the device is roaming and in the same device mobility group. Default value: None
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. Default value: None
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of **None** specifies that no rerouting of blocked calls is attempted. Default value: None
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool. Tip: Before the call occurs, the device must apply the transformation by using digit analysis. Note: If you configure the Calling Party Transformation CSS as **None** for the device pool and you select the **Use Device Pool Calling Party Transformation CSS** check box in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing. Default value: None
Called Party Transformation CSS	This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. Note: If you configure the Called Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing. Default value: None

Geolocation Configuration

The table describes the device pool settings and values on the Geolocation Configuration tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that the devices in this device pool do not associate with a geolocation. Default value: None
Geolocation Filter	From the drop-down list, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for the devices in this device pool. Default value: None

Incoming Calling Party Settings

The table describes the device pool settings and values on the Incoming Calling Party Settings tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
National Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use **National** for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word "Default" instead of entering a prefix. If the word "Default" displays in the **Prefix** field, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
National Strip Digits	Enter the number of digits, up to the number 24, that you want Unified CM to strip from the calling party number of National type before it applies the prefixes.
National Calling Search Space	This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as **None**, the transformation does not match and does not get applied. Make sure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.
International Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use **International** for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word "Default" instead of entering a prefix. If the word "Default" displays in the **Prefix** field in the **Device Pool Configuration** window, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
International Strip Digits	Enter the number of digits, up to the number 24, that you want Unified CM to strip from the calling party number of International type before it applies the prefixes.
International Calling Search Space	This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Unknown Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use **Unknown** for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
Unknown Strip Digits	Enter the number of digits, up to the number 24, that you want Unified CM to strip from the calling party number of Unknown type before it applies the prefixes.
Unknown Calling Search Space	This setting allows you to globalize the calling party number of “Unknown” calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.
Subscriber Prefix	UCM applies the prefix that you enter in this field to calling party numbers that use **User** for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word “Default” displays in the **Prefix** field in the **Device Pool Configuration** window, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
Subscriber Strip Digits	Enter the number of digits, up to the number 24, that you want UCM to strip from the calling party number of user type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to globalize the calling party number of **User** calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Incoming Called Party Settings

The table describes the device pool settings and values on the Incoming Called Party Settings Configuration tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
National Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use **National** for the Called Party Numbering Type. You can enter up to sixteen (16) characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Gateway** or **Trunk Configuration** window, you cannot configure the **Strip Digits** field in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the **Device Pool Configuration** window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix** field. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
National Strip Digits	Enter the number of digits, that you want Unified CM to strip from the called party number of “Unknown” type before it applies the prefixes.
National Calling Search Space	This setting allows you to transform the called party number of “Unknown” called party number type on the device. If you choose **None**, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
International Prefix	Unified CM applies the prefix that you enter in this field to called party numbers that use **National** for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Prefix** field in the Gateway or Trunk Configuration window, you cannot configure the **Strip Digits** field in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix** field. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
International Strip Digits	Enter the number of digits that you want Unified CM to strip from the called party number of International type before it applies the prefixes.
International Calling Search Space	This setting allows you to transform the called party number of International called party number type on the device. If you choose **None**, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Unknown Prefix	Unified CM applies the prefix that you enter in this field to called numbers that use **Unknown** for the Called Party Numbering Type. You can enter up to sixteen characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Prefix** in the Gateway or Trunk window, you cannot configure the **Strip Digits** in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix field**. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
Unknown Strip Digits	Enter the number of digits, that you want Unified CM to strip from the called party number of “Unknown” type before it applies the prefixes.
Unknown Calling Search Space	This setting allows you to transform the called party number of “Unknown” called party number type on the device. If you choose **None** no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Subscriber Prefix	UCM applies the prefix that you enter in this field to called numbers that use **User** for the Called Party Numbering Type. You can enter up to sixteen characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Prefix** field in the Gateway or Trunk Configuration window, you cannot configure the **Strip Digits** field in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix** field. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
Subscriber Strip Digits	Enter the number of digits, that you want UCM to strip from the called party number of user type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to transform the called party number of user called party number type on the device. If you choose **None**, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Caller ID For Calls From This Phone

The table describes the device pool settings and values on the Caller ID For Calls From This Phone tab/panel:

Option	Description
Calling Party Transformation CSS	From the drop-down list, choose the CSS that contains the Calling Party Transformation Pattern that you want to apply to devices in this device pool. When UCM receives a call from a device in this device pool on an inbound line, UCM immediately applies the calling party transformation patterns in this CSS to the digits in the calling party number before it routes the call. This setting allows you to apply digit transformations to the calling party number before UCM routes the call. For example, a transformation pattern can change a phone extension to appear as an E.164 number.

Connected Party Settings

The table describes the device pool settings and values on the Connected Party Settings tab/panel:

Option	Description
Connected Party Transformation CSS	This setting is applicable for inbound calls only. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. UCM includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages for SIP calls and in the Connected Number Information Element of CONNECT and NOTIFY messages for H.323 and MGCP calls. Make sure that the Connected Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. Note: If you configure the Connected Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Redirecting Party Settings

The table describes the device pool settings and values on the Redirecting Party Settings tab/panel:

Option	Description
Redirecting Party Transformation CSS	This setting allows you to transform the redirecting party number on the device to E164 format. Unified CM includes the transformed number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) sent out of Unified CM. Make sure that the Redirecting Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. that the Connected Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. Note: If you configure the Redirecting Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.

Configure regions

Tip: *Use the Action search to navigate Automate*

Overview

Regions can only be added at a Customer or Site hierarchy level. Regions added directly on CUCM are synced in at the hierarchy level the CUCM is configured at in VOSS Automate.

Regions can be modified or deleted at any hierarchy level. When deleting a region, related regions can't be removed from a region. They exist until either region is deleted.

Add or manage regions

This procedure adds, edits, and deletes regions.

1. Log in as Provider, Reseller or Customer administrator.
2. Go to (CUCM) **Regions**.
3. Choose the hierarchy (Customer or Site).
4. **Choose an option**:
   - **Delete a region**? Click on the name of the relevant region, then click **Delete**. Click **Yes** to confirm.
   - **Edit an existing region**? Click on the name of the relevant region. Go to step 5.
   - **Add a new region**? Click **Add**. Go to step 5.
5. At **CUCM** drop-down menu, choose or modify the CUCM (network device) for the region.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. At the **Name** field, for a new region, enter a unique name for the region, or to edit the region, update the name, if required.

   Note: If region is for a CUCM group, use **AR_ RSMSimPhone** as the region name.

7. At **Related Regions**, add or update the following details, as required:

Option	Description
Region Name	Drop-down menu with list of available regions. This field is mandatory.
Audio Codec Preference List	This is a drop-down containing available Audio Codec Preference Lists. The default codec is G.711.
Audio Bandwidth	Maximum Audio Bit Rate (kbps). This field is mandatory. If region is for a CUCM group, choose 64 kbps (G.711)
Video Bandwidth	Maximum Session Bit Rate for Video Calls (kbps). This field is mandatory.
Immersive Video Bandwidth	Maximum Session Bit Rate for Immersive Video Calls (kbps). This field is mandatory.

8. Click **Save**.

Media and Conferencing

Media resources

Tip: *Use the Action search to navigate Automate*

Automate allows for the management of the following media resources in Cisco UCM:

- Media Termination Point (MTP)
- Transcoder
- Conference Bridge

Note:

- Resources may be added at customer and site level
- In a multi cluster environment, Unified CM selection can be carried out for each resource.
- A media resource with a device pool and/or location are usually set up at site level. If however the media resource is created at *customer level*, consider the configuration of the device pool / location at customer level. The use of defaults available at CUCM level is possible, but a review of these settings may be required. Alternatively, creating a specific device pool / location for the media resource may be a better option.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Media Termination Point (MTP)

Automate supports the following media termination point (MTP) type: Cisco IOS Enhanced Software Media Termination Point

To add a MTP:

1. Navigate to the required customer or site level.
2. Select the Cisco UCM from the **CUCM** drop-down list.
3. Enter a **MTP Name** - up to 15 characters: (a-z, A-Z, 0-9), a dot (.), dash (-), and underscore (_).
4. Optionally complete the fields as required (refer to tooltips):
   - **Description**
   - **Mtp Type** - only one type supported: **Cisco IOS Enhanced Software Media Termination Point**. Display only.
   - **Device Pool Name** (refer to considerations at *Media resources*.)
   - **Trusted Relay Point**
5. Click **Save** and inspect the entry in the list view.

Note: The following cannot be modified: CUCM, MTP Name, MTP type

Delete a MTP

To delete a MTP, choose the MTP, and click the **Delete** button.

Add a transcoder

To add a transcoder:

1. Navigate to the required customer or site level.
2. Select the Cisco UCM from the **CUCM** drop-down list.
3. The following transcoder types are supported in the **Product** drop-down list:
   - Cisco Media Termination Point Hardware
   - Cisco IOS Media Termination Point
   - Cisco IOS Enhanced Media Termination Point
4. Enter a **Transcoder Name** - up to 15 characters: (a-z, A-Z, 0-9), a dot (.), dash (-), and underscore (_).
5. Optionally complete the fields as required (refer to tooltips):

   The device pool should reflect the physical position of the hardware.
   - **Description**
   - **Device Pool Name** (refer to considerations at *Media resources*.)
   - **Is Trusted Relay Point**
   - **Common Device Config Name** from Unified CM

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Load Information**

6. Click **Save** and inspect the entry in the list view.

Note: The following cannot be modified: CUCM, product, transcoder name

Delete a transcoder

To delete a transcoder, select it and click the **Delete** button.

Add a conference bridge

You can add, update, or delete a conference bridge.

To add a conference bridge:

1. Navigate to the required customer or site level.
2. Choose the Unified CM from the **CUCM** drop-down list.
3. The following hardware types are supported in the **Product** drop-down list:
   - Cisco Conference Bridge Hardware
   - Cisco IOS Conference Bridge
   - Cisco IOS Enhanced Conference Bridge
4. Enter a **Conference Bridge Name** - up to 15 characters: (a-z, A-Z, 0-9), a dot (.), dash (-), and underscore (_).
5. Optionally complete the fields as required (refer to tooltips):

   The device pool and location should reflect the physical position of the hardware.

   - **Description**
   - **Device Pool Name** (refer to considerations at *Media resources*.)
   - **Location Name** - as available on Unified CM
   - **Security Profile Name** - in accordance with the selected **Product**.
   - **Common Device Config Name** from Unified CM
   - **Use Trusted relay Point**
6. Click **Save** and inspect the entry in the list view.

Note: When modifying a Conference Bridge, the following cannot be modified: CUCM, product, conference bridge name

Use the **Delete** button to delete a Conference Bridge.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Cisco dial plan models

Tip: *Use the Action search to navigate Automate*

Overview

Cisco custom dial plan models (configured via **Cisco Dial Plan Models**) allow you to define the dial plan and to enter a name and type to group its elements.

The Dial Plan Type drop-down is used to tag it with its hierarchy, so that available dial plans to push or remove are filtered when using the Dial Plan Maintenance menu:

- Multi-tenant / Shared Architecture - provider hierarchy
- Global - customer hierarchy
- Site - site hierarchy

Note: If no Dial Plan Type tag is added to a dial plan, a new “in-progress” or “staging” dial plan can be created that will not show up to be pushed or removed on the Dial Plan Maintenance menu.

A description and notes for the Dial Plan Model definition can be added on the input form.

Related topics

- *Microsoft dial plan models*

Dial plan model elements

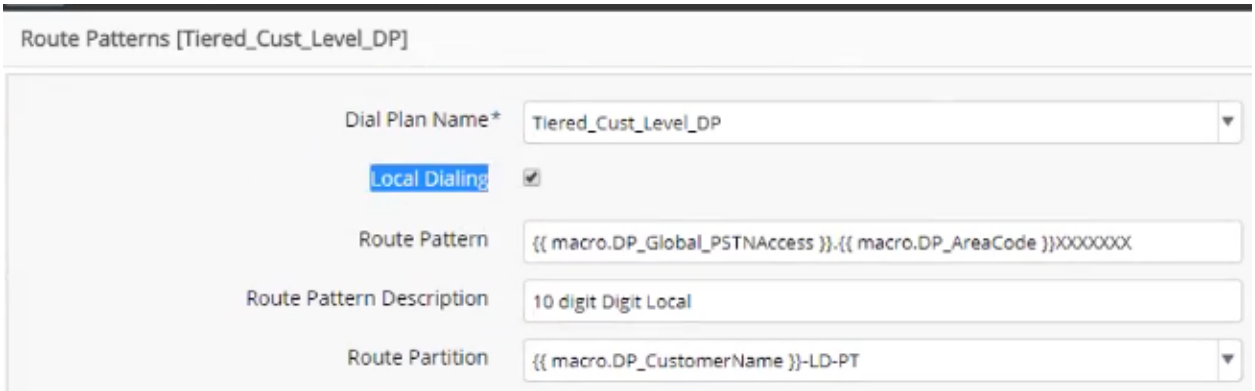
The remaining list of menus manage elements of dial plans created with the feature. Individual elements such as Route Patterns, SIP Trunks, and Translation Patterns each have a menu item from which it can be associated with a Dial Plan Model and managed.

The feature provides menu items or input fields to extend schema based dial plan management functionality. When a dial plan created with the feature is pushed from the **Dial Plan Maintenance** menu, the transaction log can be inspected to see the extended functionality:

- Device Pools - Regions - Locations -SRST
- Transcoders
- Conference Bridge
- Media Resource Groups
- Media Resource Group Lists
- Route Groups
- SIP Trunks
- CTI Route Points *with Lines* (Lines are not supported in schemas)

Copyright © 2025 VisionOSS Limited. All rights reserved.

When managing these dial plan elements, the installed named macros can be used to refer to data added from the **Dial Plan Input Data** menu.



The list view from each of these menus shows the Dial Plan Name - as defined from the **Dial Plan Model** menu - to which the element belongs. The feature structures the elements as instances of distinct data models.

There is an additional flexibility in the **Route Patterns** and **Translation Patterns** dial plan model elements so that a **Local Dialing** check box can be selected here if required when using a simpler or flat dial plan.

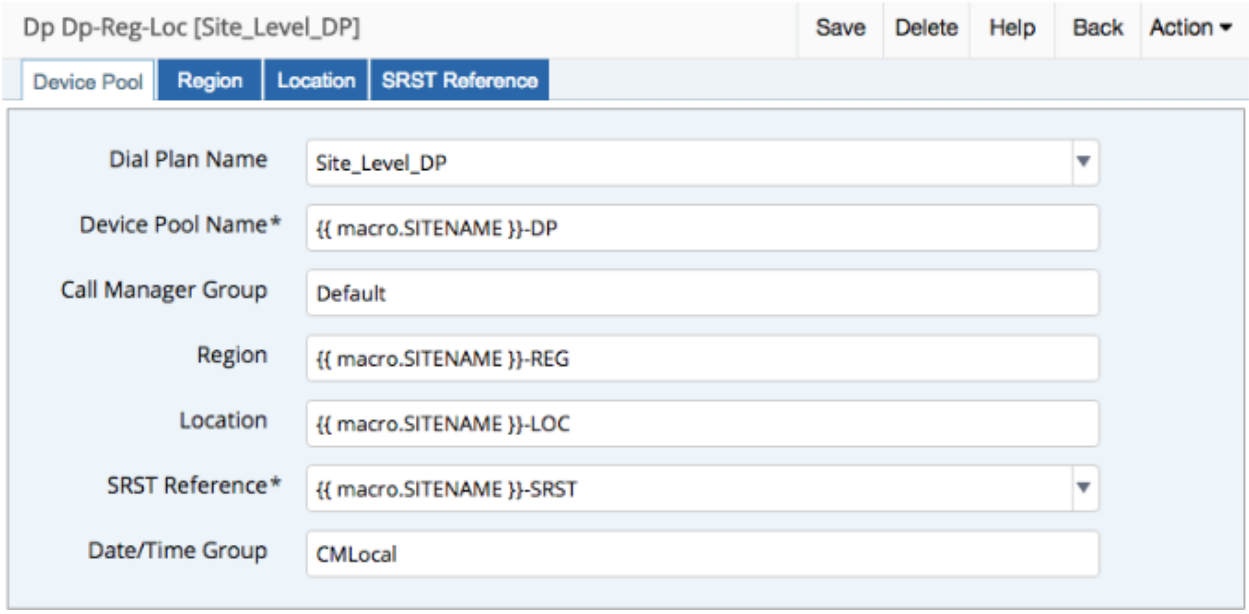
Dial Plan elements, such as Calling Search Space, can be cloned and edited to easily add another element to the dial plan by defining an “add-on” dial plan model, associating the cloned CSS element with it and pushing it to the required Call Manager cluster using the **Dial Plan Maintenance** menu. In this way the dial plan can be then be updated - functionality that is not possible in a schema based approach.

Additional workflows in the feature allow for values (for example MRGL) to be added from for example the **Device Pools - Regions - Locations -SRST** element input form, since the workflow will push to the these to the Call Manager cluster *only after* the prerequisite values become available. Inspect the transaction log to see the required sequence of data carried out with these workflows.

Device pools, regions, locations, SRST

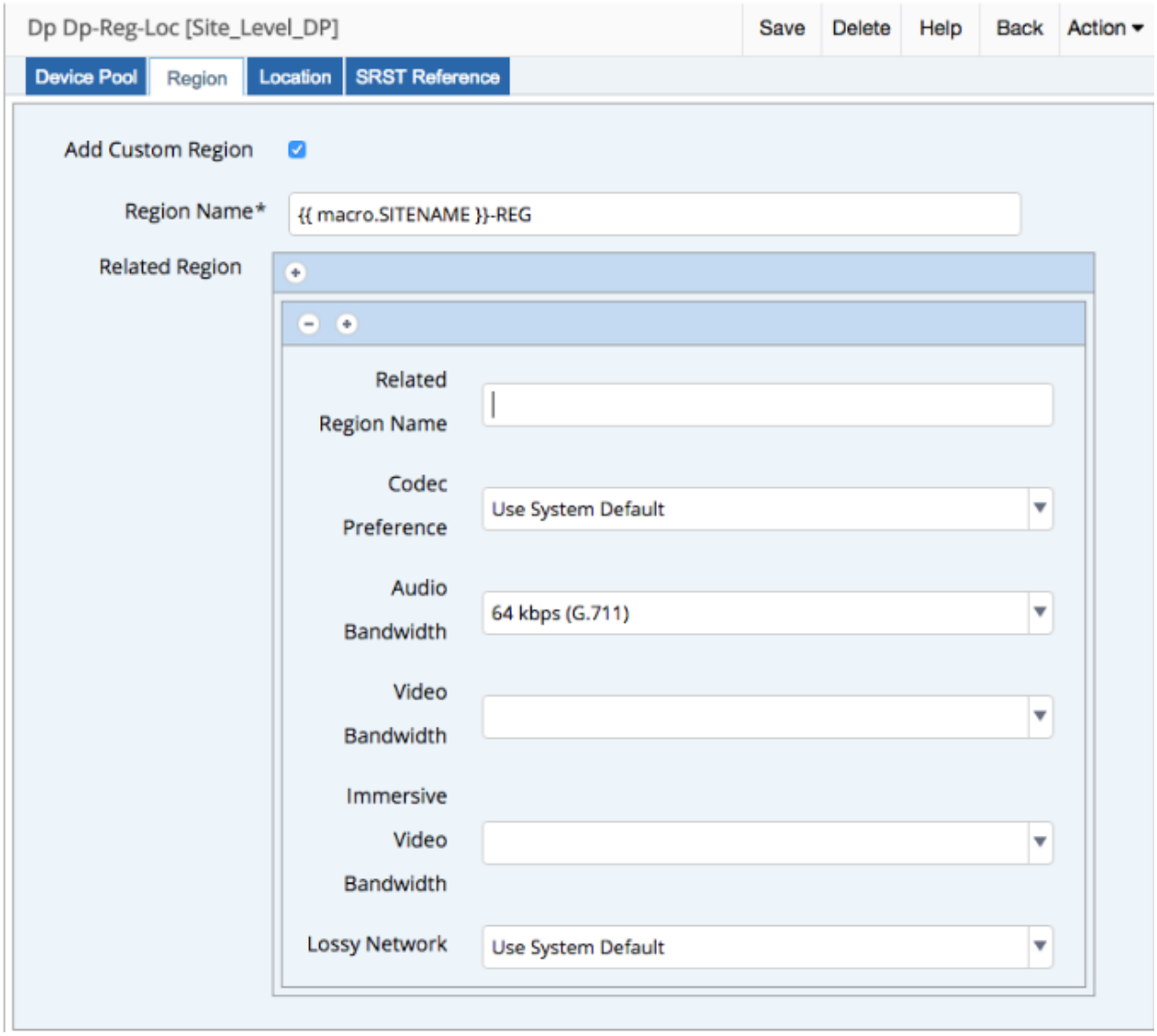
The Device Pool, Region, Location and SRST Reference dial plan model have been combined into one coherent data model for ease of entry into a call manager since the elements are often related.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- **Device Pool** tab fields:
  - **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
  - **Device Pool Name**: Free text field to add a device pool name or macro. In this example the name is built using a macro reference and a static extension of `-DP`.
  - **Call Manager Group**: Free text field to add a call manager group name.
  - **Region**: Free text field to enter a call manager existing region to the device pool or the field will automatically update with the name of the custom added region from the **Region** tab.
  - **Location**: Free text field to enter a call manager existing location to the device pool or the field will automatically update with the name of the custom added location from the **Location** tab.
  - **SRST Reference**: Free text field to enter a call manager existing SRST reference to the device pool or the field will automatically update with the name of the custom added SRST reference from the **SRST Reference** tab.
  - **Date/Time Group**: Free text field to add a date time group name.

Copyright © 2025 VisionOSS Limited. All rights reserved.

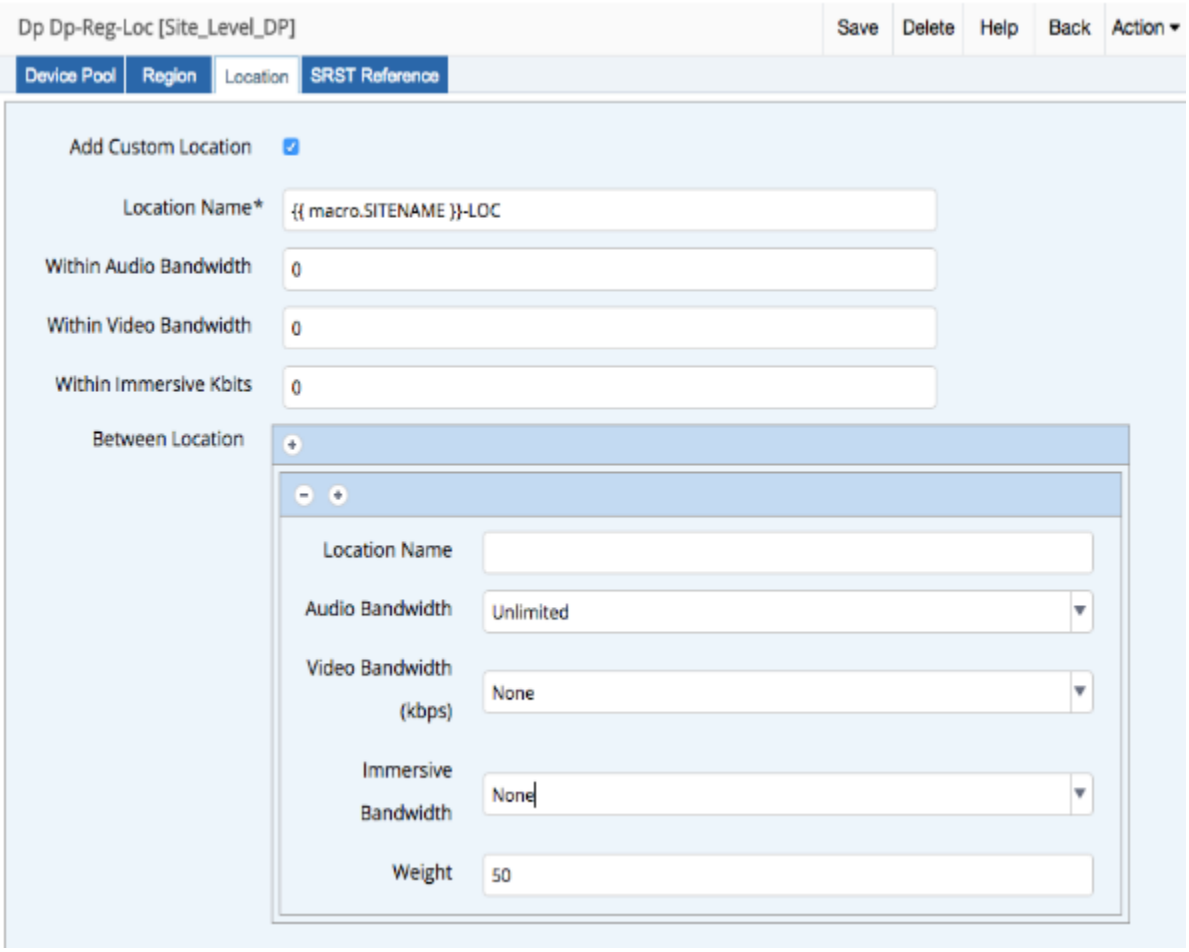


- **Region** tab fields:
  - **Add Custom Region**: Check box to optionally add a custom region.
  - **Region Name**: Free text field to add a region name. In this example the name is built using a macro reference and a static extension of `-REG`.
  - **Related Region**: Ability to add related regions to the custom region.
    - **Related Region Name**: Free text field to add a related region.
    - **Codec Preference**: Drop-down with choices:
      - Use System Default
      - Factory Default lossy
      - Factory Default low loss
    - **Audio Bandwidth**: Drop-down with choices:
      - Use System Default
      - 7 kbps (GSM-HR, G.723.1)

Copyright © 2025 VisionOSS Limited. All rights reserved.

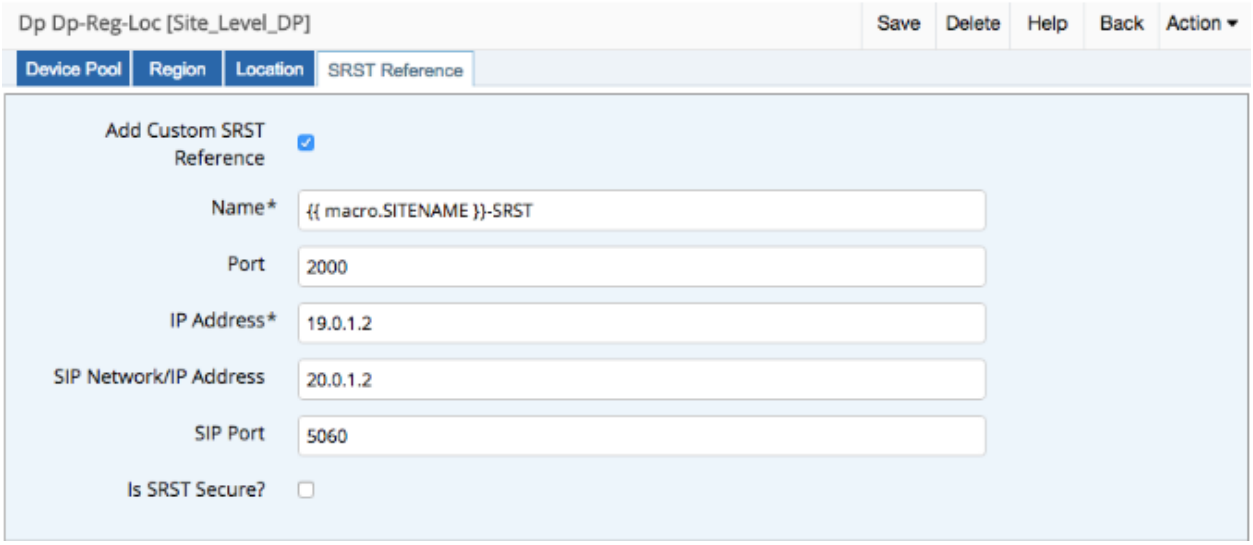
    - 8 kbps (G.729)
    - 13 kbps (GSM-FR, AMR)
    - 16 kbps (iLBC, G.728)
    - 24 kbps (AMR-WB)
    - 32 kbps (iSAC, G.722.1)
    - 64 kbps (G.711)
    - 128 kbps (AAC-LD [LATM])
    - 256 kbps (L16, AAC-LD)
  * **Video Bandwidth**: Drop-down to choose video bandwidth setting with choices:
    - Use System Default
    - Not Allowed
  * **Immersive Video Bandwidth**: Drop-down to choose immersive video bandwidth with choices:
    - Use System Default
    - Not Allowed
  * **Lossy Network**: Drop-down to choose lossy network setting with choices:
    - Use System Default
    - Keep Current Setting
    - Low Loss
    - Lossy

Copyright © 2025 VisionOSS Limited. All rights reserved.



- **Location** tab fields:
  - **Add Location**: Check box to optionally add a custom Location.
  - **Location Name**: Free text field to add a location name. In this example the name is built using a macro reference and a static extension of `-LOC`.
  - **Within Audio Bandwidth**
  - **Within Video Bandwidth**
  - **Within Immersive Kbits**
  - **Between Location** group of fields:
    - **Location Name**
    - **Audio Bandwidth**
    - **Video Bandwidth**
    - **Immersive Bandwidth**
    - **Weight**

Copyright © 2025 VisionOSS Limited. All rights reserved.

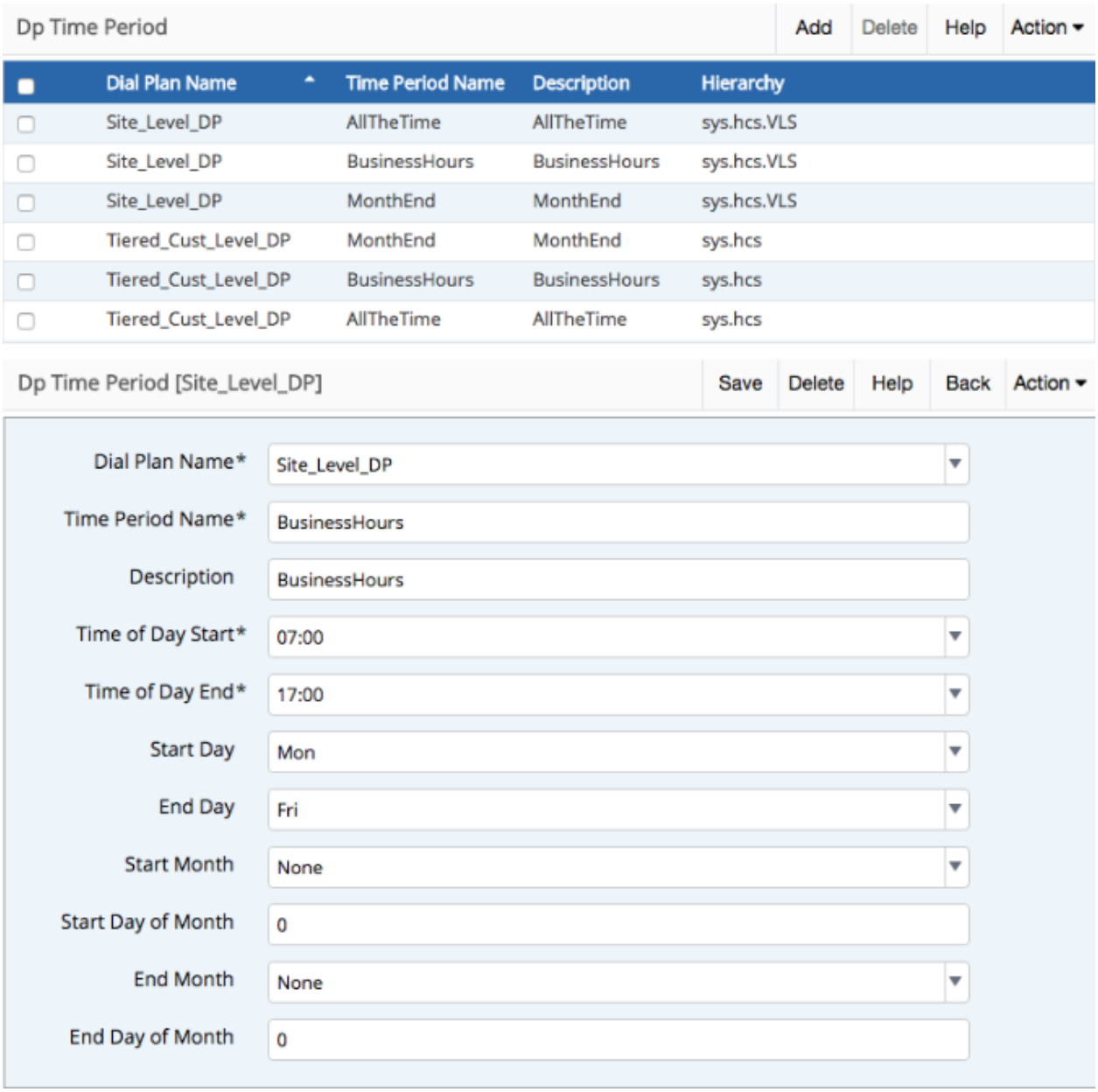


- **SRST Reference** tab fields:
  - **Add SRST Reference**: Check box to optionally add a custom SRST Reference.
  - **SRST Reference Name**: Free text field to add a SRST Reference name. In this example the name is built using a macro reference and a static extension of `-SRST`.
  - **Port**
  - **IP Address**
  - **SIP Network/IP Address**
  - **SIP Port**
  - **SRST Secure?**

Time period model

This allows the administrator to define an unlimited number of time periods.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Time Period fields:

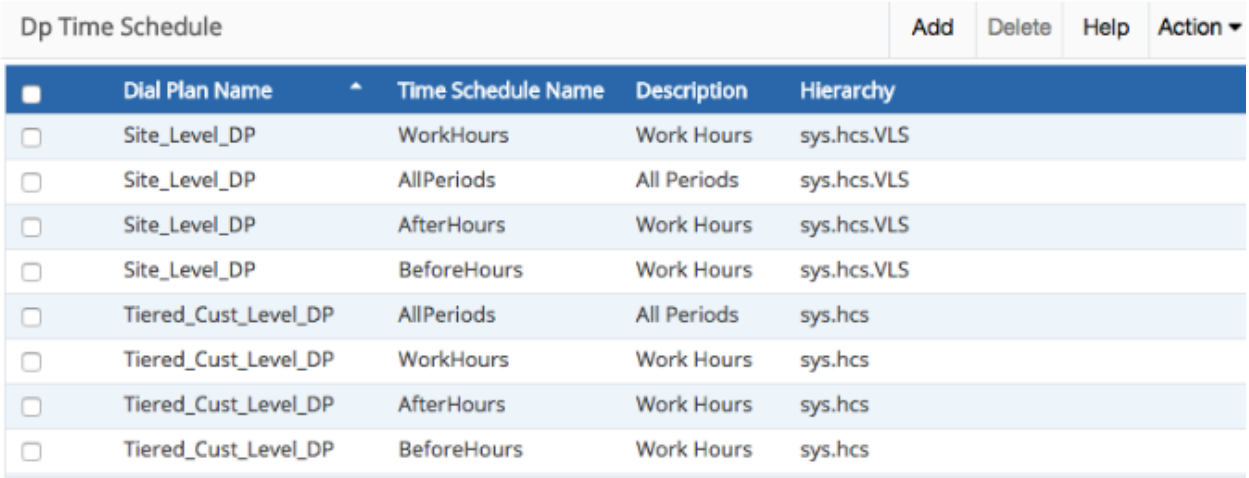
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Time Period Name**: The free text name for desired time period.
- **Description**: Meaningful description of the time period.
- **Time of Day Start**: Drop-down driven field to set start of time period in 15 minute increments.
- **Time of Day End**: Drop-down driven field to set end of time period in 15 minute increments.
- **Start Day**: Drop-down driven field to set start day giving “Mon”-“Fri” and “None” as options.
- **End Day**: Drop-down driven field to set end day giving “Mon”-“Fri” and “None” as options.
- **Start Month**: Drop-down driven field to set start month giving “Jan”-“Dec” and “None” as options.

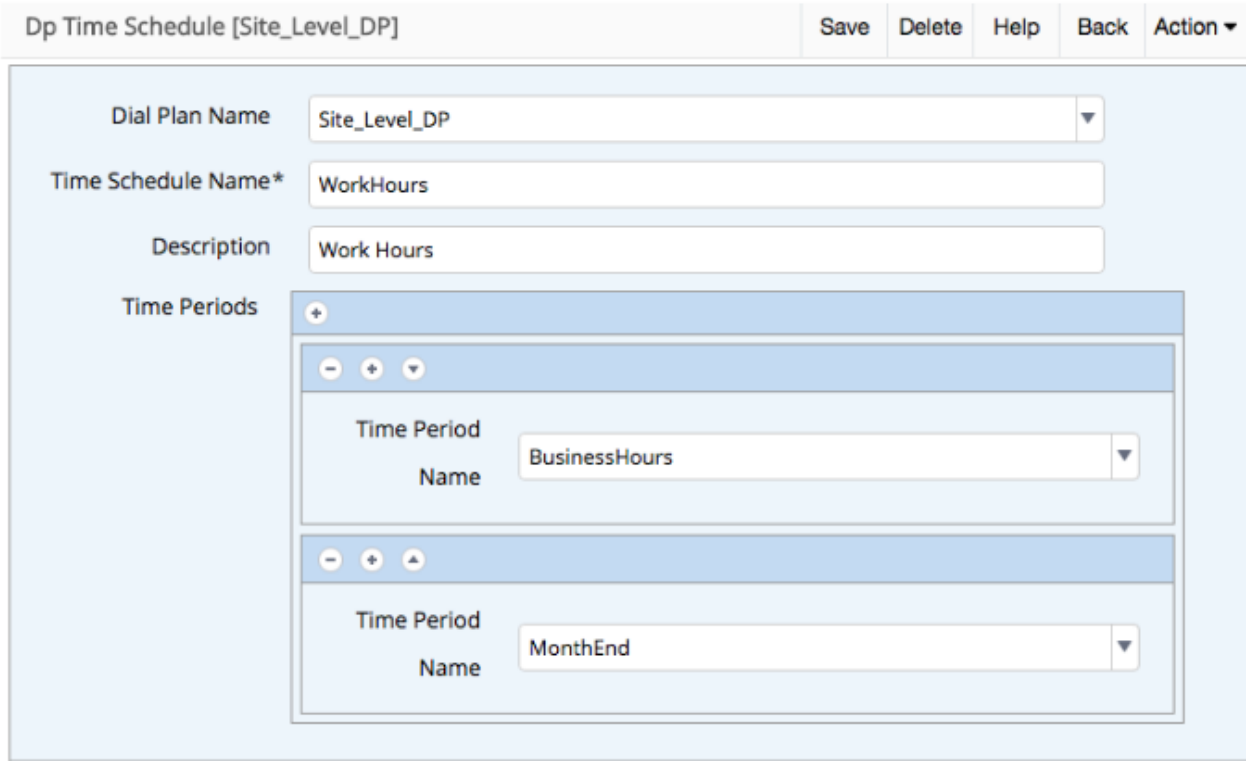
Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Start Month**: Drop-down driven field to set start month giving “Jan”-“Dec” and “None” as options.
- **Start Day of Month**: Free text field to add integer of start day of the month
- **End Month**: Drop-down driven field to set end month giving “Jan”-“Dec” and “None” as options.
- **End Day of Month**: Free text field to add integer of start day of the month.

Time schedule model

This allows the administrator to define an unlimited number of time schedules.





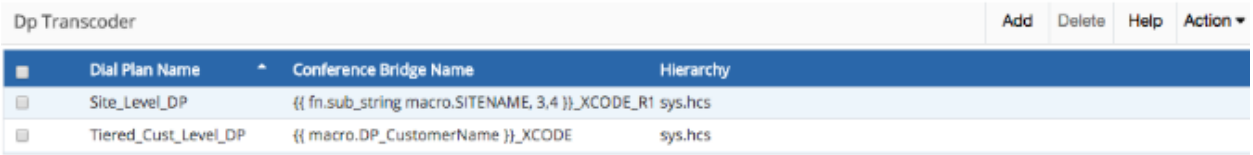
Time Schedule fields:

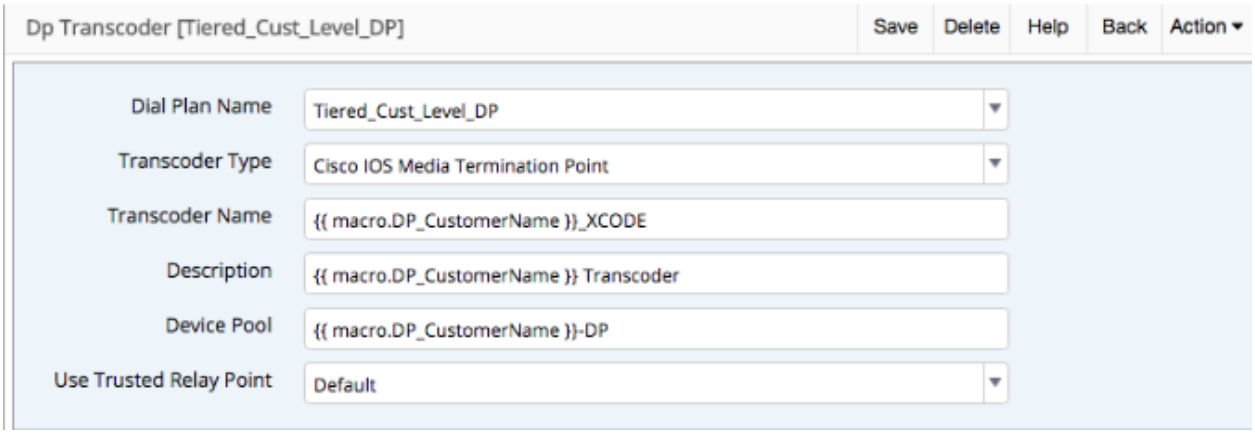
Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Time Schedule Name**: Free text field to enter a unique time schedule name.
- **Description**: Meaningful description of the time schedule.
- **Time Periods**: An array of time periods that provides drop-downs of time periods defined from the Time Period.

Transcoder model

The transcoder dial plan model allows the administrator to define an unlimited number of transcoders.





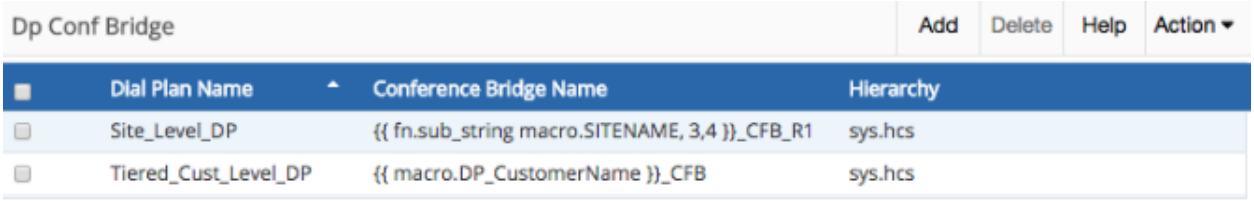
Transcoder fields:

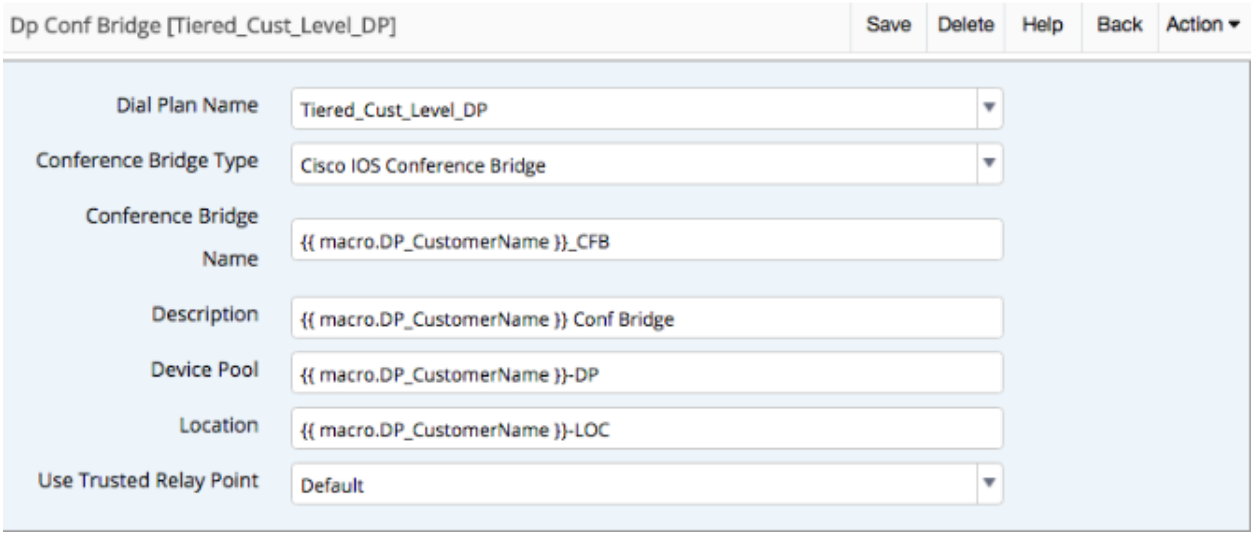
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type
- **Transcoder Type**: Drop-down field to set Transcoder Type. Currently only supports Cisco IOS Media Termination Point but will be expanded based on market input.
- **Transcoder Name**: Free Text field where a unique name should be entered. In the above example the macro will fill the Automate customer name with `_XCODE` suffix.
- **Description**: Meaningful description of the transcoder
- **Device Pool**: Free text field to identify the proper device pool.
- **Use Trusted Relay Point**: Drop-down with values:
  - Default
  - Off
  - On

Copyright © 2025 VisionOSS Limited. All rights reserved.

Conference bridge model

The Conference Bridge dial plan model allows the administrator to define an unlimited number of Conference Bridges.





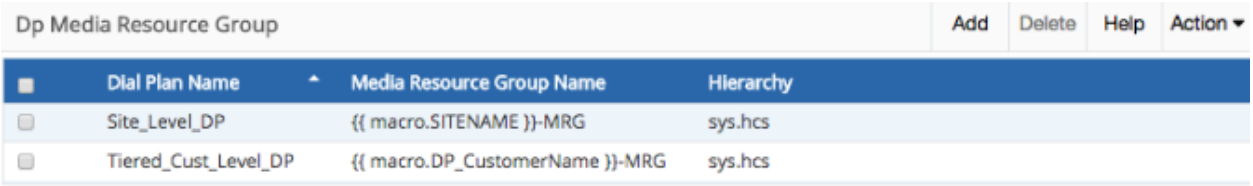
Conference Bridge fields:

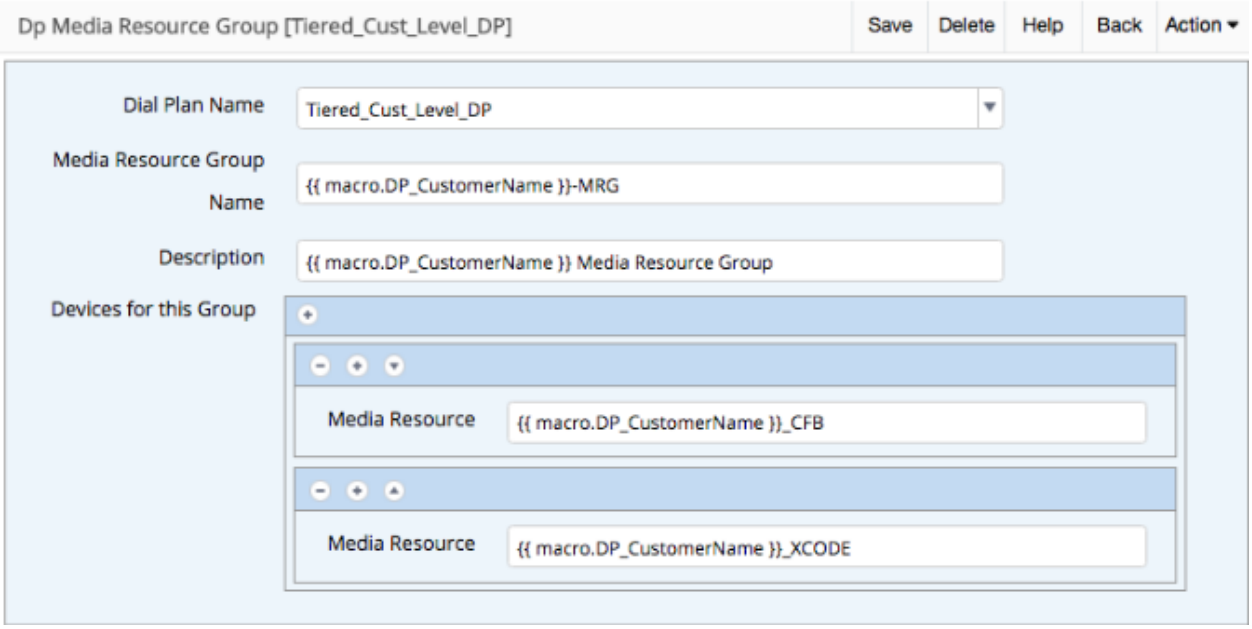
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Conference Bridge Type**: Drop-down field to set Transcoder Type. Currently only supports Cisco IOS Conference Bridge but will be expanded based on market input.
- **Conference Bridge Name**: Free Text field where a unique name should be entered. In the above example the macro will fill the Automate customer name with `_CFB` suffix.
- **Description**: Meaningful description of the Conference Bridge.
- **Device Pool**: Free text field to identify the proper Device Pool.
- **Location**: Free text field to identify the proper Location.
- **Use Trusted Relay Point**: Drop-down with values:
  - Default
  - Off
  - On

Copyright © 2025 VisionOSS Limited. All rights reserved.

Media resource group model

The Media Resource Group dial plan model allows the administrator to define an unlimited number of Media Resource Groups.





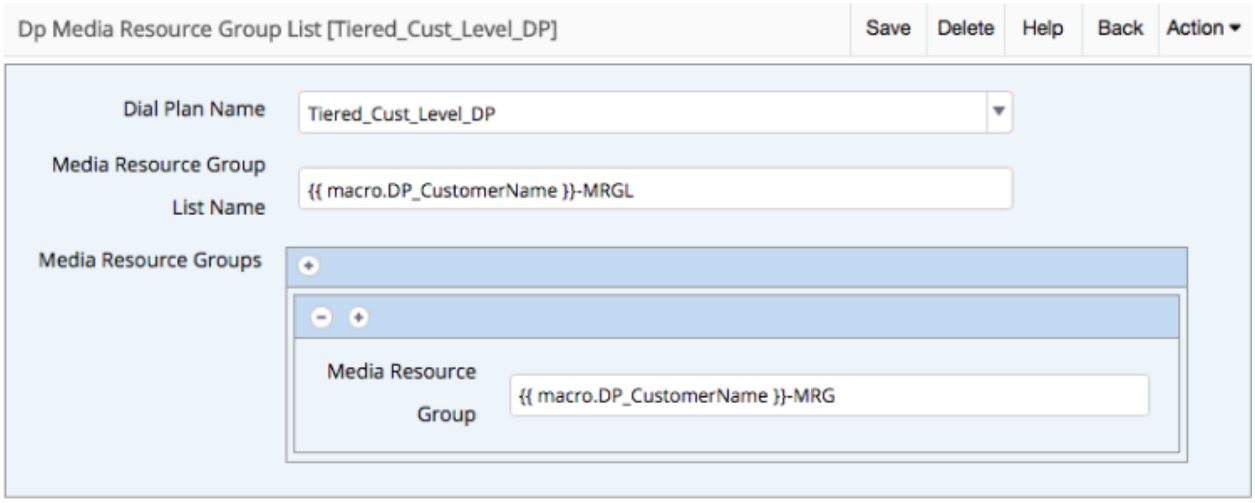
Media Resource Group fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Media Resource Group Name**: Free text field to enter a unique name for the Media Resource Group.
- **Description**: Meaningful description of the Media Resource Group.
- **Devices for this Group**: Array of member media resources for the Media Resource Group. In this instance using macros to enter the two customer level Transcoder and Conference Bridge instances.

Media resource group list model

The Media Resource Group List dial plan model allows the administrator to define an unlimited number of Media Resource Group Lists.

Copyright © 2025 VisionOSS Limited. All rights reserved.



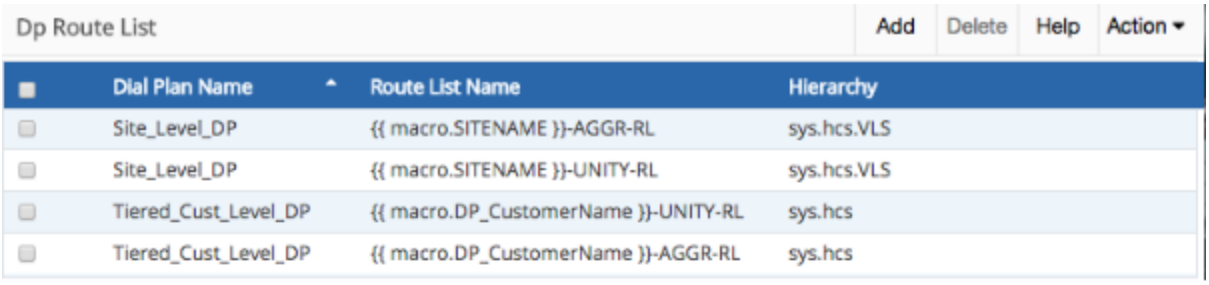
Media Resource Group List fields:

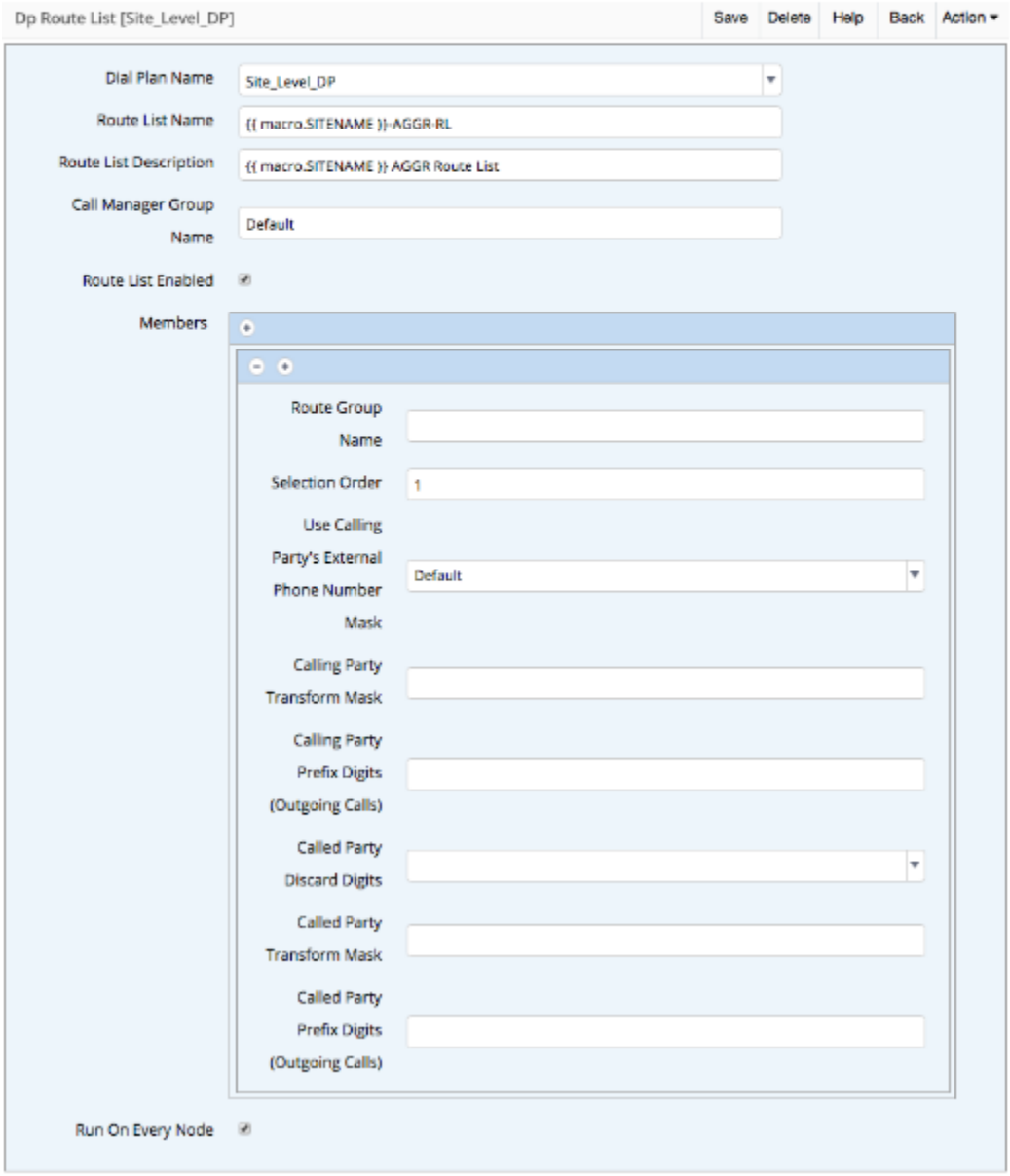
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Media Resource Group List Name**: Free text field to enter a unique name for the Media Resource Group List
- **Media Resource Groups**: Array of media resource groups to assign to the Media Resource Group List. In this example binding the customer level MRG.

Route list model

The Route List dial plan model allows the administrator to define an unlimited number of Route Lists.

Copyright © 2025 VisionOSS Limited. All rights reserved.





Route List fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Route List Name**: Free text field to enter a unique name for the Route List

Copyright © 2025 VisionOSS Limited. All rights reserved.

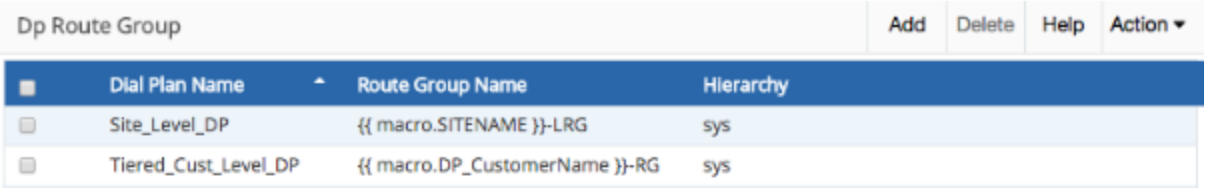
- **Route List Description**: Meaningful description of the Route List.
- **Call Manager Group Name: Free text field to designate the proper Call Manager** Group
- **Route list Enabled**: Check box to set the Route List Enabled field in Call Manager.
- **Members**: Array to enter member elements to the route list.
  - **Route Groups Name**: Free text field to assign a route group to the Route List.
  - **Selection Order**: The order in which the Route Groups will be placed in the Route List.
  - Use Calling Party's External Phone Number Mask: Drop-down providing Call Manager available options:
    - Default
    - On
    - Off
  - **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
  - **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
  - **Called Party Discard Digits**: Drop-down providing Call Manager available options:
    - None
    - PreDot
    - PreDot Trailing-#

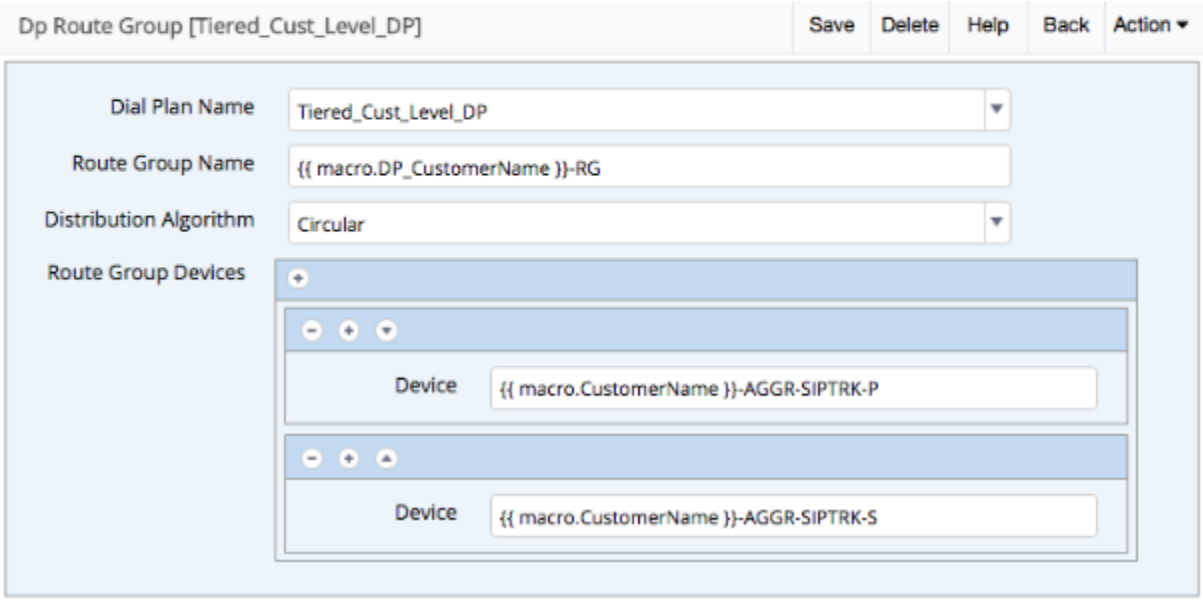
  Note that more discard instructions may be added at market demand.
  - **Called Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
  - **Called Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Called Party Prefix Digit data

Route group model

The Route Group dial plan model allows the administrator to define an unlimited number of Route Groups.

Copyright © 2025 VisionOSS Limited. All rights reserved.





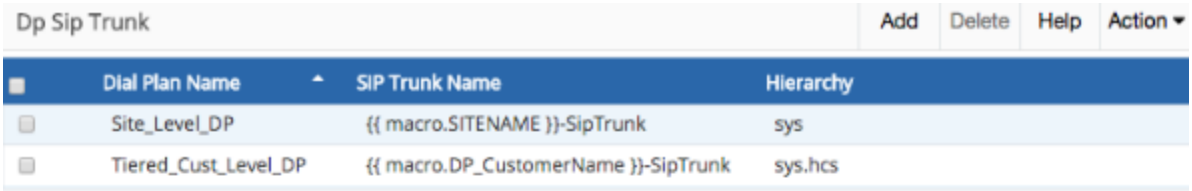
Route Group fields:

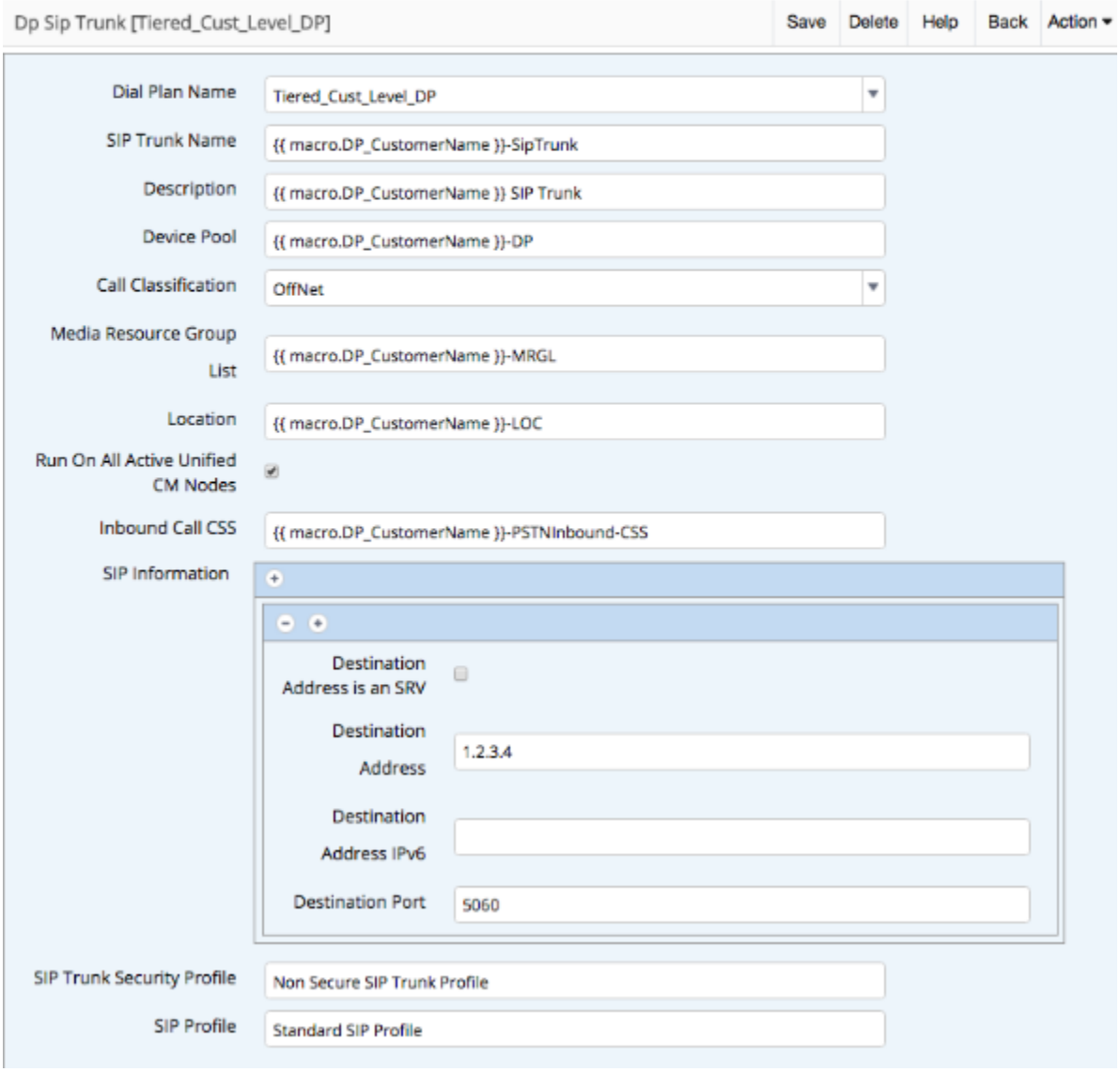
- **Dial Plan** Name: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Route Group** Name: Free text field to enter a unique name for the Route Group
- **Distribution Algorithm**: Drop-down providing the Call Manager options:
  - Top Down
  - Circular
  - Longest Idle Time
  - Broadcast
- **Route Group Devices**: Array to add devices to the route group. In this example a primary and secondary SIP trunk to aggregation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP trunk model

The SIP Trunk dial plan model allows the administrator to define an unlimited number of SIP Trunks.





SIP Trunk fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **SIP Trunk Name**: A unique identifier for the SIP Trunk
- **Description**: A descriptive name for the SIP Trunk.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Device Pool**: Free text field to enter the proper device pool for the trunk
- **Call Classification**: A drop-down to select a call manager. Options are:
  - Offnet
  - OnNet
  - Use System Default
- **Media Resource Group List**: Defines the proper media resource group list (MRGL) for the SIP Trunk.
- **PSTN Access**: Defines whether calls made through this SIP trunk may reach the PSTN. The default is false.
- **Location**: The location for the SIP Trunk, which defines the total bandwidth available for calls between this location and the central location, or hub. None specifies unlimited available bandwidth.
- **Run On All Active CM Nodes**: Defines whether to set the run on all nodes.
- **Inbound Call CSS**: Defines the proper CSS for SIP Trunks per dial plan.
- **Inbound Prefix DN**: Defines the prefix digits to append to the called party number on incoming calls. CUCM adds prefix digits after first truncating the number (based on the Significant Digits setting). You can use the exit code +
- **Incoming Number Prefix**: Typically used for outbound click-to-dial from a handset call history.
- **SIP Information**: Array to add multiple SIP IP Destination:
  - **Destination Address is an SRV**
  - **Destination Address**: The IPv4 IP address of the destination.
  - **Destination Address IPv6**: The IPv6 of the destination.
  - **Destination Port**: The TCP/IP port for the SIP Trunk instance.
- **SIP Trunk Security Profile**: Defines the SIP Trunk Security Profile.
- **SIP Profile**: Defines the SIP Profile.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Partition model

The Partition dial plan model allows the administrator to define an unlimited number of Partitions.

Dp Partition | Add | Delete | Help | Action

Dial Plan Name	Partition Name	Hierarchy
Site_Level_DP	{{ macro.SITENAME }}-PSTNInbound-PT	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-Unity-PT	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-INTL-PT	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-LD-PT	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-LOCAL-PT	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-PT	sys.hcs.VLS
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTERNAL-PT	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-PSTNInbound-PT	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LD-PT	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-Unity-PT	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTL-PT	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LOCAL-PT	sys.hcs

Dp Partition [Site_Level_DP] | Save | Delete | Help | Back | Action

Dial Plan Name	Site_Level_DP
Partition Name	{{ macro.SITENAME }}-PSTNInbound-PT
Partition Description	{{ macro.SITENAME }} PSTN Inbound
Partition Time Schedule	All the time

Partition fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Partition Name**: Free text field to enter a unique name for the Partition.
- **Partition Description**: Meaningful description of the Partition.
- **Partition Time Schedule**: Time schedule for the Partition if required per dial plan. May be left blank.

Copyright © 2025 VisionOSS Limited. All rights reserved.

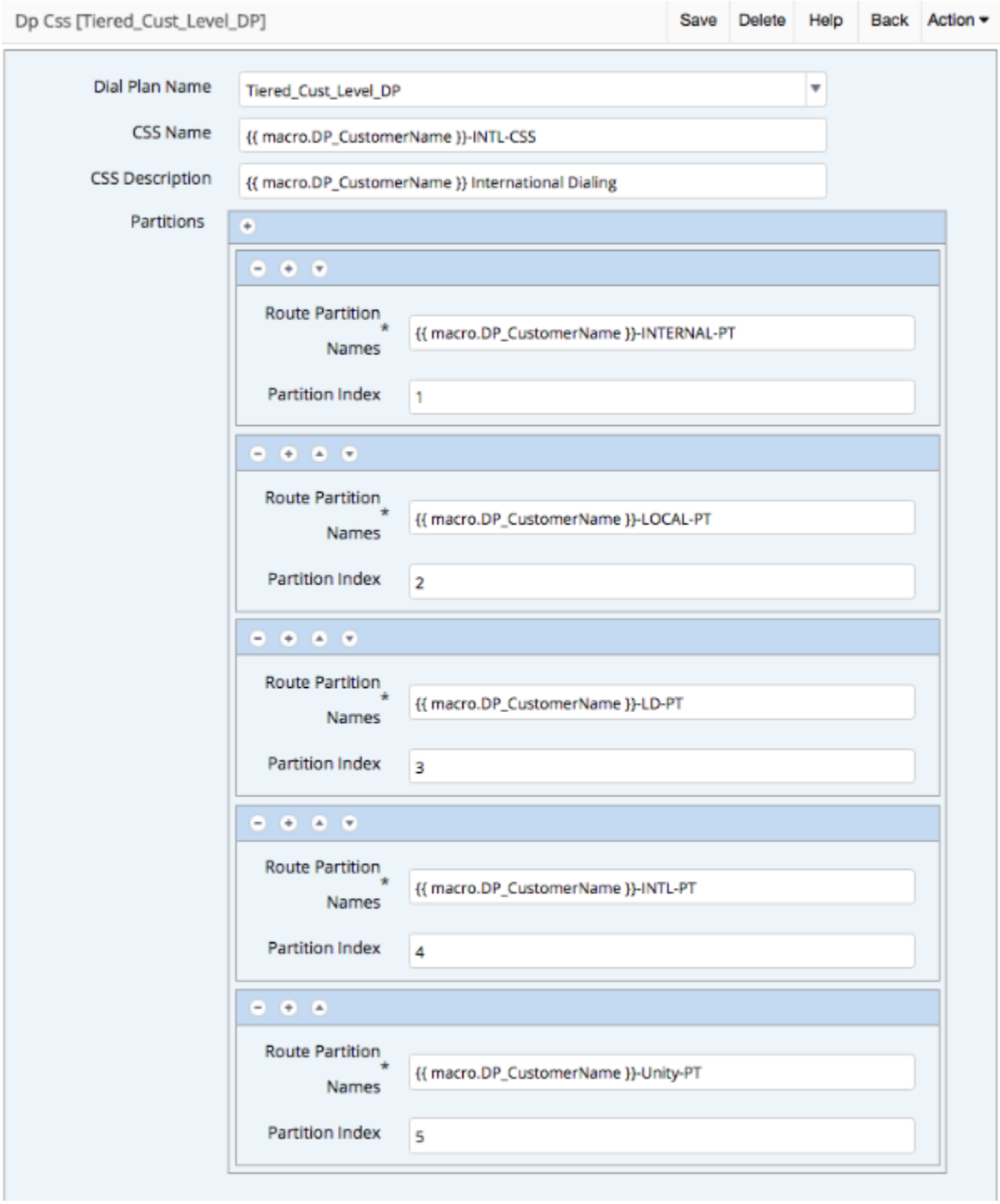
Calling search space model

The Calling Search Space (CSS) dial plan model allows the administrator to define an unlimited number of CSS.

Dp Css | Add | Delete | Help | Action

Dial Plan Name	CSS Name	Hierarchy
Site_Level_DP	{{ macro.SITENAME }}-PSTNInbound-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-LD-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-LOCAL-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-INTL-CSS	sys.hcs.VLS
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-PSTNInbound-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTL-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LD-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTERNAL-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LOCAL-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-LD-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-INTL-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-LOCAL-CSS	sys.hcs

Copyright © 2025 VisionOSS Limited. All rights reserved.



CSS fields:

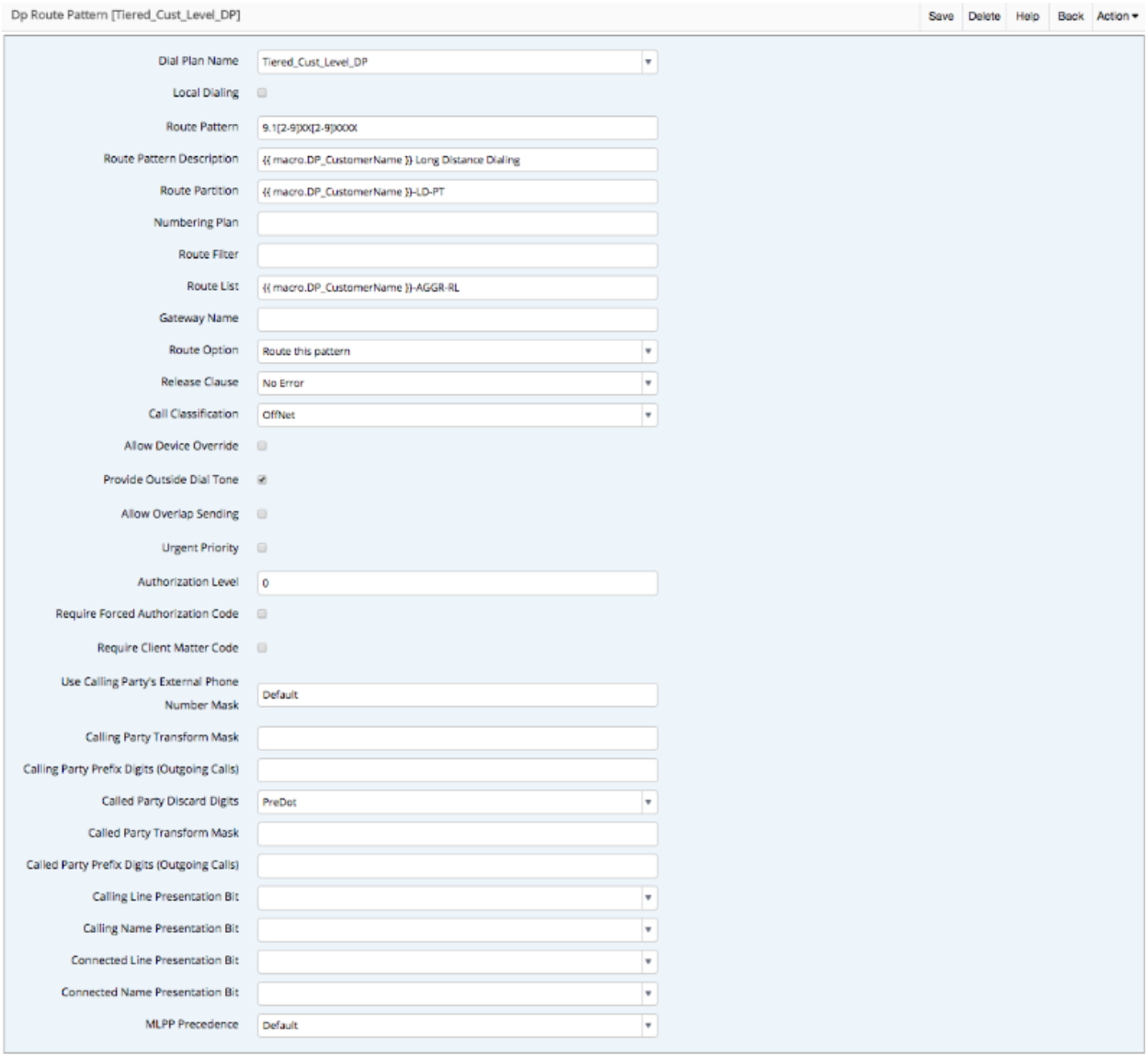
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **CSS Name**: Free text field to enter a unique name for the CSS.
- **CSS Description**: Meaningful description of the CSS.
- **Partitions**: Array to add Partitions associated in order to the CSS.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Route Partition Name**: Free text field to enter valid Partition name
- **Partition Index**: Free text field to enter the numeric id for Partition order.

Route pattern model

The Route Pattern dial plan model allows the administrator to define an unlimited number of Route Patterns. “Local Dialing” flag will be covered in a following section.



Route Pattern fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Local Dialing**: Check box to identify special patterns.
- **Route Pattern**: Free text field to enter a common Call Manager routing pattern.
- **Route Pattern Description**: Meaningful description of the Route Pattern.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Route Partition**: Free text field to enter a valid CUCM Partition.
- **Numbering Plan**: Free text field to enter a valid CUCM Numbering Plan if IDP is utilized.
- **Route Filter**: Free text field to enter a valid route filter name.
- **Route List**: Free text field to enter a valid route list name.
- **Gateway Name**: Free text field to enter a valid gateway name.
- **Route Option**: Drop-down providing Call Manager option:
  - Route this pattern
  - Block this pattern
- **Release Clause**: Drop-down providing Call Manager option:
  - No Error
  - Unallocated Number
  - Call Rejected
  - Number Changed
  - Invalid Number Format
  - Precedence Level Exceeded
- **Call Classification**: Drop-down providing Call Manager option:
  - Offnet
  - OnNet
- **Allow Device Override**: Check box to enable device override.
- **Provide Outside Dial Tone**: Check box to enable Outside Dial Tone.
- **Allow Overlap Sending**: Check box to enable Overlap Sending.
- **Urgent Priority**: Check box to enable Urgent Priority.
- **Authorization Level**: Free text box to enter Authorization Level as numeric value.
- **Require Forced Authorization Code**: Check box to enable Forced Authorization Code.
- **Require Client Matter Code**: Check box to enable Client Matter Code.
- **Use Calling Party's External Phone Number Mask**: Drop-down providing Call Manager available options:
  - Default
  - On
  - Off
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Called Party Discard Digits**: Drop-down providing Call Manager available options:
  - None
  - PreDot
  - PreDot Trailing-#

Copyright © 2025 VisionOSS Limited. All rights reserved.

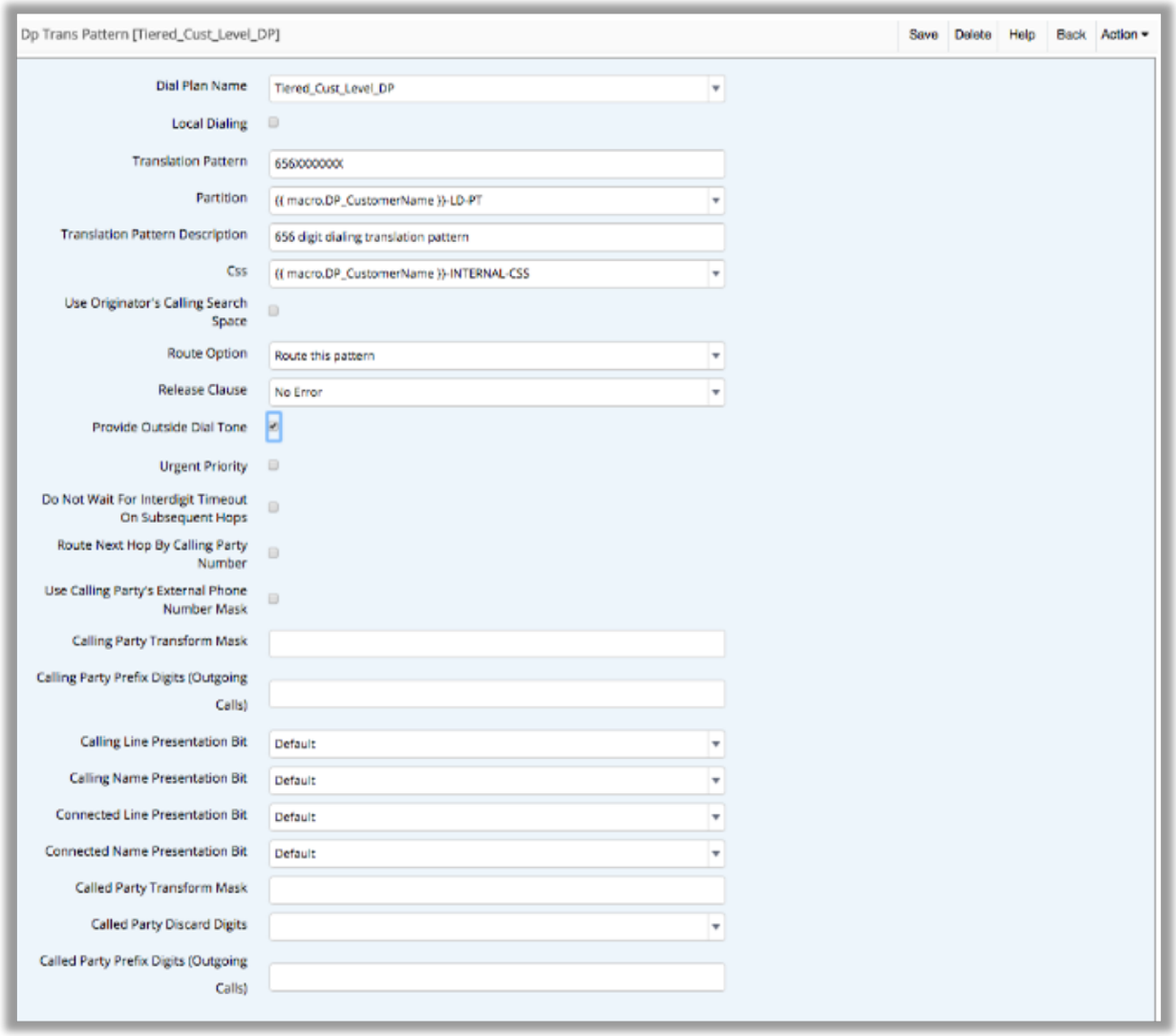
Note that more discard instructions may be added at market demand.

- **Called Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Called Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Called Party Prefix Digit data.
- **Calling Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **MLPP Precedence**: Drop-down providing Call Manager available options:
  - Default
  - Executive Override
  - Flash
  - Flash Override
  - Immediate
  - Priority
  - Routine

Translation pattern model

The Translation Pattern dial plan model allows the administrator to define an unlimited number of Translation Patterns. “Local Dialing” flag will be covered in the following section.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Translation Pattern fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Local Dialing**: Check box to identify special patterns.
- **Translation Pattern**: Free text field to enter a common Call Manager translation pattern.
- **Partition**: Free text field to enter a valid partition for the Translation Pattern.
- **Translation Pattern Description**: Meaningful description of the Translation Pattern.
- **Css**: Free text field to assign a valid CSS per the dial plan.
- **Route Option**: Drop-down providing Call Manager options:
  - Route this pattern
  - Block this pattern
- **Release Clause**: Drop-down providing Call Manager options:
  - No Error

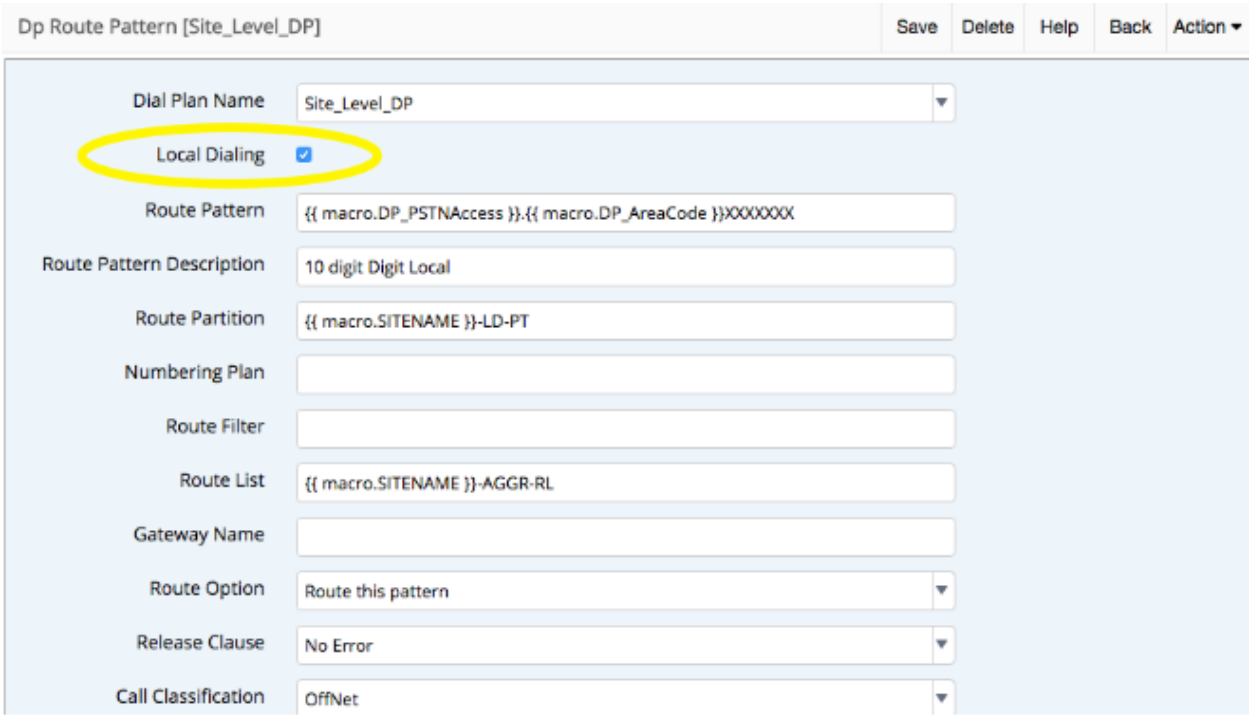
Copyright © 2025 VisionOSS Limited. All rights reserved.

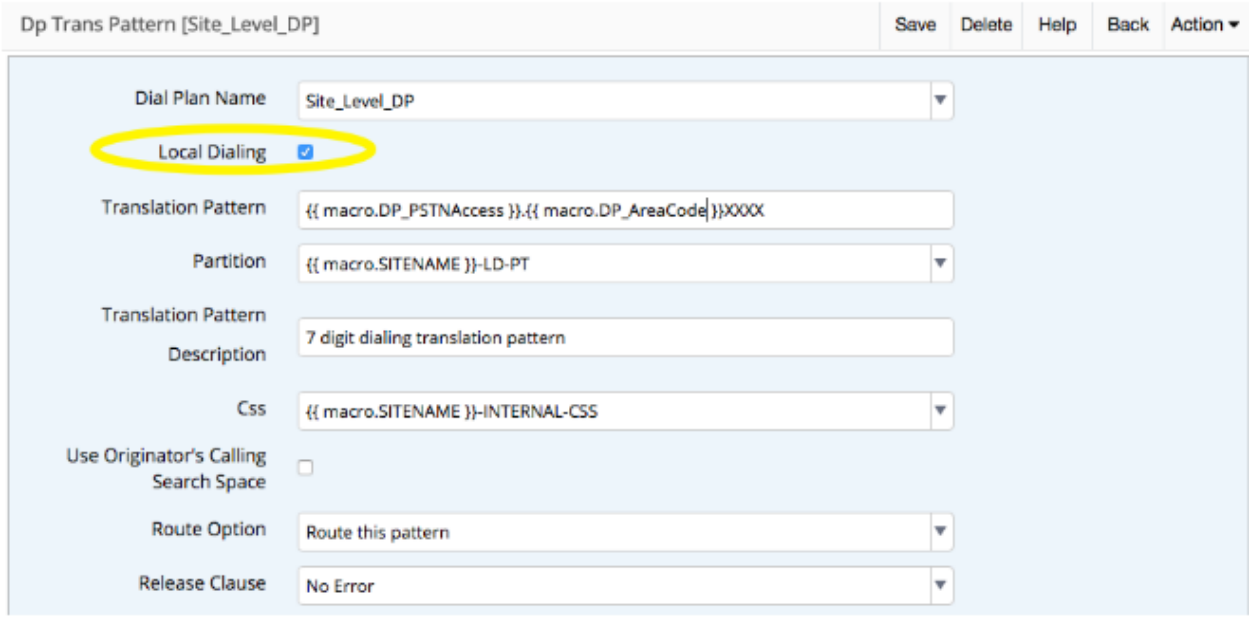
  - Unallocated Number
  - Call Rejected
  - Number Changed
  - Invalid Number Format
  - Precedence Level Exceeded
- **Provide Outside Dial Tone**: Check box to enable Outside Dial Tone.
- **Urgent Priority**: Check box to enable Urgent Priority.
- **Do Not Wait For Interdigit Timeout On Subsequent Hops**: Check box to bypass interdigit timeout.
- **Route Next Hop By Calling Party Number**: Check box to enable Route Next Hop By Calling Party Number.
- **Use Calling Party's External Phone Number Mask**: Check box to enable use of Calling Party's External Phone Number Mask.
- **Use Originator's Calling Search Space**: Check box to enable Originator's Calling Search Space.
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Calling Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Called Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Called Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Called Party Prefix Digit data.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Route pattern and translation pattern 'local'

The Translation/Route Pattern local designation in dial plan model allows the administrator to define patterns as local or looping patterns from the Site/Customer dial plan input sheet. The dial plan input sheets allow for creating a list of local area code/exchange that can be referenced via macro values to create site or customer level unique patterns.

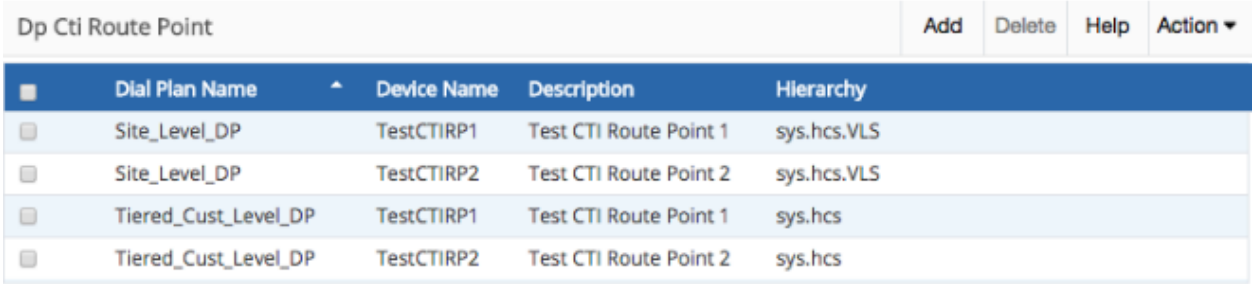


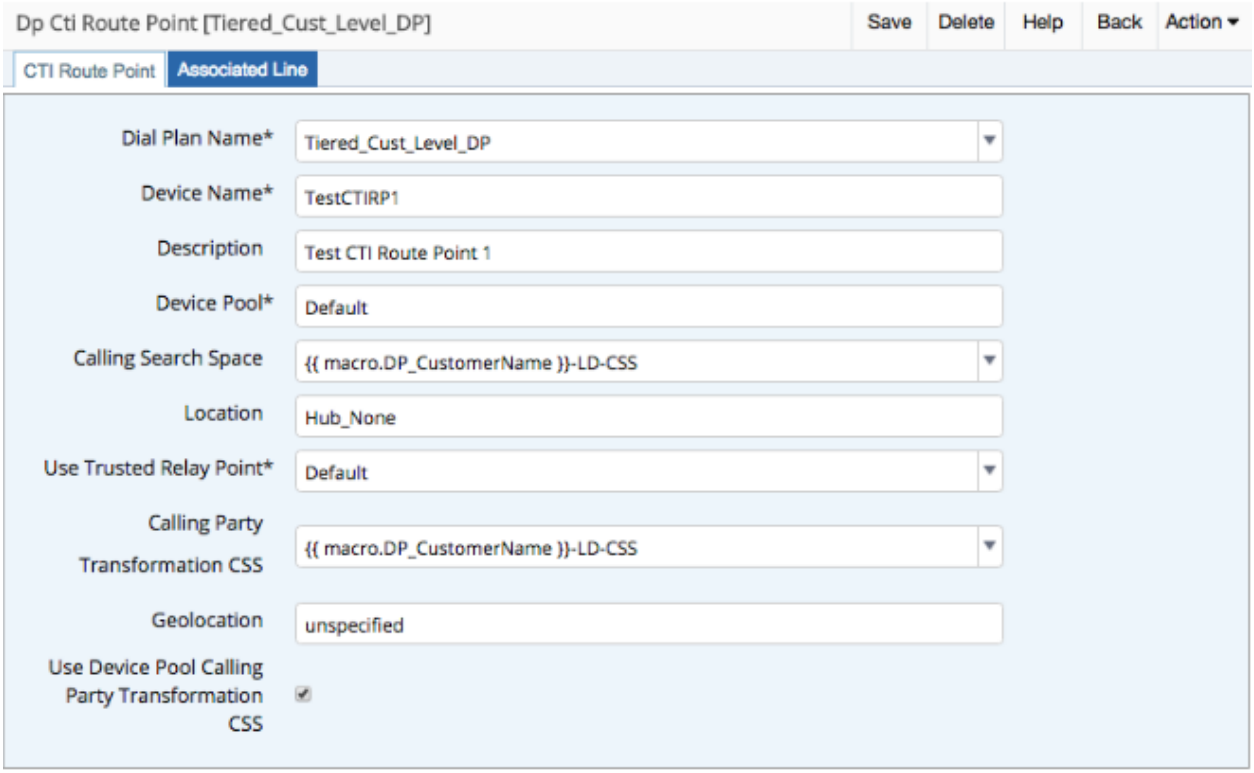


Copyright © 2025 VisionOSS Limited. All rights reserved.

CTI route points

The CTI Route Point dial plan model allows the administrator to define an unlimited number of CTI Route points with an associated line.





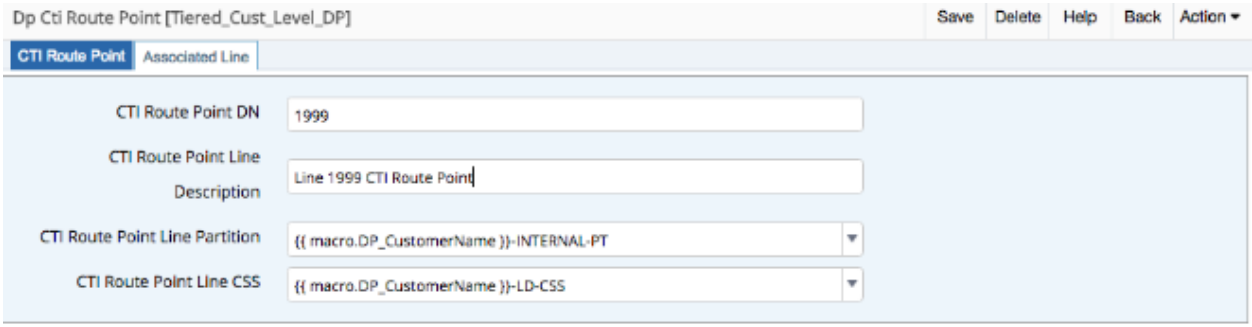
CTI Route Point Device fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Device Name**: The unique device name assigned to the CTI Route Point.
- **Description**: Meaningful description of the CTI Route Point.
- **Device Pool**: Free text field to enter the proper device pool for the CTI Route Point.
- **Css**: Drop-down field that provides a list of CSS from the dial plan css model.
- **Location**: Free text field to assign a valid Call Manager Location
- **Use Trusted Relay Point**: Drop-down with values:

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Default
  - Off
  - On

- **Calling Party Transformation CSS**: Drop-down field that provides a list of CSS from the dial plan css model.
- **Geolocation**: Free text field to enter a geolocation if necessary.
- **Use Device Pool Calling Party Transformation CSS**: Check box to enable Use Device Pool Calling Party Transformation CSS.



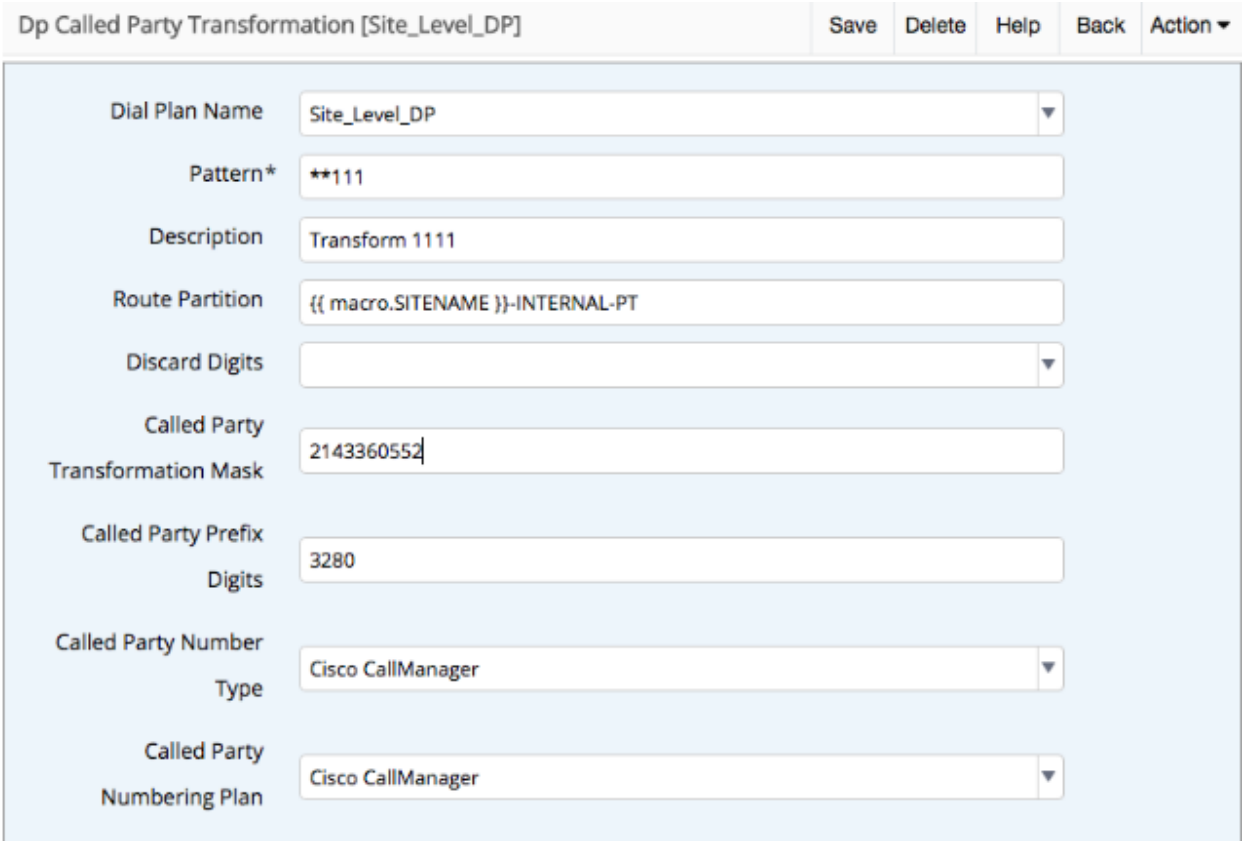
CTI Route Point Line Fields:

- **CTI Route Point DN**: The back end system will take the input from this field and create the Internal Number Inventory entry marked as used, then create a CUCM Line with the input number then finally associate the newly created line to the CTI Route Point.
- **CTI Route Point Line Description**: Meaningful description of the CTI Route Point Line.
- **CTI Route Point Line Partition**: Drop-down field that provides a list of Partitions from the dial plan partitions model.
- **CTI Route Point Line CSS**: Drop-down field that provides a list of CSS from the dial plan css model.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Called party transformation model

The Called Party Transformation dial plan model allows the administrator to define an unlimited number of Called Party Transformations.



Called Party Transformation fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Pattern**: Free text field to allow entry in standard Call Manager patterns.
- **Description**: Meaningful description of the Called Party Transformation.
- **Route Partition**: Free text field for entry of a valid Call Manager Partition.
- **Called Party Discard Digits**: Drop-down providing Call Manager available options:
  - PreDot
  - PreDot Trailing-#

Note that more discard instructions may be added at market demand.

- **Called Party Transformation Mask**: Free text field for entry of transformation mask.
- **Called Party Prefix Digits**: Free text field for entry of prefix digits.
- **Called Party Number Type**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - Unknown

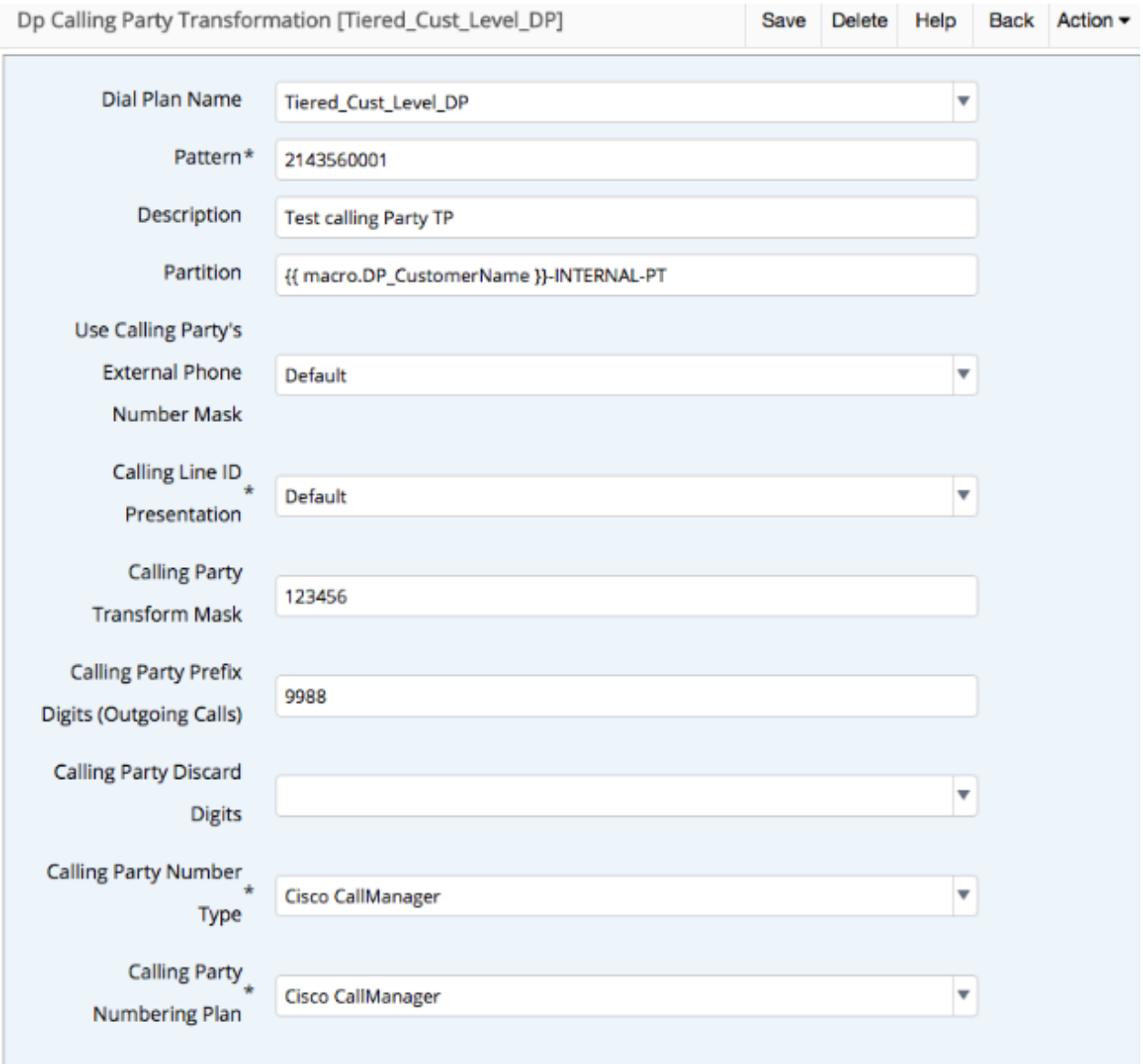
Copyright © 2025 VisionOSS Limited. All rights reserved.

  - National
  - International
  - User
- **Called Party Numbering Plan**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - ISDN
  - National Standard
  - Private
  - Unknown

Calling party transformation model

The Calling Party Transformation dial plan model allows the administrator to define an unlimited number of Calling Party Transformations.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Calling Party Transformation fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Pattern**: Free text field to allow entry of standard Call Manager patterns.
- **Description**: Meaningful description of the Called Party Transformation.
- **Partition**: Free text field for entry of a valid Call Manager Partition.
- **Use Calling Party's External Phone Number Mask**: Drop-down providing Call Manager available options:
  - Default
  - On
  - Off
- **Calling Line ID Presentation**: Drop-down providing Call Manager available options:

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Default
  - Allowed
  - Restricted
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Called Party Discard Digits**: Drop-down providing Call Manager available options:
  - PreDot

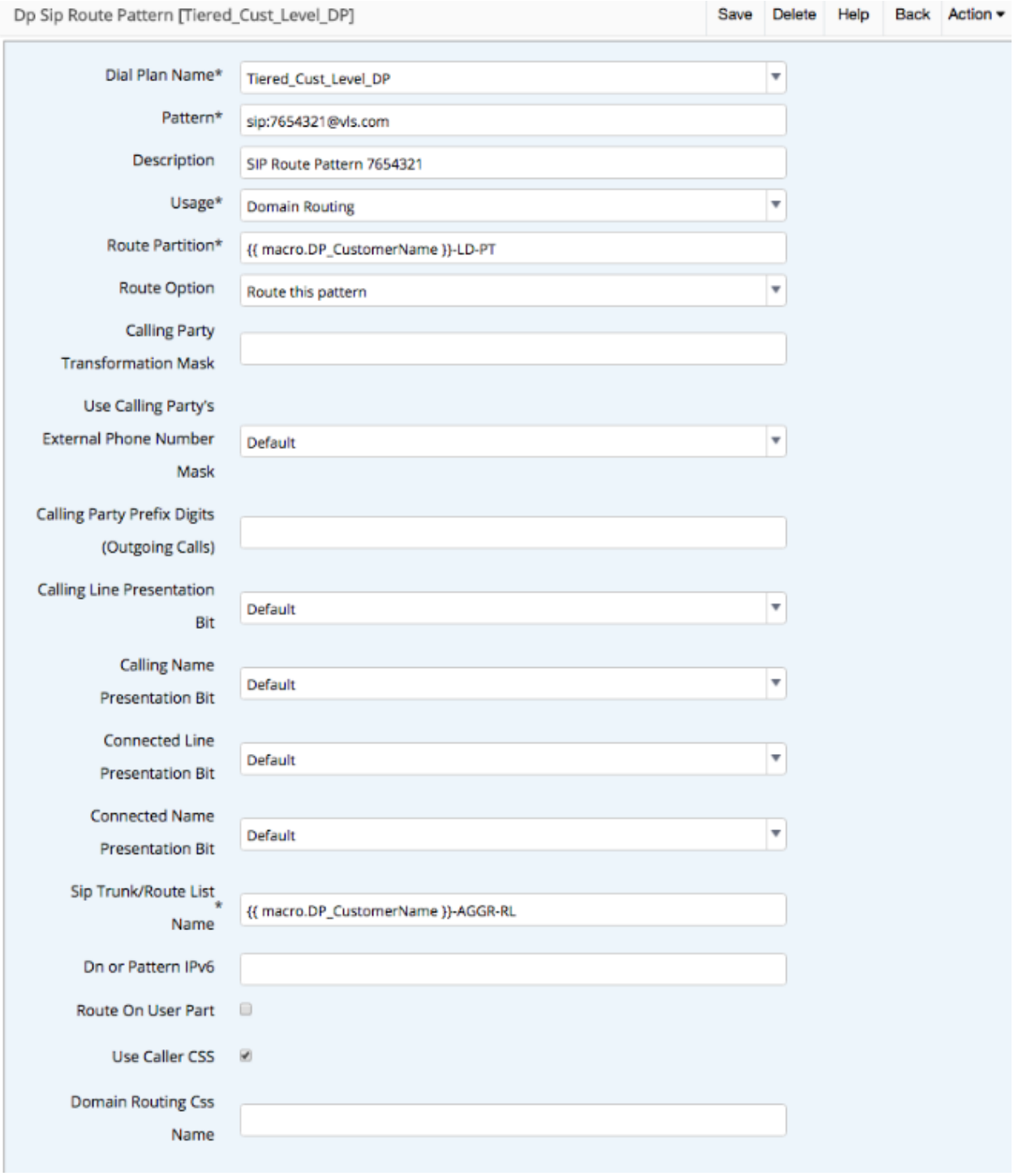
Note that more discard instructions may be added at market demand.

- **Called Party Number Type**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - Unknown
  - National
  - International
  - User
- **Called Party Numbering Plan**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - ISDN
  - National Standard
  - Private
  - Unknown

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP route pattern model

The SIP Route Pattern dial plan model allows the administrator to define an unlimited number of SIP Route Patterns.



SIP Route Pattern fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Pattern**: Free text field to allow entry in standard Call Manager patterns uri patterns.
- **Description**: Meaningful description of the SIP Route Pattern.
- **Usage**: Drop-own providing Call Manager options:
  - Domain Routing
- **Route Partition**: Free text field for entry of a valid Call Manager Partition.
- **Route Option**: Drop-down providing Call Manager options:
  - Route this pattern
  - Block this pattern
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data
- **Use Calling Party's External Phone Number Mask**: Drop-down providing Call Manager available options:
  - Default
  - On
  - Off
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Calling Line ID Presentation**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Name Presentation Bit**: Drop-down providing Call Manager available options:

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Default
  - Allowed
  - Restricted
- **Sip Trunk/Route List Name**: Free text field for entry of a valid SIP Trunk or Route List Name.
- **Dn or Pattern IPv6**: Free text field for entry of Dn or Pattern IPv6.
- **Route On User Part**: Check box to enable Route On User Part.
- **Use Caller CSS**: Checkk box to enable use of Caller CSS.
- **Domain Routing Css Name**: Free text field for entry of a domain routing CSS.

CUCM Music on Hold

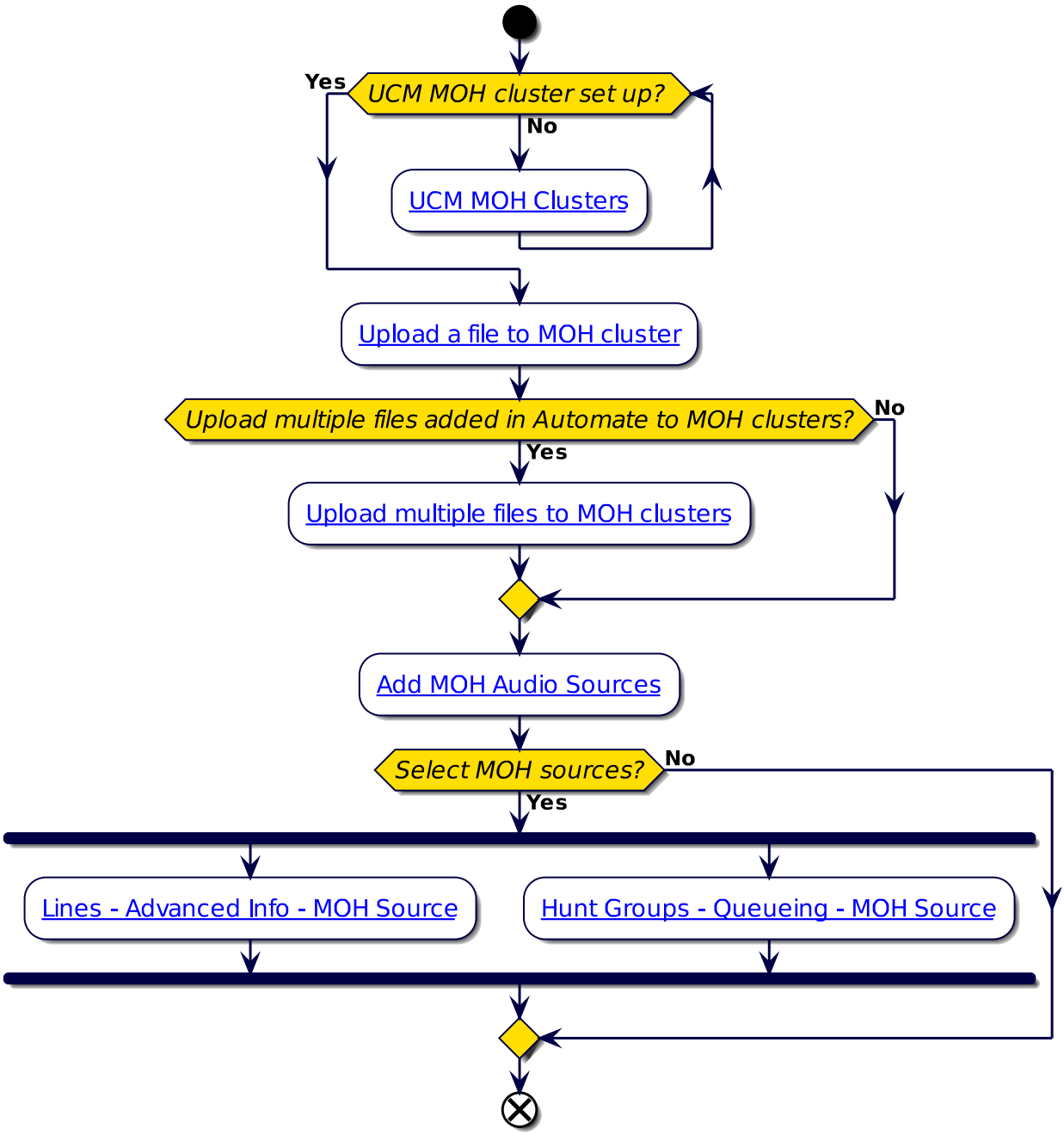
Cisco UCM Music on Hold (MOH) file management

Tip: *Use the Action search to navigate Automate*

Overview

Automate allows an administrator to manage Music On Hold (MOH) servers and files from within the Admin Portal, and to upload MOH files to Cisco UCM (UCM).

Copyright © 2025 VisionOSS Limited. All rights reserved.



Managing MOH files involves:

1. Adding a UCM MOH cluster for uploading MOH files.
2. Uploading MOH `.wav` files to Automate, and (optionally) to the UCM MOH cluster. Automate syncs the file to UCM once it's added to the UCM MOH cluster.
3. Adding MOH audio sources for use in Automate (for example, to manage lines and hunt groups).

Note: Deleting a `.wav` file from Automate does not remove the file from UCM MOH clusters.

A MOH file you're adding is uploaded to the Automate database, and if you selected a MOH cluster, the file

Copyright © 2025 VisionOSS Limited. All rights reserved.

is also added to the MOH cluster (to the publisher, and to any Cisco Subscriber servers flagged as music servers). A data sync is triggered to add the files to UCM, and any MOH files on UCM are imported to Automate in the sync. These MOH files are available for selection when adding or managing MOH audio source files.

Cisco UCM, MOH files, NDLs, and upgrading Automate

When uploading MOH files at site level, the UCM MOH cluster is automatically selected based on the site Network Device List (NDL).

Since data syncs export and import MOH files between Automate and UCM, when upgrading from a previous version of Automate, a workflow creates a new data sync entry for each of the existing call managers, and adds the call managers to the correct NDLs.

To view data sync entries, go to the **Data Sync** page. Data sync entries are prefixed with the name of the API (`CMCCS` - Call Manager Control Center Services)

Related topics

- *Introduction to data sync*
- *File management*

Add a UCM MOH cluster

This procedure adds a UCM MOH cluster.

Note: MOH files are uploaded to the UCM MOH cluster.

1. Log in to the Admin Portal.
2. Go to **Manage MOH Clusters**.
3. On the **Manage MOH Clusters** list view, click **Add** to open **Manage MOH Clusters**/**New Record**.
4. Fill out details for the new MOH cluster:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Cluster Name	Add a name for the UCM MOH cluster. You can use the same name as the UCM cluster, or a unique name.
Publisher Server Name	Choose a UCM publisher server from the list of available UCM publisher servers at the hierarchy.
Publisher Hostname or IP Address	This field is auto-populated once you choose a publisher server name. The value must match the SERVICE_PROVIDER_SPACE hostname or IPv4 address of the UCM publisher server. **Note:** By default, the port used to connect to the publisher is *443*.
Publisher username	Specify the username of a user with administrative access to the UCM server GUI.
Publisher Password	Specify the password of the publisher username.
UCM Subscriber Details	Click the Plus icon (+) to add UCM subscriber servers (one or more), and specify details for each subscriber server you're adding. These UCM subscriber servers are part of the UCM cluster. For each server you add, you will need to provide the following details: • Subscriber server name • Hostname or IP address • Username (and an associated password for this user) • Is Music Server - defines whether the subscriber server you're adding is a MOH server. MOH files are uploaded to a server with this setting enabled. At a minimum, you should add at least the subscriber with a MOH role (music servers). **Note:** The port used to connect to a subscriber server *443*.

5. Save your changes to add the UCM MOH cluster.

Copyright © 2025 VisionOSS Limited. All rights reserved.

View MOH Files

This procedure displays the list of files that exist on the Call Manager Publisher.

Note:

- Files uploaded to MOH clusters in Automate are imported to the database. An automatic sync is created for each of the CUCM (Call Manager Control Center Services MOHFile model sync, or CMCCS sync) so that you can run a manual data sync to update the list of files on this page.

  If you're upgrading to v21.2, you can immediately execute this data sync to import the files; else, they will be automatically imported automatically the next time you upload a new file to the CUCM.
- The menu for the MOH list view functionality is added to the default menus and access profiles for the following admin roles: Provider, Reseller, Customer

To view the list of MOH files:

1. Log in to the Admin Portal as a Provider, Customer, or Reseller admin.
2. Go to **List MOH Audio Files**.
3. In the list view, you can:
   - View the list of MOH files.

     Note: WAV files are stored in the database as XML files.
   - Export files (select the files you wish to export, and click the **Export** icon)

Upload a Single MOH File

This procedure uploads a `.wav` MOH file to the Automate database, and optionally also to a CUCM MOH cluster.

Note: You can upload the MOH file to the relevant CUCM at the same time as you add it to Automate, or after you've added the file to Automate.

When files are uploaded to a CUCM MOH cluster, files are uploaded to the publisher server, as well as to CUCM Subscriber servers that have the **Is Music Server** setting enabled.

To upload a MOH file:

1. Log in to the Admin Portal.
2. Go to **Manage Files and Upload to MOH Cluster**.
3. In the list view, click the Plus icon (+) to open the **Manage Files And Upload to MOH Cluster** / **New Record** page.
4. Click **Choose** to locate the `.wav` file from your filesystem.

   Note:

   - Once you've chosen the file, the name of the file displays in the **Filename** field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- If a file with same name as an existing file is uploaded at the same hierarchy, the existing file is automatically deleted.

5. Optionally, add a description for the file.
6. Optionally, at **CUCM MOH Cluster**, choose the relevant CUCM MOH cluster.

Note:

- If you don't choose a CUCM MOH cluster, the file is uploaded only to the Automate database.
- In the list view, when viewing a MOH file that has already been uploaded to a MOH cluster, you can select the MOH cluster to re-add the file to the cluster. MOH files you add to a MOH cluster here will display in CUCM.
- A `.wav` file that has previously been uploaded to Automate can be re-uploaded to the same CUCM MOH cluster, or to another CUCM MOH cluster.
- Deleting a `.wav` file from Automate does not remove the file from the CUCM MOH clusters.
- Uploading files to the pre-release version of CUCM 12.5.1 SU1(12.5.1.11900-20) will fail.

7. Save your changes.

Upload Multiple MOH Files

This procedure uploads two or more MOH files to CUCM MOH clusters.

1. Log in to the Admin Portal.
2. Go to **Upload Multiple Files to MOH Clusters**, then:
   - At **CUCM MOH Clusters**, choose the MOH cluster where you want to upload MOH files:
     - Move the MOH clusters you wish to use, from **Available** to **Selected**.
     - Move MOH clusters you don't want to use, from **Selected** to **Available**.
   - At **MOH File Names**, choose the MOH files you wish to upload:
     - Move the MOH files you wish to upload, from **Available** to **Selected**.
     - Move the MOH files you don't want to upload, from **Selected** to **Available**.

Note: Use the right and left arrows to move your choices to the relevant sides of the transfer boxes. Use the up and down arrows to re-position items in the transfer boxes.

3. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a MOH Audio Source

This procedure adds a MOH audio source instance, once MOH files have been added to CUCM.

Note: A MOH audio source instance is required in order to make use of the MOH files that have been uploaded to CUCM MOH clusters.

To add a MOH audio source:

1. Log in to the Admin Portal.
2. Go to **Add MOH Audio Source**.
3. At **CUCM MOH Cluster**, choose a CUCM MOH cluster where the audio source will be added.
4. At **MOH Audio Source Name**, provide a unique, descriptive name for the MOH audio source.

   Note: The MOH audio source name and the MOH audio file may be modified once you're created the MOH audio source.

5. At **MOH Audio Stream Number**, choose an available audio stream number.

   Note:

   - The drop-down displays only available stream numbers. The number `1` is reserved in CUCM, so only numbers from `002` display as available in Automate.
   - The following stream number is reserved for a fixed MOH audio source, and is not shown: `051`

6. At **MOH Audio Source File**, choose the MOH file previously uploaded to the CUCM MOH cluster.
7. Save your changes.

   Once you've added the first MOH audio source, Automate triggers a sync from CUCM to fetch all MOH audio sources. When you add a new MOH audio source, the workflow sync adds the new file to CUCM.

   MOH audio source files you add in Automate may be viewed, updated, or deleted via **Manage MOH Audio Source**.

Manage MOH Audio Sources

This procedure allows you to view and manage existing MOH audio sources.

Note: MOH audio sources you've added to the system are used for:

- Managing lines for users. See Directory Number Advanced Information in *Lines*
- Managing hunt groups for users. See Queuing in *Add a hunt group*

Copyright © 2025 VisionOSS Limited. All rights reserved.

View and Manage MOH Audio Sources

1. Log in to the Admin Portal.
2. Go to **Manage MOH Audio Source**.
3. View existing MOH audio sources in the **Manage MOH Audio Source** list view, and choose an action:
   - To delete a MOH audio source (one or more), select the checkbox for the relevant entries, and click the **Delete** icon.
   - To filter the list, click the toolbar **Filter** icon, or enter filter criteria in the column headers.
   - To move MOH audio sources (one or more), select the relevant checkboxes, and click the **Move** icon.
   - To view or update a MOH audio source, click on the relevant entry in the list to open its configuration screen. Go to step 4.
4. On the MOH audio source configuration page, view existing settings, and update relevant fields, as required:

MOH Audio Stream Number	Read-only. The default, reserved number in CUCM is *1*.
MOH Audio Source Name	Editable. The name of the MOH audio source.
MOH Audio Source File	WAV files uploaded and saved to the database as XML files. You can choose another file. The drop-down displays files on CUCM.
Initial Announcement	Choose an available initial announcement.
Play Initial Announcement to Hunt Pilot callers	Define whether to play an initial announcement. Clear the checkbox to disable this setting if an agent is available.
Periodic Announcement	Choose an available announcement from the drop-down.
Periodic Announcement interval	Enter a value, in seconds (10s - 300s). The default is 30s.
Locale Announcement	Choose a locale.

5. Save your changes. Updates are added to CUCM.

Cisco FAC Management

Using Automate to manage FAC

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

The Automate FAC management feature and workflows push any added FAC codes to all the clusters at that hierarchy (e.g. all clusters at a customer). This means for deployments where consistent FAC codes are being used, these don't need to be managed per cluster by administrators.

The same applies for the delete FAC code scenario where you have the choice to remove it from a single cluster or all the clusters at that hierarchy level.

There is also a sync capability in the event that a new cluster is added and the existing codes needs to be pushed to the new cluster. This mode can be used for single cluster environments as well if needed.

The ability to define the relevant FAC code authorization levels and provide text naming for them helps to provide appropriate business context to the level for administrators.

By default Automate includes all the levels for use, however you can adjust these to your needs. For example, you can configure FAC so that only five levels are shown and they have the correct naming convention, e.g. 6 - International. See *Customize authorization levels* for more details.

Use this feature to manage FAC codes:

- Add a code to all clusters - browse to the level you want the code added. Use the view to enter the details for the code - the list of authorization levels is driven by the setup above. Click **Add**. This adds the FAC code to any cluster at that hierarchy level - so if there are three clusters at level, the code will be added to all three clusters.

  If the hierarchy only has a single cluster or is not a multi-cluster environment, then the code is only added to the single cluster.
- Add a code to only a single cluster.
- Update a code - open, edit and save- this will change the code on all clusters.
- Remove a code - from a single cluster or across all clusters.

Add FAC code

1. Navigate to the required customer or site level.
2. Go to **Forced Authorization Codes**.
3. Click **Add**.
4. Complete the following mandatory settings:

   See also: *Customize Help*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field Name	Description
Name*	A unique name describing the FAC code, e.g. Customer code + UserID. This name ties the authorization code to a specific user or group of users; and displays in the CDRs for calls that use this code. 50 characters maximum.
Authorization Level*	Select the authorization level in the range of 0 to 255. This can include a description after a delimiter, e.g. 1-international[1]. The drop-down contains all authorization levels that have been cloned to this hierarchy level. If none have been cloned, then the list displays the default auth levels 0-255. To successfully route a call, the user's Authorization Level must be equal to or greater than the Authorization Level set on the Route Pattern.
Code*	Enter a unique authorization code. The user enters this code when placing a call through a FAC-enabled route pattern. 16 digits maximum.

5. Click **Save** and inspect the entry in the list view.

Delete a FAC

When deleting FAC codes, all codes are listed for each Unified CM cluster. This allows the deletion of a code on a single cluster, even if it was added at customer level to multiple clusters.

1. Browse to the required customer or site hierarchy.
2. Go to **Forced Authorization Codes**.
3. Select the check box next to the FAC instance you want to delete or click on the FAC instance you want to delete.
4. Click **Delete** and then click **Yes** to confirm deletion.

Note: All instances of a FAC can also be deleted (across all clusters) by selecting the instance on the list view, and then clicking **Delete All Instances** on the toolbar.

Sync FAC code cross cluster

All codes can be synced across **all clusters** at the customer hierarchy.

1. Browse to the required customer hierarchy.
2. Go to **Sync FAC Codes Cross Clusters**.
3. Choose **Confirm**.
4. Click **Save**.

[1] See *Customize authorization levels*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Introduction to Forced Authorization Codes (FAC)

The Forced Authorization Codes (FAC) feature provides the ability to use codes to authorize certain types of calls as setup in the dial plan. For example, to make an international call, a code might be shared with people who need it and they can enter the code after dialing their call in order to authorize this.

To use FAC, the deployed dial plan must to be set up in a way that enables the codes to be used. For more details on the use of FAC and CUCM functionality, refer to the Cisco documentation.

VOSS Automate provides full support for FAC, from setting up the dial plan elements to the management of the codes themselves. Refer to the *VOSS Automate Provider HCS Dial Plan Management Support Guide* for more details on managing the dial plan elements.

VOSS Automate supports the provisioning of FAC using two methods:

- *Using device models to manage FAC* - this basically mirrors the setting up of codes in the Unified CM. It uses the device model in VOSS Automate and allows you to add/mod/del codes for a given cluster.
- *Using Automate to manage FAC* - this feature helps to improve the usability of FAC codes and to manage consistent FAC codes across clusters in an orchestrated way. It provides the ability to define which authorization levels you require and to provide text along with the code to help administrators understand the purpose of the different levels as implemented in the dial plan.

The method to use depends on your requirements, but generally the VOSS Automate FAC Code Management method is likely to be a better overall fit.

The appropriate option(s) you want to use should be included in your menu designs for the required roles for administrators to access. You may want to use both methods if you need to manage FAC codes per cluster in some cases, and across clusters for other cases. Any existing codes synced into VOSS Automate will appear in VOSS Automate and can be managed via either method.

Using device models to manage FAC

Tip: *Use the Action search to navigate Automate*

Overview

You will typically use device models to manage Forced Authorization Code (FAC) if you want to manage FAC codes within the context of a given cluster (or only have single cluster deployments).

You can add, modify, or delete FAC codes in the system, including via the bulk management tools in Automate. If there won't be large number of FAC codes implemented and/or this remains an advanced administration task, this might be the best approach.

To manage FAC codes using this method, select the FAC Codes menu (exposed via the `device/cucm/FacInfo` device model):

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a FAC code

1. Browse to the appropriate hierarchy level for the FAC code (e.g. Customer or Site).
2. Go to FAC Code to view the list of existing codes.
3. Click **Add**. If there is more than one Unified CM cluster at that hierarchy, then you will get a pop-up to choose the appropriate cluster.
4. Enter the details of the FAC code to be added in the form and click **Save**.

Modify an existing FAC code

1. Go to FAC Code to view the list of existing codes.
2. Use the filters and/or hierarchy breadcrumb to locate the code to modify and then select it.
3. Edit the settings and click **Save**.

Delete an existing FAC code

1. Go to FAC Code to view the list of existing codes.
2. Use the filters and/or hierarchy breadcrumb to locate the code(s) to delete.
3. You can either select the code(s) from the list view via the check boxes and click **Delete** OR open the appropriate code and click **Delete**.

Customize authorization levels

Tip: *Use the Action search to navigate Automate*

Go to **Customize Authorization Levels** to access the list of valid authorization (auth) levels and optional text.

These instances are hierarchy-specific so you can have different codes/text for different hierarchies, e.g. different customers or areas of the business.

The list of auth levels available in the drop-down can be customized. By default, numeric values 0 to 250 are shown.

If a customer only requires for example 0 to 6 auth levels, then a provider administrator can clone, edit and save those instances to the lower hierarchy level. Descriptive text can also be added to the cloned auth level first by adding a '-' and then a 'description' *after* the numeric value, for example:

1-Allow Local Calls, where:

- '1' is the numeric value that gets selected on the Unified CM
- '-' is the delimiter that separates the numeric value and description
- 'Allow Local Calls'- is the (example) friendly description that describes the numeric value action

Once cloned to Customer level, only the cloned versions are displayed in the **Authorization Level** drop-down when adding forced authorization code at Customer level or lower.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Customize Help

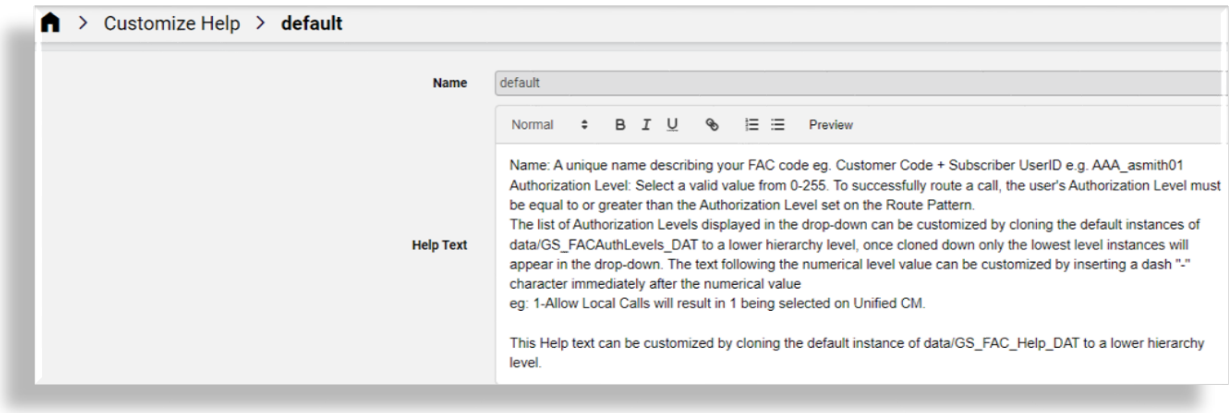
provider

Tip: *Use the Action search to navigate Automate*

This feature allows a Provider admin user to customize the CUCM FAC form help by cloning, then saving the help text on the **Customize Help** form to a lower hierarchy level.

Adding Help text to the codes allows administrators to understand the purpose of the different levels as implemented in the dial plan.

Help text can be added as Markdown or HTML in the input box and the Preview menu in the editor can then be used to show the formatted help text.



Related Topics

- *Introduction to Forced Authorization Codes (FAC)*

Calls Settings

Call park management

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate's Call Park feature (Call Park and Directed Call Park) allows you to manage call park numbers from the **Call Park** list.

Call parks can be added either individually or in bulk using number ranges.

Multiple call park numbers can be added in a single operation, which creates the required number of individual call park numbers instead of creating masked ranges of 10, etc.

Call park and directed call park can be configured as either service specific or clusterwide, dependent on the status of the **Enable Clusterwide CallPark Number/Ranges** parameter on the Unified CM.

Call park allows you to select directory numbers from a drop-down list, but also permits custom entries outside of the number inventory that can begin with '*' or '#', which are then added to the number inventory.

Note: Clusterwide call park numbers are available to devices hosted on any server within the CUCM cluster. If clusterwide call park is disabled, the call park numbers are only available to devices on the nominated CUCM server.

Clusterwide call park

Call park allows users to place a call on hold, so it can be retrieved from another phone in the system, for example, a phone in another office or in a conference room.

If your users are on an active call at your phone, they can park the call to a call park extension by pressing the **Park** softkey or the **Call Park** button. Someone on another phone in your system can then dial the call park extension to retrieve the call.

You can define either a single directory number or a range of directory numbers for use as call park extension numbers. Users can park only one call at each call park extension number.

Clusterwide directed call park

Directed call park allows a user to transfer a call to an available user-selected directed call park number.

Directed call park numbers are managed at site level, and allow a user to transfer a call to an available user-selected directed call park number. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number.

Only one call can be parked at each directed call park number. To retrieve a parked call, a user must dial a configured retrieval prefix followed by the directed call park number at which the call is parked. Configure the retrieval prefix on the **Directed Call Park Configuration** page.

Note: Whenever changes are made to directed call park numbers, any devices that are configured to monitor those directed call park numbers by using the directed call BLF must restart to correct the display. Change notification automatically restarts impacted devices when it detects directed call park number changes. You also can use the **Restart Devices** button on the **Directed Call Park Configuration** page.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Adding call parks

To add call parks:

1. Go to **CUCM** then choose either **Clusterwide Call Park** or **Clusterwide Directed Call Park**.
2. Click **Add**.
3. Browse to the required Site level.
4. Fill out at least the following mandatory fields:
   - Range Size* - Enter a range size of 1 or more.
   - First Call or Directed Call Park Number*
     - Displays call park numbers which are **not used** and **available**. If **Range Size** > 1, only contiguous ranges are made available.
     - Numbers beginning with '*' or '#' are allowed as free form numbers. However, numbers with this prefix cannot be created in the directory number inventory so directory number inventory management is not available.
   - Description - this description is used in the directory number inventory list view and also the Unified CM call park number.
   - Partition (Directed Call Park only) - The route partition of the directed call park range, selected from the drop-down list.
   - CUCM Server* - (Call Park only) - This field is mandatory, and a CUCM Server must be selected **IF** the **Enable Clusterwide CallPark Number/Ranges** parameter on the Unified CM is set to **False**.
   - Reversion Pattern (Directed Call Park only) - If a call is parked for longer than the allowed time, it reverts to the number selected from the drop-down list. Note that the allowed time is specified in the **Call Park Reversion Timer** parameter on the Unified CM.

     Note: The **Enable Clusterwide CallPark Number/Ranges** and **Call Park Reversion Timer** parameters are located on the Unified CM under **System > Service Parameters - Service Parameter Configuration (Advanced) - Cisco CallManager (Active) Service > Clusterwide Parameters (Feature - General)** section.

   - Revert CSS Name (Directed Call Park only) - This is the CSS that will be used to attempt to route the call to the reversion pattern above.
   - Retrieval Prefix* (Directed Call Park only) - for example, a '*' may be used to retrieve a number from the call park number.
5. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP Trunks and Scripts

SIP profiles

provider

Tip: *Use the Action search to navigate Automate*

Add or manage SIP profiles

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (CUCM, or CallManager) is configured.
3. Go to **SIP Profiles**.
4. **Choose an option**:
   - **Add a new SIP profile**? Click the Plus icon (+) to add a new record, then go to Step 5.
   - **Edit an existing SIP profile**? Choose the SIP profile to be updated by clicking it in the list of SIP profiles. Go to Step 6.
5. If the **Network Device List** dialog displays, select the NDL for the SIP profile from the drop-down menu.

   This dialog displays when you're on a non-site hierarchy node. If you're at a site hierarchy node, the NDL associated with the site is automatically used.

   Note: The **Network Device List** drop-down menu displays only when adding a SIP profile. It does not display when editing a SIP profile.

6. Fill out a unique name for the new SIP profile, or modify the existing name, if required.
7. Configure at least the mandatory settings on the following tabs/panels of this page:
   - *SIP Profile Information settings*.
   - *SDP Information settings*.
   - *Parameters used in Phone settings*.
   - *Normalization Script settings*.
   - *Incoming Requests FROM URI Strings settings*.
   - *Trunk Specific Configuration settings*.
   - *Trunk SIP OPTIONS Ping settings*.
   - *Trunk SDP Information settings*.
8. Click **Save** to save a new SIP profile or to update an existing SIP profile.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP Profile Information settings

Option	Description
Name (Mandatory)	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description (Optional)	This field identifies the purpose of the SIP profile; for example, SIP for 8865. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Default MTP Telephony Event Payload Type (Optional)	This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. Usually, the default value specifies the appropriate payload type. Be sure that you have a good understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. Default-101 Range-96 to 127 This parameter’s value affects calls with the following conditions: • An outgoing SIP call from Cisco Unified Communications Manager • For the calling SIP trunk, the **Media Termination Point Required** check box is checked on the SIP Trunk Configuration window
Early Offer for G.Clear Calls (Optional)	This feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options: • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
User-Agent and Server header information (Mandatory)	This feature indicates how Unified CM handles the User-Agent and Server header information in a SIP message. Choose one of the following options: • **Send Unified CM Version Information as User-Agent Header** - For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified CM passes any contact headers through untouched. • **Pass Through Received Information as Contact Header Parameters** - If selected, the User-Agent and Server header information is passed as Contact header parameters. The User-Agent and Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent and Server headers. • **Pass Through Received Information as User-Agent and Server Header** - If selected, the User-Agent and Server header information is passed as User-Agent and Server headers. The User-Agent and Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent and Server headers. Default: Send Unified CM Version Information as User-Agent Header
Version in User Agent and Server Header (Mandatory)	This field specifies the portion of the installed build version that is used as the value of the User Agent and Server Header in SIP requests. Possible values are: • **Major and Minor**; for example, Cisco-CUCM10.6 • **Major:** for example, Cisco-CUCM10 • **Major, Minor and Revision**; for example, Cisco-CUCM10.6.2 • **Full Build**; for example, Cisco-CUCM10.6.2.98000-19 • **None**; header is omitted Default: Major and Minor
Dial String Interpretation (Mandatory)	Possible values are: • Phone number consists of characters 0-9, *, #, and + (others treated as URI addresses). This is the default value. • Phone number consists of characters 0-9, A-D, *, #, and + (others treated as URI addresses) • Always treat all dial strings as URI addresses
Redirect by Application (Optional)	If you select this check box and configure this SIP Profile on the SIP trunk, the Unified CM administrator can: • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the calls get routed correctly. • Prevent a DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at stack level causes the call to be routed, not blocked. This behavior occurs if you leave the **Redirect by Application** check box clear.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Disable Early Media on 180 (Optional)	By default, Unified CM signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in these responses, instead of playing ringback locally, Unified CM connects media. The calling phone then plays whatever the called device is sending (such as ringback or busy signal). If you receive no ringback, the device you are connecting to may include SDP in the 180 response, but not send media before 200OK response. In this case, select this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response. Note: Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.
Outgoing T.38 INVITE include audio mline (Optional)	The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, configure a SIP trunk with this SIP profile. Note: The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.
Use Fully Qualified Domain Name in SIP Requests (Optional)	This feature enables Unified CM to relay a caller's alphanumeric hostname by passing it to the called device or outbound trunk as SIP header information. Enter one of the following: **f** - To disable this option. The IP address for Unified CM is passed to the line device or outbound trunk instead of the user's hostname. **t** - To enable this option. Unified CM relays an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call originates from a line device on the Unified CM cluster, and is routed on a SIP trunk, then the configured Organizational Top-Level Domain (for example, Cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call originates from a trunk on Unified CM and is being routed on a SIP trunk, then: • If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging preserves the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. • If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. Default: f - Disabled
Assured Services SIP conformance (Optional)	Select this check box for third-party AS-SIP endpoints and AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SDP Information settings

Option	Description
SDP Transparency Profile (Optional)	Displays the SDP Transparency Profile Setting (read-only)
Accept Audio Codec Preferences in Received Offer (Optional)	Choose one of the following options: • **On** - Enables Unified CM to honor the preference of audio codecs in the received offer and preserve it while processing. • **Off** - Enables Unified CM to ignore the preference of audio codecs in a received offer and apply the locally configured Audio Codec Preference List. The default selects the service parameter configuration. • **Default** - Selects the service parameter configuration. Default: Default
Require SDP Inactive Exchange for Mid-Call Media Change (Optional)	This feature determines how Unified CM handles midcall updates to codecs or connection information such as IP address or port numbers. If you select this check box, during midcall codec or connection updates Unified CM sends an INVITE a-inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. Note For early offer enabled SIP trunks, the Send send-receive SDP in midcall INVITE parameter overrides this parameter. If this check box is clear, Unified CM passes the midcall SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. Default: Clear
Allow RR/RS bandwidth modifier (RFC 3556) (Mandatory)	Specifies the RR (RTDP bandwidth allocated to other participants in an RTP session) and RS (RTCP bandwidth allocated to active data senders) in RFC 3556. Options are: • Transport Independent Application Specific bandwidth modifier (TIAS) and AS • TIAS only • AS only • CT only Default: TIAS and AS

Copyright © 2025 VisionOSS Limited. All rights reserved.

Parameters used in Phone settings

Option	Description
Timer Invite Expires (seconds) (Optional)	This field specifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values: Any positive number Default: 180 seconds
Timer Register Delta (seconds) (Optional)	This field is intended to be used by SIP endpoints only. The endpoint receives this value through a TFTP config file. The endpoint reregisters Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the `SIP Station KeepAlive Interval` service parameter. Valid values: 0 to 32767 Default: 5 seconds
Timer Register Expires (seconds) (Optional)	This field is intended to be used by SIP endpoints only. The SIP endpoint receives the value through a TFTP config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. Valid values: Any positive number Default: 3600 seconds (1 hour) If the endpoint sends a shorter Expires value than the `SIP Station Keepalive Interval` service parameter, Unified CM responds with a 423 “Interval Too Brief.” If the endpoint sends a greater Expires value than the `SIP Station Keepalive Interval` service parameter, Unified CM responds with a 200 OK with the Keepalive Interval value for Expires. Note: For mobile phones running SIP, Unified CM uses this value instead of the `SIP Station KeepAlive Interval` service parameter to determine the registration period. Note: For TCP connections, the value for the `Timer Register Expires` field must be lower than the value for the `SIP TCP Unused Connection` service parameter.
Timer T1 (msec) (Optional)	This field specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values: Any positive number Default: 500 msec
Timer T2 (msec) (Optional)	This field specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values: Any positive number Default: 4000 msec
Retry INVITE (Optional)	This field specifies the maximum number of times that an INVITE request gets retransmitted. Valid values: Any positive number Default: 6

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Retry Non-INVITE (Optional)	This field specifies the maximum number of times that a SIP message other than an INVITE request gets retransmitted. Valid values: Any positive number Default: 10
Start Media Port (Optional)	This field designates the start real-time protocol (RTP) port for media. Range: 2048 to 65535 Default: 16384
Stop Media Port (Optional)	This field designates the stop real-time protocol (RTP) port for media. Range: 2048 to 65535 Default: 32766
Call Pickup URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call pickup feature.
Call Pickup Group URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call pickup group feature.
Meet Me Service URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the meet me conference feature.
User Info (Optional)	This field configures the user- parameter in the REGISTER message. Valid values are: • **None** - No value is inserted • **Phone** - The value user-phone is inserted in the To, From, and Contact Header for REGISTER • **IP** - The value user-ip is inserted in the To, From, and Contact Header for REGISTER Default: None
DTMF DB Level (Optional)	This field specifies the in-band DTMF digit tone level. Valid values are: • 6 dB below nominal • 3 dB below nominal • Nominal • 3 dB above nominal • 6 dB above nominal Default: Nominal
Call Hold Ring Back (Optional)	This parameter causes the phone to ring in cases where you have another party on hold when you hang up a call. Valid values are: • **Off** - Off permanently and cannot be turned on and off locally by the user interface • **On** - On permanently and cannot be turned on and off locally by the user interface
Anonymous Call Block (Optional)	The field configures anonymous call block. Valid values are: • **Off** - Disabled permanently and cannot be turned on and off locally by the user interface • **On** - Enabled permanently and cannot be turned on and off locally by the user interface

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Caller ID Blocking (Optional)	This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or email address from phones that have caller identification enabled. Valid values are: • **Off** - Disabled permanently and cannot be turned on and off locally by the user interface • **On** - Enabled permanently and cannot be turned on and off locally by the user interface
Do Not Disturb Control (Optional)	This field sets the Do Not Disturb (DND) feature. Valid values are: • **User** - The dndControl parameter for the phone specifies 0. • **Admin** - The dndControl parameter for the phone specifies 2.
Telnet Level for 7940 and 7960 (Optional)	Cisco Unified IP Phones 7940 and 7960 do not support SSH for sign-in access or HTTP that is used to collect logs. However, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values: • **Disabled** - No access • **Limited** - Some access but cannot run privileged commands • **Enabled** - Full access
Resource Priority Namespace (Optional)	This field enables the administrator to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line using its SIP Profile.
Timer Keep Alive Expires (seconds) (Optional)	Unified CM requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages sent to the backup Unified CM to ensure its availability for failover. Default: 120 seconds
Timer Subscribe Expires (seconds) (Optional)	This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the`` Expires`` header field. Valid values: Any positive number Default: 120 seconds
Timer Subscribe Delta (seconds) (Optional)	Use this parameter with the `Timer Subscribe Expires` setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by `Timer Subscribe Expires`. Range: 3 to 15 seconds Default: 5 seconds
Maximum Redirections (Optional)	Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call. Default: 70 redirections
Off hook To First Digit Timer (msec) (Optional)	This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. Range: 0 to 15,000 microseconds Default: 15,000 microseconds
Call Forward URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call forward feature.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Speed Dial (Abbreviated Dial) URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) do not download to the phone. The phone uses the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI contains the abbreviated dial digits (for example, 14), and the Call-Info header indicates the abbreviated dial feature. Unified CM translates the abbreviated dial digits into the configured digit string and extends the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.
Conference Join Enabled (Optional)	Select this check box to join the remaining conference participants when a conference initiator using a Cisco Unified IP Phone 7940 or 7960 hangs up. Leave it clear if you do not want to join the remaining conference participants. Note: This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.
RFC 2543 Hold (Optional)	Select this check box to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Unified CM. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer (Optional)	This check box determines whether the Cisco Unified IP Phones 7940 and 7960 caller can transfer an attended transfer's second leg while the call is ringing. Select the check box if you want semi attended transfer enabled; leave it clear if you want semi attended transfer disabled. Note: This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.
Enable VAD (Optional)	Select this check box if you want voice activation detection (VAD) enabled; leave it clear if you want VAD disabled. When VAD is enabled, no media is sent when voice is detected.
Stutter Message Waiting (Optional)	Select this check box if you want stutter dial tone when the phone goes off hook and a message is waiting. Leave clear if you do not want a stutter dial tone when a message is waiting. This setting supports Cisco Unified IP Phones 7960 and 7940 that run SIP.
MLPP User Authorization (Optional)	Select this check box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Normalization Script settings

Option	Description
Normalization Script	From the drop-down list, choose the script that you want to apply to this SIP profile. To import another script from Unified CM, go to the SIP Normalization Configuration window (Device Device Settings SIP Normalization Script), and import a new script.
Enable Trace	Select this check box to enable tracing within the script or clear this check box to disable tracing. When selected, the trace.output API provided to the Lua scripter produces SDI trace. Note: We recommend that you only enable tracing while debugging a script. Tracing impacts performance and is not recommended under normal operating conditions.
Script Parameters	Enter parameter names and parameter values in the **Script Parameters** box as comma-delineated key-value pairs. Valid values include all characters except equals signs (-), semicolons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value. Alternatively, to add another parameter line from Unified CM, click the + (plus) button. To delete a parameter line, click the - (minus) button.

Incoming Requests FROM URI Strings settings

Option	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX - Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 55000 - Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Presentation Info

Option	Description
Is Anonymous	Display configured External Presentation Number and External Presentation as Anonymous on the called party device.
External Presentation Name	Configure presentation number of choice.
External Presentation Number	Configure presentation name of choice.

Trunk Specific Configuration settings

Option	Description
Reroute Incoming Request to new Trunk based on	Unified CM only accepts calls from a SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Unified CM accepts the call, Unified CM uses the configuration for this setting to determine whether to reroute the call to another trunk. From the drop-down list, choose the method that Unified CM uses to identify the SIP trunk where the call gets rerouted: • **Never** - If the SIP trunk matches the IP address of the originating device, choose this option. Unified CM, which identifies the trunk by the incoming packet's source IP address and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • **Contact Info Header** - If the SIP trunk uses a SIP proxy, choose this option. Unified CM parses the IP address or domain name and the signaling port number in the incoming request's header. Unified CM then reroutes the call to the SIP trunk using that IP address and port. If no SIP trunk is identified, the call occurs on the trunk where the call arrived. • **Call-Info Header with purpose-x-cisco-origIP** - If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Unified CM performs the following: – parses the Call-Info header – looks for the parameter `purpose-x-cisco-origIP` – uses the IP address or domain name and signaling port number in the header to reroute the call to the SIP trunk using the IP address and port If the parameter is not in the header, or no SIP trunk is identified, the call occurs on the SIP trunk where the call arrived. Default: Never Note: This setting does not work for SIP trunks connected to: • A Unified CM IM and Presence Service proxy server. • Originating gateways in different Unified CM groups

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
RSVP Over SIP	This field configures RSVP over SIP trunks. From the drop-down list, choose the method that Unified CM uses to configure RSVP over SIP trunks: • **Local RSVP** - In a local configuration, RSVP occurs within each cluster, between the endpoint and the local SIP trunk, but not on the WAN link between the clusters. • **E2E** - In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the endpoints, including within the local cluster and over the WAN.
Resource Priority Namespace List	Select a configured Resource Priority Namespace list from the drop-down menu. The Namespace List is configured in Unified CM in the Resource Priority Namespace List menu. You can access the menu in Unified CM from System MLPP > Namespace.
Fall back to local RSVP	Select this check box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this check box is clear, end-to-end RSVP calls that cannot establish an end-to-end connection fail.
SIP Rel1XX Options	This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint. Valid values are: • **Disabled** - Disables SIP Rel1XX. • **Send PRACK if 1XX contains SDP** - Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • **Send PRACK for all 1XX messages** - Acknowledges all1XX messages with PRACK. If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.
Video Call Traffic Class	Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list, select one of: • **Immersive** - High-definition immersive video. • **Desktop** - Standard desktop video. • **Mixed** - A mix of immersive and desktop video. Unified CM Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth and Immersive Bandwidth. The pool used depends on the type of call determined by the Video Call Traffic Class. Refer to the “Call Admission Control” chapter of the Cisco Unified Communications Manager System Guide for more information.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Line Identification Presentation (Mandatory)	Select one of: • **Strict From URI presentation Only** - To select the network-provided identity • **Strict Identity Headers presentation Only** - To select the user-provided identity • **Default** - To select the system default calling line identification Default: Default
Session Refresh Method (Mandatory)	Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions. This allows the Unified CM and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified CM received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified CM initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified CM can send both Update and Invite requests. Specify whether to use **Invite** or **Update** as the Session Refresh Method. Default: Invite Note: Sending a midcall Invite request requires specifying an offer SDP in the request. This means that the far end must send an answer SDP in the Invite response. Update: Unified CM requests a SIP Update if the SIP session's far end supports the Update method in the Supported or Require headers. When sending the Update request, the Unified CM includes an SDP. This simplifies the session refresh since no SDP offer or answer exchange is required. Note: If the far end of the SIP session does not support the Update method, the Unified CM continues using the Invite method for session refresh.
Early Offer Support for voice and video calls (Mandatory)	This field configures Early Offer support for voice and video calls. When enabled, Early Offer support includes a session description in the initial INVITE for outbound calls. Early Offer configuration settings on SIP profile apply only to SIP trunk calls. These configuration settings do not affect SIP line side calls. If this profile is shared between a trunk and a line, only a SIP trunk that uses the profile is affected by these settings. The Media Transfer Point (MTP) Required check box on the Trunk Configuration window, if enabled, overrides the early offer configuration on the associated SIP profile. Unified CM sends the MTP IP address and port with a single codec in the SDP in the initial INVITE. From the drop-down list box, select one of the following three options: • **Disabled (Default value)** - Disables Early Offer; no SDP will be included in the initial INVITE for outbound calls. • **Best Effort (no MTP Inserted)** – Provide Early Offer for the outbound call only when caller side's media port, IP and codec information is available. – Provide Delayed Offer for the outbound call when caller side's media port, IP and codec information is not available. No MTP is inserted to provide Early Offer in this case. • **Mandatory (insert MTP if needed)** - Provide Early Offer for all outbound calls and insert MTP when caller side's media port, IP and codec information is not available. Default: Disabled (Default value)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Selecting the **Enable ANAT** and **MTP Required** check boxes sets Unified CM to insert a dual-stack MTP and send an offer with two m-lines, for IPv4 and IPv6. If a dual- stack MTP cannot be allocated, Unified CM sends an INVITE without SDP. When you select the **Enable ANAT** check box and the **Media Termination Point Required** check box is clear, Unified CM sends an INVITE without SDP. When the **Enable ANAT** and **MTP Required** check boxes are cleared (or when an MTP cannot be allocated), Unified CM sends an INVITE without SDP. When you clear the **Enable ANAT** check box but you select the **MPT Required** check box, consider the information, which assumes that an MTP can be allocated: • Unified CM sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Unified CM sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Unified CM determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.
Deliver Conference Bridge Identifier	When checked, the SIP trunk passes the b-number identifying the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require this field. Selecting this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Selecting this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.
Allow Passthrough of Configured Line Device Caller Information	Select this check box to allow passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Select this check box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Select this check box to reject anonymous outgoing calls.
Send ILS Learned Destination Route String	When this check box is selected, for calls routed to a learned directory URI, learned number, or learned pattern, Unified CM: • adds the `x-cisco-dest-route-string` header to outgoing SIP INVITE and SUBSCRIBE messages • inserts the destination route string into the header When this check box is clear, Unified CM does not add the x-cisco-dest-route-string header to any SIP messages. The x-cisco-dest-route-string header allows Unified CM to route calls across a Session Border Controller.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Trunk SIP OPTIONS Ping settings

Option	Description
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	Select this check box if you want to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device is unresponsive or returns a SIP error response such as 503 Service Unavailable or 408 Timeout, Unified CM reroutes the calls by using other trunks or a different address. If this check box is clear, the SIP trunk does not track the status of SIP trunk destinations. When this check box is selected, you can configure two request timers.
Ping Interval for In-service and Partially In-service Trunks (seconds)	This field configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service. Default: 60 seconds Range: 5 to 600 seconds
Ping Interval for Out-of-service Trunks (seconds)	This field configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if: • it fails to respond to OPTIONS • it sends 503 or 408 responses • the Transport Control Protocol (TCP) connection cannot be established If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service. Default: 120 seconds Range: 5 to 600 seconds
Ping Retry Timer (msec)	This field specifies the maximum waiting time before retransmitting the OPTIONS request. Range: 100 to 1000 milliseconds Default: 500 milliseconds
Ping Retry Count	This field specifies the number of times that Unified CM resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low. Range: 1 to 10 Default: 6

Copyright © 2025 VisionOSS Limited. All rights reserved.

Trunk SDP Information settings

Option	Description
Send send-receive SDP in midcall INVITE	Select this check box to prevent Unified CM from sending an INVITE a-inactive SDP message during call hold or media break during supplementary services. Note: This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls. When you enable Send send-receive SDP in midcall INVITE for an early offer SIP trunk in tandem mode, Unified CM inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a-inactive or sendonly or recvonly in audio media line. In tandem mode, Unified CM depends on the SIP devices to reestablish media path by sending either a delayed INVITE or midcall INVITE with send-recv SDP. When you enable Send send-receive SDP in midcall INVITE and Require SDP Inactive Exchange for Mid-Call Media Change on the same SIP Profile, the Send send-receive SDP in midcall INVITE overrides the Require SDP Inactive Exchange for Mid-Call Media Change, so Unified CM does not send an INVITE with a-inactive SDP in midcall codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled. Note: To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter in Unified CM (System Service Parameters) to True.
Allow Presentation Sharing using BFCP	If the check box is selected, Unified CM allows supported SIP endpoints to use the Binary Floor Control Protocol (BFCP) to enable presentation sharing. The use of BFCP creates an added media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from someone's laptop, into a SIP videophone. If the check box is clear, Unified CM rejects BFCP offers from devices associated with the SIP profile. The BFCP application line and associated media line ports are set to 0 in the answering SDP message. Default: Clear Note: BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP, or Transcoder. For more information on BFCP, refer to the Cisco Unified Communications Manager System Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Allow iX Application Media	Select this check box to enable support for iX media channel.
Allow multiple codecs in answer SDP	This option applies when incoming SIP signals do not indicate support for multiple codec negotiation and Unified CM can finalize the negotiated codec. When this check box is selected, the endpoint behind the trunk can handle multiple codecs in the answer SDP. For example, an endpoint that supports multiple codec negotiation calls the SIP trunk, and Unified CM sends a Delay Offer request to a trunk. The endpoint behind the trunk returns all support codecs without the Contact header to indicate the support of multiple codec negotiation. In this case, Unified CM identifies that the trunk can handle multiple codec negotiation, and sends SIP response messages to both endpoints with multiple common codecs. When clear, Unified CM identifies that the endpoint behind the trunk cannot handle multiple codec negotiation, unless SIP contact header URI states it can. Unified CM continues the call with single codec negotiation.

SIP trunks

Tip: *Use the Action search to navigate Automate*

Overview

This section describes how to add, edit, and delete SIP trunks, and how to reset or restart SIP trunks.

Add and edit SIP trunks

This procedure adds new SIP trunks and edits existing SIP trunks.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (UCM) is configured.
3. Go to **SIP Trunks**.
4. **Choose an option**:
   - **Add a new SIP trunk**? Click the Plus icon (+) to add a new record, then go to Step 5.
   - **Edit an existing SIP trunk**? Click on the relevant SIP trunk in the list of SIP trunks; then, go to step 6.
5. From the **CUCM** drop-down, select the hostname, domain name, or IP address of the CUCM where you're adding the SIP trunk.

   Note: The **CUCM** drop-down displays only when you're adding a new SIP trunk (not when editing). This drop-down menu displays the CUCM located at the node, and all the CUCM nodes in the hierarchies

Copyright © 2025 VisionOSS Limited. All rights reserved.

above the node where you're adding the SIP trunk.

To provision a CUCM server, see the Installation Tasks section of Installing Cisco Unified Communications Manager.

6. At **Device Name**, fill out a unique name for the new SIP trunk (or modify the existing device name, as applicable).
7. Complete at least the minimum, mandatory fields on the following tabs/panels:
   - *Device Information tab*
   - *Call Routing General tab*
   - *Call Routing Inbound tab*
   - *Call Routing Outbound tab*
   - *SP Info tab*
   - *GeoLocation tab*
8. Save your changes for the new or modified SIP trunk.

   The SIP trunk appears in the SIP trunk list. The SIP trunk is automatically reset on the CUCM once it's added. To reset the SIP trunk at any other time, see "Reset SIP Trunk".

   To view the SIP trunk and its properties, log in to the CUCM where you added the SIP trunk, select Device Trunk, and perform the "Find" operation. Clicking on the SIP trunk name in the list displays its characteristics.

Delete a SIP trunk

To delete a SIP trunk:

1. Log in as provider, reseller or customer administrator.
2. Choose an option, depending on your login profile:
   - Logged in as Provider or Reseller admin? Go to (CUCM) **SIP Trunks**.
   - Logged in as Customer admin? Go to (Advanced) **SIP Trunks**.
3. From the list of trunks, choose the SIP trunk to be deleted.
4. Click **Delete** to delete the SIP trunk.
5. Click **Yes** to confirm the deletion.

Reset a SIP trunk

This procedure shuts down a SIP trunk and brings it back into service.

Note: This procedure does not physically reset the hardware; it only re-initializes the configuration that is loaded by the UCM cluster. To restart a SIP trunk without shutting it down, use **Restart SIP Trunks**.

Perform these steps:

1. Log in as provider, reseller or customer administrator.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Choose an option, depending on your login profile:
   - Logged in as Provider or Reseller admin? Go to (CUCM) **SIP Trunks**.
   - Logged in as Customer admin? Go to (Advanced) **SIP Trunks**.
3. From the list of SIP trunks, click the SIP trunk to be reset, then choose **Action > Reset**.

Restart SIP trunks

This procedure restarts a SIP trunk without shutting it down first.

Note:

- To shut down a SIP trunk prior to the reset, see *Reset a SIP trunk*.
- If the SIP trunk is not registered with Cisco UCM, you cannot restart it.

Warning: Restarting a SIP trunk drops all active calls that are using the trunk.

Perform these steps:

1. Log in as provider, reseller or customer administrator.
2. Choose an option, depending on your login profile:
   - Logged in as Provider or Reseller admin: Go to (CUCM) **SIP Trunks**.
   - Logged in as Customer admin? Go to (Advanced) **SIP Trunks**.
3. From the list of trunks, click the SIP trunk to be restarted, then click **Action > Restart**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIP Trunks Configuration Settings

Device Information tab

Option	Description
Device Name *	Enter a unique identifier for the trunk using up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only. Default value: None
Trunk Service Type	Choose one of: • **None** - Choose this option if the trunk is not used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine • **Call Control Discovery** - Choose this option to enable the trunk to support call control discovery. • **Extension Mobility Cross Cluster** - Choose this option to enable the trunk to support the Extension Mobility Cross Cluster (EMCC) feature. Choosing this option causes the following settings to remain blank or clear and become unavailable for configuration, thus retaining their default values: Media Termination Point Required, Unattended Port, Destination Address, Destination Address IPv6, and Destination Address is an SRV. • **Cisco Intercompany Media Engine** - Ensure that the Cisco IME server is installed and available before you configure this field. • **IP Multimedia Subsystem Service Control (ISC)** - Choose this option to enable the trunk to support IP multimedia subsystem service control. Default value: None (Default)
Description (Optional)	Enter a descriptive name for the trunk using up to 114 characters in any language, but not including double-quotes ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>). Default value: empty
Device Pool *	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers (Unified CMs) that the trunk uses to distribute the call load dynamically. Note: Calls that are initiated from a phone that is registered to a Unified CM that does not belong to the device pool of the trunk use different Unified CMs of this device pool for different outgoing calls. Selection of Unified CM nodes occurs in a random order. A call that is initiated from a phone that is registered to a Unified CM that does belong to the device pool of the trunk uses the same Unified CM node for outgoing calls if the Unified CM is up and running. Default value: Default
Common Device Configuration	Choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Default value: None
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Unified CM clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Default value: Use System Default

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. Default value: None
Location *	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. Choose the appropriate location for this trunk: • Hub_None - Specifies that the locations feature does not keep track of the bandwidth that this trunk consumes. • Phantom - Specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. • Shadow - Specifies a location for intercluster enhanced location CAC. Valid for SIP intercluster trunks (ICT) only. Default value: Hub_None
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls is attempted. Default value: None
Tunneled Protocol	Choose the QSIG option if you want to use SIP trunks or SIP gateways to transport (tunnel) QSI messages from Unified CM to other PINXs. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Path Replacement, and Message Waiting Indication (MWI). Note: Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway. Default value: None
QSIG Variant	To display the options in the **QSIG Variant** drop-down list, choose QSIG from the **Tunneled Protocol** drop-down menu. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down menu, select one of: • No Changes - Default. Keep this parameter set to the default value unless a VOSS support engineer instructs otherwise. • Not Selected • ECMA - Select for ECMA PBX systems that use Protocol Profile 0x91 • ISO - Select for PBX systems that use Protocol Profile 0x9F Default value: No Changes

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down menu, choose QSIG from the **Tunneled Protocol** drop-down menu. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down menu, select one of • No Changes - Keep this parameter set to the default value unless a VOSS support engineer instructs otherwise. • Not Selected • Use Global Value ECMA - If you selected the ECMA option from the QSIG Variant drop-down menu, select this option. • Use Global Value ISO - If you selected the ISO option from the QSIG Variant drop-down menu, select this option. • Use Local Value Default value: No Changes
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. From the drop-down menu, select one of: • None - This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode - Unified CM writes the decrypted or non-encrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. Default value: None
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. Default value: 0 (zero), Range is from 0 to 300 minutes

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Media Termination Point Required	You can configure Unified CM SIP trunks to always use an Media Termination Point (MTP). Select this box to provide media channel information in the outgoing INVITE request. When this check box is selected, all media channels must terminate and re-originate on the MTP device. If you clear the check box, the Unified CM can decide whether calls are to go through the MTP device or be connected directly between the endpoints. Note: If the check box remains clear, Unified CM attempts to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible. For example, existing phones that run SCCP support only out-of-band DTMF, and existing phones that run SIP support RFC2833. Because the DTMF methods are not identical, the Unified CM dynamically allocates an MTP. If, however, a new phone that runs SCCP, which supports RFC2833 and out-of band, calls an existing phone that runs SIP, Unified CM does not allocate an MTP because both phones support RFC2833. So, by having the same type of DTMF method supported on each phone, there is no need for MTP. Default value: False (Cleared)
Retry Video Call as Audio	This check box pertains to outgoing SIP trunk calls and does not impact incoming calls. By default, the system selects this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you clear this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call using Automatic Alternate Routing (AAR) and route list or hunt list. Default value: True (Selected)
Path Replacement Support	This check box is relevant when you select QSIG from the **Tunneled Protocol** drop-down menu. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement. Default value: False (Clear)
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you select this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool. If the user locale setting matches the terminating phone user locale, the phone displays the characters. Note: The phone may display malformed characters if the two ends of the trunk are configured with user locales that do not belong to the same language group. Default value: False (Cleared)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Transmit UTF-8 Names for QSIG APDU	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you select this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format. If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8 bit format) and encodes in ISO8859-1 format. Default value: False (Cleared)
Unattended Port	Select this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. Default value: False (Cleared)
SRTP Allowed	Select this check box if you want Unified CM to allow secure and nonsecure media calls over the trunk. Selecting this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not select this check box, Unified CM prevents SRTP negotiation with the trunk and uses RTP negotiation instead. Caution: If you select this check box, we strongly recommend that you use an encrypted TLS profile, so that keys and other security related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP still works but the keys get exposed in signaling and traces. In that case, you must ensure the security of the network between Unified CM and the destination side of the trunk. Default value: False (Cleared)
Consider Traffic on This Trunk Secure	This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. From the drop-down menu, select one of: • When using both sRTP and TLS • When using sRTP Only - Displays when you select the **SRTP Allowed** check box. Default value: When using both sRTP and TLS

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Route Class Signaling Enabled	From the drop-down menu, enable or disable route class signaling for the port. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the Hotline feature. From the drop-down menu, select one of: • Default - The device uses the setting from the Route Class Signaling service parameter • Off - Enables route class signaling. This setting overrides the Route Class Signaling service parameter • On - Disables route class signaling. This setting overrides the Route Class Signaling service parameter. Default value: Default
Use Trusted Relay Point	From the drop-down menu, enable or disable whether Unified CM inserts a trusted relay point (TRP) device with this media endpoint. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. If both TRP and RSVPAgent are needed for the endpoint, Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Unified CM first tries to find a transcoder that is also designated as a TRP. Select one of: • Default - The device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates • Off - Disables the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On - Enables the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. Default value: Default
PSTN Access	If you use the Cisco Intercompany Media Engine feature, select this check box to indicate that calls made through this trunk might reach the PSTN. Select this check box even if all calls through this trunk device do not reach the PSTN. For example, select this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When selected, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. Default value: True (Selected)
Run On All Active Unified CM Nodes	Select this check box to enable the trunk to run on every node. Default value: False (Cleared)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call Routing General tab

Option	Description
Remote-Party-ID	Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Unified CM to the remote destination. If you select this box, the SIP trunk always sends the RPID header. If you do not select this check box, the SIP trunk does not send the RPID header. Note: Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled. Outgoing SIP Trunk Calls The configured values of the Calling Line ID Presentation and Calling Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. If either option is set to Default, the corresponding information (Calling Line ID Presentation and/or Calling Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Unified CM. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Incoming SIP Trunk Calls The configured values of the Connected Line ID Presentation and Connected Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. Be aware that the Connected Line ID Presentation and Connected Name Presentation options are relevant for 180/200 messages that the SIP trunk sends in response to INVITE messages that Unified CM receives. If either option is set to Default, the corresponding information (Connected Line ID Presentation and/or Connected Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Unified CM. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Asserted-Identity	Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you select this check box, the SIP trunk always sends the Asserted-Type header; whether or not the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. Outgoing SIP Trunk Calls - P Headers The decision of which Asserted Identity (either P-Asserted Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Unified CM Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Unified CM Call Control dictates the type of Asserted-Identity. Outgoing SIP Trunk Calls - SIP Privacy Header The SIP Privacy header gets used only when you select the **Asserted-Identity** check box and when the SIP trunk sends either a Privacy-Asserted Identity (PAI) or Privacy Preferred Identity (PPI) header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages). The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Unified CM Call Control. If the SIP Privacy option is set to Default, the Calling Line ID Presentation and Calling Name Presentation that the SIP trunk receives from Unified CM Call Control determines the SIP Privacy header. Incoming SIP Trunk Calls - P Headers The decision of which Asserted Identity (either P-Asserted Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Unified CM Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Unified CM Call Control dictates the type of Asserted-Identity. Incoming SIP Trunk Calls - SIP Privacy Header The SIP Privacy header gets used only when you select the **Asserted Identity** check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither
	gets sent nor processed in incoming SIP messages.) The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Unified CM Call Control. If the SIP Privacy option is set to Default, the Connected Line ID Presentation and Connected Name Presentation that the SIP trunk receives from Unified CM Call Control determine the SIP Privacy header. Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Asserted-Type	From the drop-down menu, select one of the following values to specify the type of Asserted Identity header that SIP trunk messages should include: • Default - Screening information that the SIP trunk receives from Unified CM Call Control determines the type of header that the SIP trunk sends. • PAI - The Privacy-Asserted Identity header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Unified CM. • PPI - The Privacy Preferred Identity header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Unified CM. Note: These headers get sent only if the **Asserted- Identity** check box is selected. Default value: Default
SIP Privacy	From the drop-down menu, select one of the following values to specify the type of SIP privacy header for SIP trunk messages to include: • Default - This option represents the default value; Name/Number Presentation values that the SIP trunk receives from the Unified CM Call Control compose the SIP Privacy header. For example, if Name/Number presentation specifies Restricted, the SIP trunk sends the SIP Privacy header; however, if Name/Number presentation specifies Allowed, the SIP trunk does not send the Privacy header. • None - The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Unified CM. • ID - The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Unified CM. • ID Critical - The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label critical implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Unified CM. Note: These headers get sent only if the **Asserted Identity** check box is selected. Default value: Default

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call Routing Inbound tab

Option	Description
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32, or choose 99 to indicate all digits. Note: Unified CM counts significant digits from the right (last digit) of the number that is called. Default value: 99
Connected Line ID Presentation	Unified CM uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send connected line information. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. • Restricted - Choose Restricted if you do not want Unified CM to send connected line information. Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default
Connected Name Presentation	Unified CM uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send connected name information. • Restricted - Choose Restricted if you do not want Unified CM to send connected name information. Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default
Calling Search Space	From the drop-down menu, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down menu by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Find and List Calling Search Spaces window. Find and choose a calling search space name. Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. Default value: None

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. Default value: None
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Unified CM adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +. Default value: None
Redirecting Diversion Header - Delivery Inbound	Select this check box to accept the Redirecting Number in the incoming INVITE message to the Unified CM. Clear the check box to exclude the Redirecting Number in the incoming INVITE message to the Unified CM. You use Redirecting Number for voice messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should select the check box. Default value: False (Cleared)
Incoming Calling Party - Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape field, you cannot configure the Strip Digits field. In this case, Unified CM takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. Default value: None
Incoming Calling Party - Strip Digits	Enter the number of digits, up to the number 24, that you want Unified CM to strip from the calling party number of Unknown type before it applies the prefixes. Default value: None
Incoming Calling Party - Calling Search Space	This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing. Default value: None

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Incoming Calling Party - Use Device Pool CSS	Select this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. Default value: True (Selected)
Incoming Called Party - Prefix	Unified CM applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. Tip: If the word Default displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Unified CM takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word Default displays in the Prefix field in the Device Pool Configuration window, Unified CM does not apply any prefix or strip digit functionality. Default value: None
Incoming Called Party - Strip Digits	Enter the number of digits that you want Unified CM to strip from the called party number of Unknown type before it applies the prefixes. Tip: To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. Default value: None
Incoming Called Party - Calling Search Space	This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device. Default value: None
Incoming Called Party - Use Device Pool CSS	Select this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. Default value: True (Selected)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Connected Party Transformation CSS	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Unified CM includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update and reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. Note: If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing. Default value: None
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window. Default value: True (Selected)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call Routing Outbound tab

Option	Description
Called Party Transformation CSS	This setting allows you to send the transformed called party number in an INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. Note: If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing. Default value: None
Use Device Pool Called Party Transformation CSS	To use the Called Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Called Party Transformation CSS that you configured for this device in the Trunk Configuration window. Default value: True (Selected)
Calling Party Transformation CSS	This setting allows you to send the transformed calling party number in an INVITE message for outgoing calls made over a SIP Trunk. Also when redirection occurs for outbound calls, this CSS is used to transform the connected number that is sent from Unified CM side in outgoing reINVITE / UPDATE messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Tip: If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing. Default value: None
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window. Default value: True (Selected)
Calling Party Selection	Choose the directory number that is sent on an outbound call. Select one of the following options to specify which directory number is sent: • Originator - Send the directory number of the calling device • First Redirect Number - Send the directory number of the redirecting device. • Last Redirect Number - Send the directory number of the last device to redirect the call. • First Redirect Number (External) - Send the external directory number of the redirecting device • Last Redirect Number (External) - Send the external directory number of the last device to redirect the call. Default value: Originator

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Line ID Presentation	Unified CM uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send calling number information. • Restricted - Choose Restricted if you do not want Unified CM to send the calling number information. Default value: Default
Calling Name Presentation	Unified CM used calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send calling name information. • Restricted - Choose Restricted if you do not want Unified CM to send the calling name information. Note: This service is not available when QSIG tunneling is enabled. Default value: Default
Calling and Connected Party Info Format *	This option allows you to configure whether Unified CM inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages. From the drop-down menu, select one of: • Deliver DN only in connected party - In outgoing SIP messages, Unified CM inserts the calling party - s directory number in the SIP contact header information. • Deliver URI only in connected party, if available - In outgoing SIP messages, Unified CM inserts the sending party - s directory URI in the SIP contact header. If a directory URI is not available, Unified CM inserts the directory number instead. • Deliver URI and DN in connected party, if available - In outgoing SIP messages, Unified CM inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Unified CM includes the directory number only. Note: You should set this field to Deliver URI only in connected party or Deliver URI and DN in connected party only if you are setting up URI dialing between Unified CM systems of Release 9.0 or greater, or between a Cisco Unified Communications Manager system of Release 9. 0 or greater and a third party solution that supports URI dialing. Otherwise, you must set this field to Deliver DN only in connected party. Default value: Deliver DN only in connected party

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Redirecting Diversion Header Delivery - Outbound	Select this check box to include the Redirecting Number in the outgoing INVITE message from the Unified CM to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Clear the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. Use Redirecting Number for voice-messaging integration only. If your configured voice messaging system supports Redirecting Number, select the check box. Default value: False (Cleared)
Use Device Pool Redirecting Party Transformation CSS	Select this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to this device. If you do not select this check box, the device uses the Redirecting Party Transformation CSS that you configured for this device (see field below).
Redirecting Party Transformation CSS	Allows you to localize the redirecting party number on the device. Make sure that the Redirecting Party Transformation CSS that you enter contains the redirecting party transformation pattern that you want to assign to this device.
Caller Information Caller ID DN	Enter the pattern, from 0 to 24 digits that you want to use to format the Called ID on outbound calls from the trunk. For example, in North America: • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +. Default value: None
Caller Information - Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device. Default value: None
Caller Information - Maintain Original Caller ID DN and Caller Name in Identity Headers	This check box is used to specify whether you will use the caller ID and caller name in the URI outgoing request. If you select this check box, the caller ID and caller name is used in the URI outgoing request. If you do not select this check box, the caller ID and caller name is not used in the URI outgoing request. Default value: False (Cleared)

Copyright © 2025 VisionOSS Limited. All rights reserved.

SP Info tab

Option	Description
Destination Address is an SRV	This field specifies that the configured Destination Address is an SRV record. Default value: False (Cleared)
Destination - Destination Address IPv4	The Destination Address IPv4 represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is selected. Tip: For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field. Note: SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. Note: For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and select the Destination Address is an SRV Destination Port check box. If the remote end is a Unified CM cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Unified CMs within the cluster. Default value: None
Destination - Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is selected. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Unified CM cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Unified CMs within the cluster. Tip: For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field. Default value: None. If IPv4 field above is completed, this field can be left blank.
Destination - Destination port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0. Note: You can now have the same port number that is specified for multiple trunks. You do not need to enter a value if the destination address is a DNS SRV port. The default 5060 indicates the SIP port. Default value: 5060

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Sort Order *	Indicate the order in which the prioritize multiple destinations. A lower sort order indicates higher priority. This field requires an integer value. Default value: Empty
Destination Address is an SRV	This field specifies that the configured Destination Address is an SRV record. Default value: False (Cleared)
Destination - Destination Address IPv4	The Destination Address IPv4 represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is selected. Tip: For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field. Note: SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. Note: For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and select the Destination Address is an SRV Destination Port check box. If the remote end is a Unified CM cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Unified CMs within the cluster. Default value: None
Destination - Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is selected. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Unified CM cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Unified CMs within the cluster. Tip: For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field. Default value: None. If IPv4 field above is completed, this field can be left blank.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Destination - Destination port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0. Note: You can now have the same port number that is specified for multiple trunks. You do not need to enter a value if the destination address is a DNS SRV port. The default 5060 indicates the SIP port. Default value: 5060
Sort Order *	Indicate the order in which the prioritize multiple destinations. A lower sort order indicates higher priority. This field requires an integer value. Default value: Empty
MTP Preferred Originating Codec	Indicate the preferred outgoing codec by selecting one of: • 711ulaw • 711alaw • G729/G729a • G729b/G729ab Note: To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. This field is used only when the **Media Termination Point Required** check box is selected on the **Device Information** tab. Default value: 711ulaw
BLF Presence Group *	Configure this field with the Presence feature. From the drop-down menu, select a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor. • Standard Presence group is configured with installation. Presence groups that are configured in Unified CM Administration also appear in the drop-down menu. • Presence authorization works with presence groups to allow or block presence requests between groups. Tip: You can apply a presence group to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk. Default value: Standard Presence Group

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
SIP Trunk Security Profile *	Select the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks that are configured in Unified CM Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. Default value: Non Secure SIP Trunk Profile
Rerouting Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. Default value: None
Out-Of-Dialog Refer Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The out-of-dialog calling search space gets used when a Unified CM refers a call (B) that is coming into SIP user (A) to a third party (C) when no involvement of SIP user (A) exists. In this case, the system uses the out-of dialog calling search space of SIP user (A). Default value: None
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified CM routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk. From the drop-down menu, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Unified CM Administration display in the SUBSCRIBE Calling Search Space drop-down menu. If you do not select a different calling search space for the SIP trunk from the drop-down menu, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, configure a calling search space as you do all calling search spaces. Default value: None
SIP Profile *	From the drop-down list box, select the SIP profile that is to be used for this SIP trunk. Default value: Standard SIP Profile

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
DTMF Signaling Method	Select one of: • No Preference - Unified CM picks the DTMF method to negotiate DTMF, so the call does not require an MTP. If Cisco Unified Communications Manager has no choice but to allocate an MTP (if the **Media Termination Point Required** check box is selected on the **Device Information** tab), SIP trunk negotiates DTMF to RFC2833. • RFC 2833 - Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Unified CM makes every effort to negotiate RFC2833, regardless of MTP usage. Out of band (OOB) provides the fallback method if the peer endpoint supports it. • OOB and RFC 2833 - Choose this configuration if both out of band and RFC2833 should be used for DTMF. Note: If the peer endpoint supports both out of band and RFC2833, Unified CM negotiates both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events are sent for the same DTMF keypress (one out of band and the other, RFC2833). Default value: No Preference
Normalization Script	From the drop-down menu, choose the script that you want to apply to this trunk. To import another script, on Unified CM go to the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script), and import a new script file. Default value: None
Normalization Script - Enable Trace	Select this check box to enable tracing within the script or clear the check box to disable tracing. When selected, the trace.output API provided to the Lua scripter produces SDI trace. Note: We recommend that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions. Default value: False (Cleared)
Script Parameters	Enter parameter names and values in the format Param1Name=Param1Value; Param2Name=Param2Value where Param1Name is the name of the first script parameter and Param1Value is the value of the first script parameter. Multiple parameters can be specified by putting semicolon after each name and value pair . Valid values include all characters except equal signs (=), semi-colons (;); and non-printable characters, such as tabs. You can enter a parameter name with no value.
Recording Information	Enter one of • 0 - None (default) • 1 - This trunk connects to a recording-enabled gateway • 2 - This trunk connects to other clusters with recording-enabled gateways

Copyright © 2025 VisionOSS Limited. All rights reserved.

GeoLocation tab

Option	Description
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. On Unified CM, you can also choose a geolocation that has been configured with the System > Geolocation Configuration menu option. Default value: None
Geolocation Filter	From the drop-down menu, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. On Unified CM, you can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option. Default value: None
Send Geolocation Information	Select this check box to send geolocation information for this device. Default value: False (Cleared)

SIP trunk security profiles

provider

Tip: *Use the Action search to navigate Automate*

Add or edit SIP trunk security profiles

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (CUCM, or CallManager) is configured.
3. Go to **SIP Trunk Security Profiles**.
4. **Choose an option**:
   - **Add a new SIP trunk security profile**? Click the Plus icon (+) to add a new record, then go to Step 5.
   - **Edit an existing SIP trunk security profile**? Click the SIP trunk security profile to be updated. Go to Step 6.
5. If the **Network Device List** dialog displays, select the NDL for the SIP trunk security profile from the drop-down. The dialog displays only when you're on a non-site hierarchy node. If you're at a site hierarchy node, the NDL associated with the site is automatically used.

   Note: The **Network Device List** drop-down displays when a SIP trunk security profile is added. It does not display when you edit a SIP trunk security profile.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Mandatory. Fill out a unique name for the new SIP trunk security profile in the **Name** field, or modify the existing Name if desired.
7. Complete, at minimum, the other mandatory *SIP trunk security profile settings*
8. Click **Save** to save a new SIP trunk security profile or to update an existing SIP trunk security profile.

SIP trunk security profile settings

SIP trunk security profiles are configured on the **SIP Trunk Security Profiles** page.

The table describes the configuration options on this page:

Option	Description
Name (Mandatory)	Enter a name for the security profile. When you save the new profile, the name displays in the **SIP Trunk Security Profile** drop-down list in the Trunk Configuration window. The maximum length for the name is 64 characters.
Description (Optional)	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Security Mode (Optional)	From the drop-down list, choose one of the following options: • **Non Secure** - No security features except image authentication apply. A TCP or UDP connection opens to Cisco Unified Communications Manager. • **Authenticated** - Unified CM provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • **Encrypted** - Unified CM provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling.
Incoming Transport Type (Optional)	Choose one of: • TCP+UDP • UDP • TLS • TCP If you do not specify an incoming transport type, **TCP+UDP** is assigned. When **Device Security Mode** is **Non Secure**, **TCP+UDP** specifies the transport type. When **Device Security Mode** is **Authenticated** or **Encrypted**, **TLS** specifies the transport type. Note: The Transport Layer Security (TLS) protocol secures the connection between Unified CM and the trunk.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Outgoing Transport Type (Optional)	From the drop-down list, choose the outgoing transport mode. Choose one of: • TCP+UDP • UDP • TLS • TCP When **Device Security Mode** is **Non Secure**, choose **TCP** or **UDP**. When **Device Security Mode** is **Authenticated** or **Encrypted**, **TLS** specifies the transport type. Note: **TLS** ensures signaling integrity, device authentication, and signaling encryption for SIP trunks. Tip: Use **UDP** as the outgoing transport type when connecting SIP trunks between Unified CM systems and IOS gateways that do not support TCP connection reuse. See "Understanding Session Initiation Protocol (SIP)" in the "Cisco Unified Communications Manager System Guide" for more information.
Enable Digest Authentication (Optional)	Select this check box to enable digest authentication. If you select this check box, Unified CM challenges all SIP requests from the trunk. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of **Authenticated** or **Encrypted** to use these features. Tip: Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.
Nonce Validity Time (mins) (Optional)	Enter the number of minutes (in seconds) that the nonce value is valid. When the time expires, Unified CM generates a new value. Note: A nonce value (a random number that supports digest authentication) is used to calculate the MD5 hash of the digest authentication password. Default = 600 minutes. If you do not specify a Nonce Validity Time, the default of 600 minutes is assigned.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
X.509 Subject Name (Optional)	This field applies if you configured TLS for the incoming and outgoing transport type. For device authentication, enter the subject name of the X.509 certificate for the SIP trunk device. If you have a Unified CM cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts. This situation results in multiple X.509 subject names for the trunk. If multiple X.509 subject names exist, enter one of the following characters to separate the names: space, comma, semicolon, or a colon. You can enter up to 4096 characters in this field. Tip: The subject name corresponds to the source connection TLS certificate. Ensure that subject names are unique for each subject name and port. You cannot assign the same subject name and incoming port combination to different SIP trunks. Example: SIP TLS trunk1 on port 5061 has X.509 Subject Names my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has X.509 Subject Names my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have X.509 Subject Name my_ccm4 but cannot have X.509 Subject Name my_cm1.
Incoming Port (Optional)	Choose the incoming port. Enter a value that is a unique port number from 0 to 65535. The value that you enter applies to all SIP trunks that use the profile. The default port value for incoming TCP and UDP SIP messages is 5060. The default SIP secured port for incoming TLS messages is 5061. If the incoming port is not specified, the default port of 5060 is used. Tip: All SIP trunks that use TLS can share the same incoming port; all SIP trunks that use TCP + UDP can share the same incoming port. You cannot mix SIP TLS transport trunks with SIP non-TLS transport trunk types on the same port.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Enable application level authorization (Optional)	Application-level authorization applies to applications that are connected through the SIP trunk. If you select this check box, also select the **Enable Digest Authentication** check box and configure digest authentication for the trunk. Unified CM authenticates a SIP application user before checking the allowed application methods. When application level authorization is enabled, trunk-level authorization occurs first, and application-level authorization occurs second. Unified CM checks the methods authorized for the trunk (in this security profile) before the methods authorized for the SIP application user in the **Application User Configuration** window. Tip: Consider using application-level authorization if you do not trust the identity of the application or if the application is not trusted on a particular trunk. Application requests may come from a different trunk than you expect. For more information about configuring application level authorization at the **Application User Configuration** window, see the “Cisco Unified Communications Manager Administration Guide”.
Accept presence subscription (Optional)	If you want Unified CM to accept presence subscription requests that come through the SIP trunk, select this check box. If you selected **Enable Application Level Authorization**, go to the **Application User Configuration** window and select **Accept Presence Subscription** for any application users authorized for this feature. When application-level authorization is enabled, if you select **Accept Presence Subscription** for the application user but not for the trunk, a 403 error message is sent to the SIP user agent connected to the trunk.
Accept out-of-dialog refer (Optional)	If you want Unified CM to accept incoming non-INVITE, Out-of-Dialog REFER requests that come through the SIP trunk, select this check box. If you selected **Enable Application Level Authorization**, go to the **Application User Configuration** window and select **Accept out-of-dialog refer** for any application users authorized for this method. Note: If this profile is associated with an EMCC SIP trunk, Accept Out-of-Dialog REFER is enabled regardless of the setting on this page.
Accept unsolicited notification (Optional)	If you want Unified CM to accept incoming non-INVITE, unsolicited notification messages that come through the SIP trunk, select this check box. If you selected **Enable Application Level Authorization**, go to the **Application User Configuration** window and select **Accept Unsolicited Notification** for any application users authorized for this method.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Accept replaces header (Optional)	If you want Unified CM to accept new SIP dialogs, which have replaced existing SIP dialogs, select this check box. If you selected **Enable Application Level Authorization**, go to the **Application User Configuration** window and select **Accept Header Replacement** for any application users authorized for this method.
Transmit security status (Optional)	If you want Unified CM to send the security icon status of a call from the associated SIP trunk to the SIP peer, select this check box. Default = Cleared.
Allow charging header (Optional)	If you want to allow RFC 3455 SIP charging headers in transactions (for example, where billing information is passed in the headers for prepaid accounts), select this check box. If the check box is clear, RFC 3455 SIP charging headers are not allowed in sessions that use the SIP profile. Default = **Cleared**.
SIP V.150 Outbound SDP Offer Filtering (Mandatory)	Choose one of the following filter options from the drop-down list: • **Use Default Filter** - The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System Service Parameters Clusterwide Parameters (Device-SIP) in Unified CM Administration. • **No Filtering** - The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • **Remove MER V.150** - The SIP trunk removes V.150 MER SDP lines in outbound offers. Choose this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified CM. • **Remove Pre-MER V.150** - The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Choose this option to reduce ambiguity when your cluster is in a network of MER-compliant devices that cannot process offers with pre-MER lines. Default = **Use Default Filter** .

EMCC Settings

Introduction to EMCC

Overview

Extension Mobility Cross Cluster (EMCC) extends VOSS Automate's current extension mobility functionality to allow a user to log in to a device from within a connected cluster, anywhere in the world. This allows the user to retain the settings, services, and lines they're familiar with at their home location.

VOSS Automate automates most of the EMCC provisioning to enable this feature to work on all dial plans across multiple Cisco Unified Communications Manager (CUCM) clusters that are managed by the same platform instance. A small number of manual configurations remain, specifically around network security, which is outlined in a separate section. VOSS Automate only automates provisioning of the home cluster in cases where the CUCM clusters are managed by separate platforms, that is, cross-cluster configuration across multiple platforms is not supported.

Copyright © 2025 VisionOSS Limited. All rights reserved.

EMCC Use Case

The table describes a scenario where a user from the HOME cluster goes to the VISITING cluster and logs on to a phone. The two clusters can be in different countries/territories. The cluster is EMCC-enabled. The user is also subscribed to the EMCC service.

HOME Cluster	VISITING Cluster
User Profile	Phone (with Geolocation)
Geolocation Filter	
Roaming Device Pool (with Geolocation)	

In this scenario:

- The user cannot be authenticated in the VISITING cluster, but since the cluster is EMCC enabled, and the phone is subscribed to the EMCC service, the cluster searches for the user in defined EMCC remote clusters.
- Once the user (also subscribed to the EMCC service) is authenticated, the phone is unregistered from the VISITING cluster, and re-registered to the HOME cluster.
- The geolocation of the phone is sent to the HOME cluster, which allows the HOME cluster to associate the relevant roaming device pool to the user's phone using the geolocation filter.
- The phone behaves and dials exactly the same as if the user is logged in at the HOME cluster. Additionally, all the user's settings and preferences are preserved.
- Calls to the HOME cluster emergency numbers as well as the VISITING cluster emergency numbers break out at the VISITING cluster (physical location).

Note:

- Various other elements (such as trunks and EMCC countries) must be configured on both the HOME cluster and the VISITING cluster to ensure that this feature works.
- Refer to the "Cisco Unified Communications Manager Features and Services Guide" for more information about the EMCC feature.

Configuring EMCC using VOSS Automate

Before configuring EMCC using VOSS Automate, ensure that the following parameters have already been configured on each required EMCC cluster (CUCM) located at the relevant Customers:

- EMCC feature configuration, such as Default TFTP Server for EMCC Login Device, EMCC Geolocation Filter

Copyright © 2025 VisionOSS Limited. All rights reserved.

EMCC groups

Tip: *Use the Action search to navigate Automate*

Overview

An Extension Mobility Cross Cluster (EMCC) group is a collection of clusters and countries that essentially forms an 'EMCC Cloud', which determines the specific clusters between which a user can roam.

Note: A cluster can only be included in one group.

EMCC groups typically cater for situations where all the clusters are in different countries, and are managed by the same platform instance. To support multiple clusters in the same country, you need to refine the geo-locations and geo-location filters to uniquely identify the clusters in the default provisioning of country. This is supported by using the home cluster setup for each of the clusters in the group.

The **EMCC Group** page allows a provider administrator to add or remove clusters and countries to or from an EMCC group, or to modify/delete an existing EMCC group.

Add EMCC group

When adding an EMCC group, the cluster the user is on when taking this action is automatically selected/included in the new group.

Prerequisites:

- Create the required route patterns. See *Add EMCC route pattern*.

Perform these steps:

1. Log in as Provider administrator or higher.
2. Go to the **EMCC Group** page.
3. Click the Plus icon (+) to add a new record.
4. Choose the required customer from the **Hierarchy** drop-down list.
5. On the **EMCC Group** page, fill out the mandatory EMCC group name.
6. Choose the required CUCM Clusters and Countries to include in the EMCC group by selecting single or multiple entries in the **Available** areas of the screen, and then clicking **Select** to move them to the **Selected** area of the screen.

   Note: Use the Remove, Move Up and Move Down buttons as required to assist in creating the EMCC group. An EMCC group **must contain** a minimum of two clusters.

7. Ensure that the required CUCM clusters and countries are listed in the **CUCM Clusters** and **Countries** areas of the screen respectively.
8. Click **Save**.

   The EMCC group is added to Automate. Once created, the following elements are provisioned per country and EMCC route pattern:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Route list
- Geolocation filter
- SIP profile
- IP phone services
- SIP trunk
- Geolocation
- Route partition
- CSS
- Device pool
- Route pattern

Modify EMCC group

1. Log in as Provider administrator or higher.
2. Go to **EMCC Group**.
3. Click on the EMCC group that you want to modify.
4. On the **EMCC Group** page, add or remove the CUCM Clusters and Countries within the EMCC Group by selecting single or multiple entries in the **Available** or **Selected** areas of the screen, and then clicking **Select** or **Remove** to include or exclude them from the group as required.

   Note: Use the Move Up and Move Down buttons as required to assist in creating the EMCC Group.

5. Save your changes.

Delete EMCC group

To delete an EMCC Group, click on the Group to delete on the EMCC Group page, then click **Delete**.

EMCC configuration templates

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Extension mobility cross cluster (EMCC) templates allow you to define the common EMCC attributes to add a group of new EMCC.

Related Topics

- *Configuration templates*

Clone and add EMCC template

Prerequisites:

- Before creating the template, ensure the EMCC settings are already configured in Cisco Unified Communications Manager (CUCM) Administration.

Perform these steps:

1. Log in as Provider administrator or higher.
2. Set the hierarchy to the relevant customer or location node.
3. Go to **EMCC Configuration Templates**.
4. Click on the EMCC template from which you want to create a new EMCC template.
5. Click **Action > Clone**. The selected EMCC Template is cloned. See also *Configuration templates* for more information.
6. (Mandatory) Fill out a name for the EMCC template.
7. Edit existing fields, and add new fields as required.
8. Click **Save** to add the EMCC template.

Modify EMCC template

1. Log in as Provider administrator or higher.
2. Set the hierarchy to the relevant customer or location node.
3. Go to **EMCC Configuration Templates**.
4. Click on the EMCC template that you want to edit. See also *Configuration templates* for more information.
5. Edit and add the required fields, making sure that all mandatory fields are complete.
6. Click **Save** to save the modified EMCC template.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete EMCC template

To delete an EMCC template, click on the template to delete, on the EMCC templates list view, then click **Delete**.

EMCC route patterns

Tip: *Use the Action search to navigate Automate*

Add EMCC route pattern

1. Log in as provider administrator or higher.
2. Set the hierarchy to the relevant customer.
3. Go to the **EMCC Route Patterns** page.
4. Click the Plus icon (+) to add an EMCC Route Pattern.
5. Fill out details:
   a. **Country**. Choose the relevant ISO country code from the drop-down list.
   b. **Pattern**. Enter the route pattern, including numbers and wild cards. Do **not** use spaces in your route pattern.
   c. **Called Party Transformation Mask**. Enter a transformation mask value. Valid entries include digits 0 to 9, the wild card character X. Note that if this field is left blank, no calling party transformation takes place.
6. Click **Save** when complete to add the EMCC Route Pattern.

Modify EMCC route pattern

1. Log in as provider administrator or higher.
2. Set the hierarchy to the relevant customer.
3. Go to the **EMCC Route Patterns** page.
4. Click the EMCC route pattern that you want to modify.
5. Update the following fields as required:
   a. **Country**. Choose the relevant ISO country code from the drop-down list.
   b. **Pattern**. Enter the route pattern, including numbers and wild cards. Do **not** use spaces in your route pattern.
   c. **Called Party Transformation Mask**. Enter a transformation mask value. Valid entries include digits 0 to 9, the wild card character X. Note that if this field is left blank, no calling party transformation takes place.
6. Click **Save** when complete to save the changes to the EMCC route pattern.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete EMCC route pattern

To delete an EMCC route pattern, click on the pattern to delete on the **EMCC Route Patterns** list view, and then click **Delete**.

Routing

Route groups

Tip: *Use the Action search to navigate Automate*

Overview

A route group allows you to define the order in which gateways are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

For example, if you use two long distance carriers, you could add a route group so that long distance calls to the less expensive carrier are given priority. Calls only route to the more expensive carrier if the first trunk is unavailable.

Configure route groups

This procedure adds or updates route groups.

Prerequisites:

- You must define one or more gateway or SIP trunks before you add a route group.

Note: Each gateway or gateway and port combination can only belong to one route group and can only be listed once within that route group. All gateways in a route group must have the same route pattern. The pattern is assigned to the route list containing the route group (not the route group itself).

Route groups are optional. If a proposed route group only contains one gateway or one gateway and port combination and that route group is not to be included in a route list, the route group is not needed.

Perform these steps:

1. Log in as Provider, Reseller or Customer administrator.
2. Go to (Cisco UCM) **Route Groups**.
3. **Choose an option**:
   - **Add new route group**? Click **Add**. Go to step 4.
   - **Edit an existing route group**? Click the group to be updated, edit the fields as required, then click **Save** to save the edited route group.
4. In the **CUCM** drop-down, select the Cisco Unified Communications Manager corresponding to the route group.

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. In the **Route Group Name** field, enter a unique name for the new route group.

   Note: A route group name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, period(s), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.

   Use concise and descriptive names for the route group. The `CompanynameLocationGroup` format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route group. For example, - CiscoDallasAA1 - identifies a Cisco Access Analog route group for the Cisco office in Dallas.

6. Select Distribution Algorithm options for the route group. The default value is Circular.

Option	Description
Top Down	Allows UCM to distribute a call to idle or available members starting with the first idle or available member of a route group to the last idle or available member of a route group. This option is mandatory if you want to prioritize the order of devices.
Circular	Allows UCM to Communications Manager to distribute a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which the UCM most recently extended a call. If the nth member is the last member of a route group, UCM distributes a call starting from the top of the route group.

7. Click the Plus icon (+) to open the **Members** box.
8. Choose an option:
   - Add a device to the route group? Go to Step 9.
   - Modify the priority of a device? Go to Step 10.
   - Remove a device from the route group? Select the relevant device, and click the Minus sign (-). Ensure you leave at least one device in the route group.
8. To add a device to the route group:
   a. From the **Device Name** drop-down menu, choose the device where the route group is added.

      Note: When adding a SIP trunk or gateway, all ports on the device are selected.

   b. For Device Selection Order, indicate the order in which to prioritize multiple devices. A lower selection order indicates higher priority. This field requires an integer value. The default is no setting. The device selection order, if specified, overrides the position of the device in the list.
   c. To add another device to the route group, click the Plus icon (+) at **Members**, then repeat this step for each device you want to add.
10. If no device selection order is specified, you can change the priority of a device by moving the device up or down in the list by clicking the arrows on the right side of the **Members** box. Using the Up arrow, move the device higher in the list to make it a higher priority in the route group, or using the Down arrow, move the device lower in the list to make it a lower priority in the route group.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: The Top Down distribution algorithm must be selected in Step 6 to prioritize the order of devices.

11. Click **Save**. The new route group displays **Route Group** list.

Delete a route group

To delete a route group:

1. Log in as Provider, Reseller or Customer administrator.

Warning: When deleting a route group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to delete a route group at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

2. Go to **Route Groups**.
3. From the list of trunks, select the route group you wish to delete.
4. Click **Delete**, then click **Yes** to confirm.

Route lists

Tip: *Use the Action search to navigate Automate*

Overview

Route lists are made up of route groups and are associated with route patterns. A route list associates a set of route groups with a route pattern and determines the order in which those route groups are accessed. The order controls the progress of the search for available trunk devices for outgoing calls.

A route list can contain only route groups. Each route list should have at least one route group. Each route group includes at least one device, such as a gateway, that is available. Based on device type, Cisco Unified Communications Manager (Cisco UCM) can choose some, or all, ports as resources in each route group. Some devices, such as digital access, only allow you to choose all ports.

You can add a route group to any number of route lists.

Configure route groups

This procedure adds route lists and adds, removes, or changes the order of route groups in a route list.

Pre-requisites:

- Configure the route groups.

Perform these steps:

Copyright © 2025 VisionOSS Limited. All rights reserved.

1. Log in to as Provider, Reseller or Customer administrator.

   Note: When configuring a route list as a provider or reseller, ensure that you select a valid customer or site under your customer in the hierarchy node breadcrumb at the top of the view.

2. Go to **Route Lists**.
3. **Choose an appropriate option**:
   - **Add a new route list**? Click the Plus icon (+) to add a new record, then go to Step 4.
   - **Edit an existing route list**? Choose the list to be updated by clicking on its box in the leftmost column, then click **Edit** to update the selected route list. Go to Step 5.
4. Complete at minimum, the mandatory *Route lists configuration*.
5. To add a route group to this route list, click + on the right side of the **Route Group Items** box and complete at minimum, the mandatory *Route Group settings*.
6. To remove a route group from this route list, click - on the right side of its row in the **Member** box.
7. To change the priority of a route group, move it up or down in the list by clicking the arrows on the right side of the **Member** box. Using the Up arrow, move the group higher in the list to make it a higher priority, or using the Down arrow, move the group lower in the list to make it a lower priority.
8. To save a new or updated route list, click **Save**.

Route lists configuration

Field	Description
CUCM *	Select a Cisco UCM for the route list. Mandatory.
Name *	Enter a unique name for the new route list. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, period(s), hyphens (-), and underscore characters (_). This field is mandatory. Tip: Use concise and descriptive names for the route list. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route list. For example, 'CiscoDallasMetro' identifies a route list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.
Description	A description of the route list.
Call Manager Group Name *	Select a Cisco UCM Group. Default is the default field. You can choose from **Default**, **None**, or select a group. This field is mandatory. Note: The route list registers with the first UCM in the group (which is the Primary UCM).
Route List Enabled	Select to enable the route list. This is the default. Clear to disable the route list. When disabling a route list, calls in progress do not get affected, but the route list does not accept additional calls.
Run on Every Node	Select to enable the active route list to run on every node.
Route Group Items	See "Route Group Items fields".

Copyright © 2025 VisionOSS Limited. All rights reserved.

Route Group settings

Field	Description
Route Group *	Choose the route group. This field is mandatory.
Selection Order	Indicate the order in which to prioritize multiple routes. A lower selection order indicates higher priority. This field requires an integer value. The default is no setting.
Use Calling Party's External Phone Number Mask *	Choose **On** from the drop-down list if you want the full external phone number to be used for calling line identification (CLID) on outgoing calls. Choose **Off** or **Default** if you do not want to use the full external phone number for CLID on outgoing calls. You may also configure an External Phone Number Mask on all phone devices. This field is mandatory.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the **Digit Discards** field is blank, the **Prefix Digits** field is blank, the **Calling Party Transformation Mask** field is blank, and **Use Calling Party's External Phone Number Mask** is set to **Off** or **Default**, no calling party transformation takes place.
Calling Party Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Party Number Type	Choose the format for the number type in calling party directory numbers. Cisco UCM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non national type numbering plan. Choose one of the following options: • **Cisco CallManager** - Use when the Cisco UCM sets the directory number type. • **Unknown** - Use when the dialing plan is unknown. • **National** - Use when you are dialing within the dialing plan for your country. • **International** - Use when you are dialing outside the dialing plan for your country. • **Subscriber** - Use when you are dialling a user by using a shortened user number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco UCM sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • **Cisco CallManager** - Use when the Cisco UCM sets the numbering plan in the directory number. • **ISDN** - Use when you are dialing outside the dialing plan for your country. • **National Standard** - Use when you are dialing within the dialing plan for your country. • **Private** - Use when you are dialing within a private network. • **Unknown** - Use when the dialing plan is unknown.
Called Party Discard Digits	Choose the discard digit instructions that you want to be associated with this called party transformation pattern.
Called Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Called Party Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#),the international escape character +, and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco UCM sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • **Cisco CallManager** - Use when the Cisco UCM sets the directory number type. • **Unknown** - Use when the dialing plan is unknown. • **National** - Use when you are dialing within the dialing plan for your country. • **International** - Use when you are dialing outside the dialing plan for your country. • **Subscriber** - Use when you are dialling a user by using a shortened user number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco UCM sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • **Cisco CallManager** - Use when the Cisco UCM sets the numbering plan in the directory number. • **ISDN** - Use when you are dialing outside the dialing plan for your country. • **National Standard** - Use when you are dialing within the dialing plan for your country. • **Private** - Use when you are dialing within a private network. • **Unknown** - Use when the dialing plan is unknown.

Route partitions

Tip: *Use the Action search to navigate Automate*

Overview

A partition contains a list of route patterns (directory number (DN) and route patterns). Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.

Tip: Use concise and descriptive names for your partitions. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

Configure route partitions

If you're updating a partition, use the **Apply Config** button (as described in this procedure) to synchronize a partition with affected devices. When you apply the configuration to devices that are associated with the partition, all calls on affected gateways drop.

1. Log in as the Provider, Reseller, or Customer administrator.
2. Go to **Route Partitions**.
3. Choose the relevant hierarchy.
4. Choose an option:
    - To add a new route partition, click **Add**, then go to step 5.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To edit an existing route partition, click the line item in the table. Go to step 6.

5. In the pop-up, select from the drop-down the network device list (NDL) to which you are adding the route partition, and click **OK**.

Note: The NDL pop-up only appears when you are adding a new route partition. If you are updating an existing partition, go to step 6.

If you are adding the partition to a site hierarchy node, the NDL pop-up will not appear. You will go right to the route partitions add page using the NDL associated to the site.

6. On the **Route Partitions** page, modify the following fields as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Name (Mandatory)	Enter a name for the new partition that you are creating. Ensure that each partition name is unique to the route plan. Partition names can contain a-z, A-Z, and 0-9 characters, as well as spaces, hyphens (-), and underscore characters (_). Note: The length of the partition names limits the maximum number of partitions that can be added to a calling search space (CSS). The CSS partition limitations table provides examples of the maximum number of partitions that can be added to a CSS with partition names of fixed length.
Description	Enter a description of the new partition that you are creating. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (), angle brackets (<>), or brackets ([ ]). If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field. Default value: None
Time Schedule	From the drop-down list box, choose a time schedule to associate with this partition. The associated time schedule specifies when the partition is available to receive incoming calls. This field is empty by default, which indicates that time-of-day routing is not in effect and the partition remains active. With the time zone value in the following field, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks incoming calls to this partition against the specified time schedule.
Time Zone	Choose one of the following options to associate a partition with a time zone: • Use Originating Device Time Zone: If you choose this option, the system checks the partition against the associated time schedule with the calling device’s time zone. • Time Zone: If you choose this option, choose a time zone from the drop-down list box. The system checks the partition against the associated time schedule at the time that is specified in this time zone. These options all specify the time zone. When an incoming call occurs, the current time on the Cisco Unified Communications Manager gets converted into the specific time zone set when one option is chosen. The system validates this specific time against the value in the Time Schedule field.

The following table provides examples of the maximum number of partitions that can be added to a CSS if partition names are of fixed length.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86
...	...
10 characters	46
15 characters	32

7. Click **Save**. The route partition appears in the route partition list.
   - To modify any of these properties, click the item in the list, make your changes, and click **Save**.
   - To delete a route partition, select the checkbox to the left of the Name column in the group list, and click **Delete**.

SIP route patterns

Tip: *Use the Action search to navigate Automate*

Overview

provider

Cisco Unified Communications Manager (Cisco UCM) uses SIP route patterns to route or block both internal and external calls.

The domain name or IP address provides the basis for routing. The administrator can add domains, IP addresses, and IP network (subnet) addresses and associate them to SIP trunks (only). This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

Configure SIP route patterns

This procedure configures a SIP route pattern.

Prerequisites

- Configure at least one SIP Profile and SIP trunk before configuring a SIP route pattern.

Perform these steps

1. Log in as Provider, Reseller, or Customer administrator.
2. Ensure that the hierarchy path is set to a customer or site level.
3. If prompted, choose the NDL that contains the UCM which you are configuring the SIP Route Pattern.
4. Go to **SIP Route Patterns**.
5. Click **Add**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Configure settings on the tabs/panels on this page:
   - *Pattern Definition Tab*
   - *Calling Party Transformations Tab*
   - *Connected Party Transformations Tab*
7. Click **Save**.

SIP Route Patterns settings

Pattern Definition Tab

Field	Description
Pattern Usage	From the drop-down list, choose either **Domain Routing** or **IP Address Routing**. This field is mandatory.
IPv4 Pattern	Enter the domain, subdomain, IPv4 address, or IP subnetwork address. This field is mandatory. For Domain Routing pattern usage, enter a domain name **IPv4 Pattern** field that can resolve to an IPv4 address. The domain name can contain the following characters: -, ., 0-9, A-Z, a-z, *,], and [. For IP Address Routing pattern usage, enter an IPv4 address with the format X.X.X.X, where X represents a number between 0 and 255. For the IP subnetwork address, in classless interdomain routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix that denotes the number of bits in the network address. Tip: If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.
IPv6 Pattern	UCM uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. Tip: If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 pattern.
Description	Enter a description of the SIP Route Pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Route Partition	If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, leave the Route Partition value empty.
SIP Trunk/Route List	Choose the SIP trunk or route list to which the SIP route pattern is associated. This field is mandatory.
Block Pattern	Select this check box if you want this pattern to be used for blocking calls.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Calling Party Transformations Tab

Field	Description
Use Calling Party's External Phone Mask	Select **On** if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. Select **Default** to use the default External Phone Number Mask. This field is mandatory.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 to 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not selected, no calling party transformation takes place.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 to 9 and the wildcard characters asterisk (*) and octothorpe (#). Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Line ID Presentation	Calling line ID presentation (CLIP/CLIR) is a supplementary service that allows or restricts the originating caller phone number on a call-by-call basis. Choose whether you want to allow or restrict the display of the calling party phone number on the called party phone display for this SIP route pattern. Choose **Default** if you do not want to change calling line ID presentation. Choose **Allowed** if you want to allow the display of the calling number. Choose **Restricted** if you want to block the display of the calling number.
Calling Line Name Presentation	Calling line name presentation (CNIP/CNIR) is a supplementary service that allows or restricts the originating caller name on a call-by-call basis. Choose whether you want to allow or restrict the display of the calling party name on the called party phone display for this SIP route pattern. Choose **Default** if you do not want to change calling name presentation. Choose **Allowed** if you want to allow the display of the caller name. Choose **Restricted** if you want to block the display of the caller name.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Connected Party Transformations Tab

Field	Description
Connected Line ID Presentation	Connected line ID presentation (COLP/COLR) is a supplementary service that allows or restricts the called party phone number on a call-by-call basis. Choose whether you want to allow or restrict the display of the connected party phone number on the calling party phone display for this SIP route pattern. Choose **Default** if you do not want to change the connected line ID presentation. Choose **Allowed** if you want to display the connected party phone number. Choose **Restricted** if you want to block the display of the connected party phone number. If a call originating from an IP phone on UCM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed.
Connected Line Name Presentation	Connected name presentation (CONP/CONR) is a supplementary service that allows or restricts the called party name on a call-by-call basis. Choose whether you want to allow or restrict the display of the connected party name on the calling party phone display for this SIP route pattern. Choose **Default** if you do not want to change the connected name presentation. Choose **Allowed** if you want to display the connected party name. Choose **Restricted** if you want to block the display of the connected party name.

Cisco UCM route patterns

Tip: *Use the Action search to navigate Automate*

Overview

Default Cisco Unified Communications Manager (Cisco UCM) dial plan route patterns are deployed as part of the default dial plan schemas that ship with the Automate template package.

This section describes how you can update these default CUCM dial plan route patterns.

Caution: The Cisco HCS default dial plan includes most common translation and route patterns and in most cases, should be added automatically when a customer dial plan, site dial plan, and voice mail service is provisioned. If you wish to update translation and route patterns using Automate, you must have a full understanding of the Cisco HCS dial plan. Refer to the Automate Dial Plan Management Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure UCM route patterns

This procedure updates the UCM route patterns that are provisioned by the dial plan schema, and adds new new route patterns from Automate that are not part of the standard dial plan package.

Note: For more information on the latest UCM route patterns, refer to http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Perform these steps

1. Log in as a Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node where you want to add or edit the route pattern.
3. Go to **Route Patterns**.
4. Choose an option:
   - **Add a new route pattern**? Click **Add**, then go to Step 5.
   - **Edit an existing route pattern**? Click on the route pattern to be updated and go to Step 6.
5. From the **CUCM** drop-down menu, select the hostname, domain name, or IP address of the Unified CM to which you want to add the route pattern.

   Note: The **CUCM** drop-down menu only appears when adding a route pattern, and not when editing an existing route pattern.

   Important: If you're adding or editing a route pattern at any hierarchy node above a site level, the only CUCMs that appear in the **CUCM** drop-down list are CUCMs that are located at the node where you're adding the route pattern, and all CUCMs in hierarchies above the node where you're adding the route pattern. If you're adding or editing a route pattern at a site level, the CUCM that appears in the **CUCM** drop-down list is the CUCM in the site's Network Device List (NDL). If the site does not have an NDL, or the NDL at the site does not have a CUCM, the drop-down list is empty and a route pattern cannot be added to the site.

6. Mandatory. In the **Route Pattern** field, enter the route pattern, or modify the existing route pattern, as required.

   Note: Enter the route pattern, including numbers and wildcards (do not use spaces); for example, enter 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +.

7. If you want to use a partition to restrict access to the route pattern, choose the relevant partition from the **Route Partition** drop-down. If you do not want to restrict access to the route pattern, choose <None> for the partition.

   Note: Ensure that the combination of route pattern, route filter, and partition is unique within the CUCM cluster.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8. In the **Description** field, enter a description for the route pattern and route partition if desired.

   Note: Description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

9. Complete at minimum, the mandatory fields on each of the tabs/panels on this page, as appropriate.
10. Click **Save**.

Route patterns configuration settings

Pattern Definition

Tip: Use the Corresponding Cisco UCM Attribute information provided in the table to manually verify in the UCM GUI that fields have been mapped correctly.

Option	Description
MLPP Precedence *	From the drop-down menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern: • Executive Override - Highest precedence setting for MLPP calls • Flash Override - Second highest precedence setting for MLPP calls • Flash - Third highest precedence setting for MLPP calls • Immediate - Fourth highest precedence setting for MLPP calls • Priority - Fifth highest precedence setting for MLPP calls • Routine - Lowest precedence setting for MLPP calls • Default - Does not override the incoming precedence level but rather lets it pass unchanged Default: Default Corresponding Unified CM Attribute: MLPP Precedence.
Apply Call Blocking Percentage	Select this check box to enable the Destination Code Control (DCC) feature. By enabling DCC, all calls other than flash and higher precedence calls made to destination are filtered and allowed or disallowed based on the Call Blocking Percentage quota set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default. Note: The **Apply Call Blocking Percentage** field gets enabled only if the MLPP level is immediate, priority, routine, or default. Default: Clear Corresponding Unified CM Attribute: Apply Call Blocking Percentage.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Call Blocking Percentage	Enter the percentage of calls to be blocked for this destination in numerals. This value specifies the percentage of lower precedence calls made to this destination that get blocked by the route pattern. This percentage limits the lower precedence calls only; the flash and higher precedence calls made to this destination are allowed at all times. Values between 0 and 99 are allowed. Note: Unified CM calculates the maximum number of low priority calls to be allowed through this route pattern based on the call blocking percentage that you set for this destination. Note: The **Call Blocking Percentage** field gets enabled only if the **Apply Call Blocking Percentage** check box is selected. Default: None Corresponding Unified CM Attribute: <Entry box next to Apply Call Blocking Percentage>.
Route Class *	From the drop-down menu, choose a route class setting for this route pattern: • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data The route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. The Default setting uses the existing route class of the incoming call. You can use non-default route class settings to translate an inbound T1 CAS route class digit into a Unified CM route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration. If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class. Default: Default Corresponding Unified CM Attribute: Route Class.
Route List (Mandatory if gateway or trunk is not specified)	Choose the route list for which you are adding a route pattern. Default: None Corresponding Unified CM Attribute: Gateway/Route List.
Gateway/Trunk (Mandatory if route list is not specified)	Choose the gateway or trunk list for which you are adding a route pattern. Note: If the gateway is included in a Route Group, this drop-down menu does not display the gateway. When a gateway is chosen in the drop-down menu, Unified CM uses all the ports in the gateway to route or block this route pattern. This action does not apply for MGCP gateways. Default: Clear Corresponding Unified CM Attribute: Gateway/Route List.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Block this pattern	Indicates whether you want this route pattern to be used for routing calls (such 8[2-9]XX) or for blocking calls. Default: Clear (meaning route pattern is used for routing calls). Corresponding Unified CM Attribute: Block this pattern.
Block Reason	If you click Block this pattern radio button above, you must choose the reason that you want this route pattern to block calls. From the drop-down menu, choose one of: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded Default: No Error Corresponding Unified CM Attribute: <entry box next to Block this pattern>.
Call Classification *	Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. When adding a route pattern, if you clear the **Provide Outside Dial Tone** check box, you set Call Classification as OnNet. Default: OnNet Corresponding Unified CM Attribute: Call Classification.
Allow Device Override	When the check box is selected, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet. Default: Clear Corresponding Unified CM Attribute: Allow Device Override
Provide Outside Dial Tone	Leave this check box selected to provide outside dial tone. To route the call in the network, clear the check box. Default: Clear Corresponding Unified CM Attribute: Provide Outside Dial Tone.
Allow Overlap Sending	With overlap sending enabled, when Unified CM passes a call to the PSTN, it relies on overlap sending in the PSTN to determine how many digits to collect and where to route the call. Select this check box for each route pattern that you consider to be assigned to a gateway or route list that routes the calls to a PSTN that supports overlap sending. The Client Matter Code (CMC) and Forced Authorization Code (FAC) features do not support overlap sending because the Unified CM cannot determine when to prompt the user for the code. If you select the **Require Forced Authorization Code** or the **Require Client Matter Code** check box, the system clears the **Allow Overlap Sending** check box. Default: Clear Corresponding Unified CM Attribute: Allow Overlap Sending
Urgent Priority	If the dial plan contains overlapping patterns, Unified CM does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Select this check box to interrupt interdigit timing when Unified CM must route a call immediately. Default: Clear Corresponding Unified CM Attribute: Urgent Priority.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Require Forced Authorization Code	If you want to use forced authorization codes with this route pattern, select the check box. The FAC feature does not support overlap sending because the Unified CM cannot determine when to prompt the user for the code. If you select the **Allow Overlap Sending** check box, you should clear the **Require Forced Authorization Code** check box. Default: Clear Corresponding Unified CM Attribute: Require Forced Authorization Code.
Authorization Level *	Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern. Range is 0 to 255. Default: 0 Corresponding Unified CM Attribute: Authorization Level
Require Client Matter Code	If you want to use client matter codes with this route pattern, select this check box. The CMC feature does not support overlap sending because the Unified CM cannot determine when to prompt the user for the code. If you select the **Allow Overlap Sending** check box, you should clear the **Require Client Matter Code** check box. Default: Clear Corresponding Unified CM Attribute: <Entry box next to Authorization Level>.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Calling Party Transformations

Option	Description
Use Calling Party's External Phone Number Mask	Select the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. Note: The calling party transformation settings that are assigned to the route groups in a route list override any calling party transformation settings that are assigned to a route pattern that is associated with that route list. Default: Default Corresponding Unified CM Attribute: Use Calling Party's External Phone Number Mask
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is clear, no calling party transformation takes place. Default: None Corresponding Unified CM Attribute: Calling Party Transform Mask
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Line ID Presentation *	Unified CM uses calling line ID presentation/restriction (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party phone number on the called party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change calling line ID presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling number. • Restricted - Choose if you want Unified CM to block the display of the calling number. For more information about this field, see topics related to calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Line ID Presentation.
Calling Name Presentation *	Unified CM uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party name on the called party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change calling name presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling name information. • Restricted - Choose if you want Unified CM to block the display of the calling name information. For more information about this field, see calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Name Presentation.
Calling Party Number Type *	Choose the format for the number type in calling party directory numbers. Unified CM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of: • Unified CM - the Unified CM sets the directory number type. • Unknown - The dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when dialing a user by using the shortened user name. Default: Unified CM Corresponding Unified CM Attribute: Calling Party Number Type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Calling Party Numbering Plan *	Choose the format for the numbering plan in calling party directory numbers. Unified CM sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of: • Unified CM - Use when the Unified CM sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown. Default: Unified CM Corresponding Unified CM Attribute: Calling Party Numbering Plan.

Connected Party Transformations

Option	Description
Connected Line ID Presentation *	Unified CM uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party phone number on the calling party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change the connected line ID presentation. • Allowed - Choose if you want to display the connected party phone number. • Restricted - Choose if you want Unified CM to block the display of the connected party phone number. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Line ID Presentation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Connected Name Presentation *	Unified CM uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party name on the calling party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change the connected name presentation. • Allowed - Choose if you want to display the connected party name. • Restricted - Choose if you want Unified CM to block the display of the connected party name. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Name Presentation.

Called Party Transformations

Option	Description
Discard Digits	Choose the discard digits instructions that you want to be associated with this route pattern. See topics related to discard digits instructions in the Cisco Unified Communications Manager System Guide for more information. Default: None Corresponding Unified CM Attribute: Discard Digits.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed. Default: None Corresponding Unified CM Attribute: Called Party Transform Mask.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#);the international escape character +; and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Called Party Number Type *	Choose the format for the number type in called party directory numbers. Unified CM sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of: • Unified CM - Use when the Unified CM sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you're dialing a user by using a shortened user number. Default: Unified CM Corresponding Unified CM Attribute: Called Party Number Type.
Called Party Numbering Plan *	Choose the format for the numbering plan in called party directory numbers. Unified CM sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of: • Unified CM - Use when the Unified CM sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown. Default: Unified CM Corresponding Unified CM Attribute: Called Party Numbering Plan.

CTI route points

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

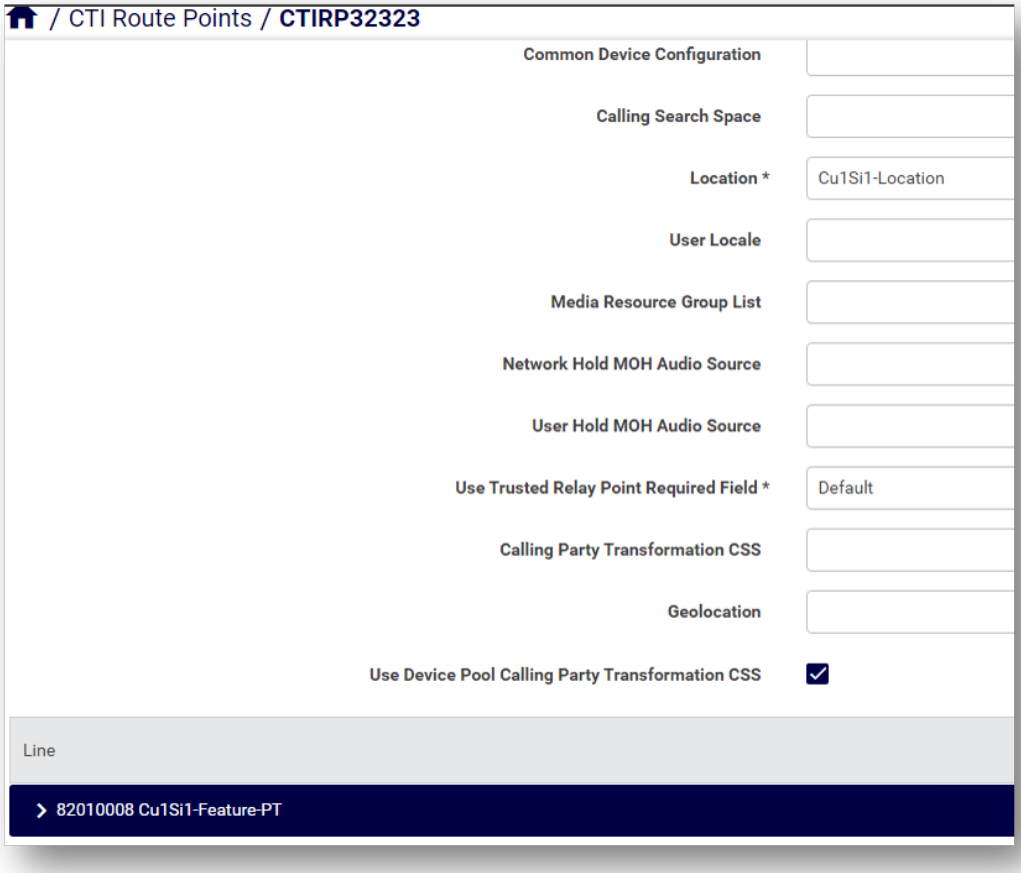
Overview

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

Add a CTI route point

This procedure adds a CTI route point.

1. Log in as Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the site for which you want to configure CTI route points.
3. Go to **CTI Route Points**.
4. Choose an option:
   - To view the details on an existing CTI route point, click an entry in the list view.



   - To add a new CTI route point, click **Add**. Go to step 5.
5. Complete at least the mandatory fields. See *CTI route points settings*.
6. In the **Line** section, click the Plus icon (+) to associate a line with the CTI route point. Complete at least the mandatory fields. See *CTI route points line settings*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

7. Click **Save**.

CTI route points settings

Option	Description
Device Name *	Enter a unique identifier for this device, from 1 to 15 characters, including alphanumeric, dot, dash, or underscores. This field is mandatory.
Description	Enter a descriptive name for the CTI route point. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool *	Choose the name of a Device Pool. The device pool specifies the collection of properties for this device, including Cisco UCM group, Date Time Group, Region, and Calling Search Space for autoregistration. This field is mandatory.
Common Device Configuration	Choose the common device configuration to which you want this CTI route point assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure common device configurations in the Common Device Configuration window.
Calling Search Space	From the drop-down list, choose a calling search space. The calling search space specifies the collection of partitions that are searched to determine how a collected (originating) number is routed.
Location *	From the drop-down list, choose the appropriate location for this CTI route point. This field is mandatory. Locations implement call admission control (CAC) in a centralized call-processing system. CAC regulates audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls between locations. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of Hub_None means that the locations feature does not track the bandwidth that this CTI route point consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.
User Locale	From the drop-down list, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font. Note: If no user locale is specified, Cisco UCM uses the user locale that is associated with the device pool
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List is a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources. The application chooses according to the priority order defined in a Media Resource Group List. If you choose <none>, Cisco UCM uses the Media Resource Group that is defined in the device pool.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option	Description
Network Hold MOH Audio Source	Choose the audio source that plays when the network starts a hold action. If you do not choose an audio source, Cisco UCM uses the audio source that is defined in the device pool. If the device pool does not specify an audio source, the system default is used.
User Hold MOH Audio Source	Choose the audio source that plays when an application starts a hold action. If you do not choose an audio source, Cisco UCM uses the audio source that is defined in the device pool. If the device pool does not specify an audio source, the system default is used.
Use Trusted Relay Point Required Field *	Enable or disable whether Cisco UCM inserts a trusted relay point (TRP) device with this media endpoint. This field is mandatory. Choose one of the following values: • **Default** - If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • **Off** - Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **On** - Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Tip: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Calling Party Transformation CSS that you configured in the CTI Route Point Configuration window.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CTI route points line settings

Field	Description
Directory Number *	Enter a dialable phone number. Values can include route pattern wildcards and numeric characters (0 to 9). Special characters such as a question mark (?), exclamation mark (!), backslash (\), brackets ([ ]), plus sign (+), dash (-), asterisk (*), caret (^), pound sign (#), and an X are also allowable. Special characters that are not allowed are a period (.), at sign (@), dollar sign ($), and percent sign (%). This field is mandatory. At the beginning of the pattern, enter \+ if you want to use the international escape character +. For this field, \+ does not represent a wildcard; instead, entering \+ represents a dialable digit. When saving the CTI route point, the combination of directory number and route partition name displays as a summary header in the **Line** section.
Route Partition *	Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the Directory Number field is unique within the partition that you choose. If you do not want to restrict access to the directory number, choose <None> for the partition. When saving the CTI route point, the combination of directory number and route partition name displays as a summary header in the **Line** section.
Index	This field is the line position on the device. If left blank, an integer is automatically assigned.
External Phone Number Mask	Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number, the international escape character +, and "X" characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.
Line Text Label	Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line and phone combination. Suggested entries include boss name, department name, or other appropriate information to identify multiple directory numbers to a secretary or assistant who monitors multiple directory numbers.
Display (Internal Caller ID)	Leave this field blank to have the system display the extension. Use a maximum of 30 characters. Typically, use the username or the directory number. If using the directory number, the person receiving the call may not see the proper identity of the caller.
ASCII Display (Caller ID)	This field provides the same information as the Display (Internal Caller ID) field, but limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the ASCII Display (Internal Caller ID) field.
Ring Setting (Phone Active)	If applicable, the ring setting that is used when this phone has another active call on a different line. Choose one of the following options: • **Use system default** • **Disable** • **Flash only** • **Ring once** • **Ring** • **Beep only**

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Ring Setting (Phone Idle)	If applicable, the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Choose one of the following options: • **Use system default** • **Disable** • **Flash only** • **Ring once** • **Ring**
Recording Option	This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled. Choose one of the following options: • **Call Recording Disabled** - Calls made on this line appearance cannot be recorded. • **Automatic Call Recording Enabled** - Calls made on this line appearance are recorded automatically. • **Selective Call Recording Enabled** - Calls made on this line appearance can be recorded using a softkey or programmable line key that is: – assigned to the device – a CTI-enabled application – both interchangeably
Recording Profile	This field determines the recording profile on the line appearance of an agent.
Recording Media Source	This field determines the recording media source option on the line appearance. Choose one of the following options: • **Gateway Preferred** - Voice gateway is selected as the recording media source when the call is routed through a recording enabled gateway. • **Phone Preferred** - Phone is selected as the recording media source.
Monitoring Calling Search Space	The monitoring calling search space of the supervisor line appearance must include the agent line or device partition to allow monitoring the agent.
Visual Message Waiting Indicator Policy	Use this field to configure the handset lamp illumination policy. Choose one of the following options: • **Use System Policy** (The directory number refers to the service parameter "Message Waiting Lamp Policy" setting.) • **Light and Prompt** • **Prompt Only** • **Light Only** • **None**
Audible Message Waiting Indicator Policy	Use this field to configure an audible message waiting indicator policy. Choose one of the following options: • **Off** • **On** - When you select this option, you receive a stutter dial tone when you take the handset off hook. • **Default** - When you select this option, the phone uses the default that was set at the system level.
Log Missed Calls	If selected, Cisco UCM logs missed calls in the call history for the shared line appearance on the phone.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Busy Trigger	This setting, working with Maximum Number of Calls and Call Forward Busy, determines the maximum call number for the line. Use this field with Maximum Number of Calls for CTI route points. The default specifies 4500 calls
Maximum Number of Calls	For CTI route points, you can configure up to 10,000 calls for each port. The default specifies 5000 calls. Use this field with the **Busy Trigger** field. Note: We recommend that you set the maximum number of calls to no more than 200 per route point. This prevents system performance degradation. If the CTI application needs more than 200 calls, we recommend that you configure multiple CTI route points.
Dialed Number	Select to display original dialed number upon call forward.
Redirected Number	Select to display the redirected number upon call forward.
Caller Number	Select to display the caller number upon call forward.
Caller Name	Select to display the caller name upon call forward.
End User, User ID	The User ID of a user associated with the line.

Call Redirection Routing Plan for Disaster Recovery

Overview

VOSS Automate provides a set of tools to configure and enable alternate call routing for disaster recovery (DR) from the failure of back-end services. This allows business continuity for end-customers, without service provider engagement.

Note: This feature only supports Oracle SBCs (Session Border Controller) and will provision the required redirection routing entries in the Local Route Table (LRT) of the Oracle SBC.

The feature provides the following:

- An interface to manage DR routing plans
- An interface to enable/disable DR routing plans
- Email notifications to addressees or groups of enabled and disabled DR routing plans

High level administrators with required permissions can expose the necessary interfaces for the models of this feature on menu layouts and ensure user access profiles are updated accordingly:

- `relation/dr_routing_plan_rel`: manage call redirection routing plans
- `view/dr_routing_plan_view`: enable/disable call redirection routing plans

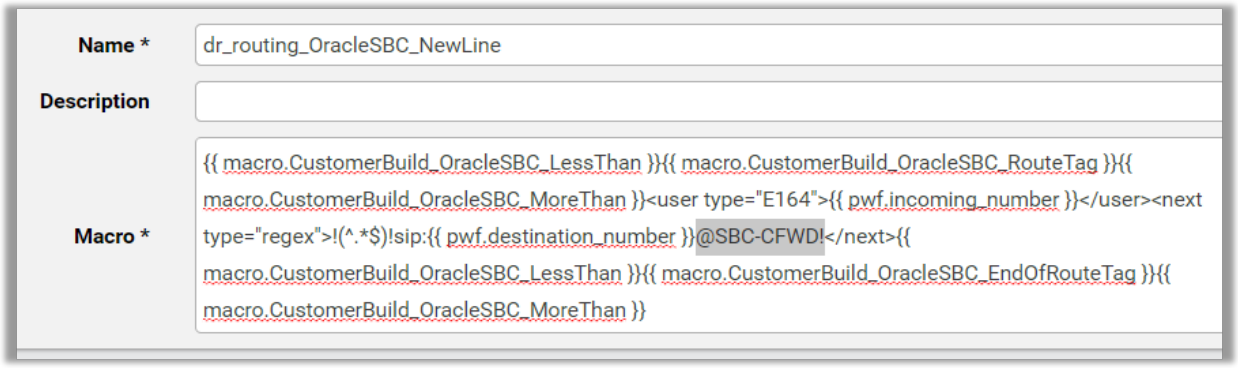
The instance of `data/EmailHtmlTemplate` called `DR Activation` is the email notification template that by default contains variables:

- `{{ pwf.EMAIL.status }}`: activated/deactivated
- `{{ pwf.EMAIL.plans }}`: list of DR plans

The following macro is used when creating the redirection entry and will need to be cloned down and customized to set the value after the @ symbol, as required:

- `dr_routing_OracleSBC_NewLine`

Copyright © 2025 VisionOSS Limited. All rights reserved.



Manage Call Redirection Routing Plans

If this model interface is available to an administrator, the list of plans is available to manage.

Note: The input form provides an interface to add *individual numbers* per plan. A separate plan is required for each number to be redirected. (This feature is typically used on a small scale.)

To add or modify a plan:

1. Add or update the **DR Plan name** and **Description**.
2. Add the **Destination Number** in E164 Format
3. Add or update the **Network Device List** that contains the session-based controller (SBC - `device/oraclesbc/`) that holds the local routing table configuration. This routing configuration on the SBC is then of a higher priority than any other routing.

   See: *Network device lists (NDLs)*.
4. Choose to enter individual **Email Addresses** and select an **Email Group Name** from the drop-down list to receive an email notification when a redirection routing plan is activated or deactivated.

   This feature requires the setup of:

   - an SMTP server - see: *Add a SMTP Server*
   - if used, email groups - see: *Email groups*.
5. Select an **Incoming Number** from the drop-down list that requires redirection.

The **Current Activation Status** will show if the current plan has been activated or not.

Enable or Disable Call Redirection Routing Plans

If this model interface is available to an administrator, a set of transfer boxes is available to activate or deactivate selected plans that have been created.

1. Choose the operation to be carried out on the selected plans: **Enable selected DR plans** or **Disable selected DR plans**
2. In the **Plans** transfer box, move created plans according to the selected required enable or disable operation.
3. When the operation is saved:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Individual updates are made to the SBC available in the NDL: an update per selected plan.
- If email messaging has been set up, target addressees and groups are sent an email notification of the operations.
- The **Current Activation Status** of a redirection routing plan is updated accordingly.

MGCP and SCCP Analog Gateways

CUCM Network Elements

Cisco CUCM LDAP Settings

Run Cisco UCM LDAP directory sync

Tip: *Use the Action search to navigate Automate*

This procedure runs an on-demand Cisco UCM LDAP directory sync to add new UCM users into a UCM from Automate.

Note: This sync uses Automate's generic driver to perform a doLdapSync AXL request. For details around regular scheduled syncs, see *LDAP user sync*.

To perform a UCM LDAP directory sync:

1. Log in to the Admin Portal as a Provider administrator or higher.
2. Go to **CUCM LDAP Directory Sync**.
3. From the **CUCM** drop-down, choose a UCM cluster.
4. From the **CUCM LDAP Directory Name** drop-down, choose the name of the LDAP directory to sync.
5. Select the **Sync** checkbox to define whether the sync will run once you save. The default is True.
6. Save your changes.

   If you have the **Sync** checkbox selected on this form, the sync triggers the workflow to add and update UCM users into the UCM LDAP directory.

User authentication

Overview

When logging in to a user interface, a user's credentials can be authenticated based on their credentials in:

- The internal system database
- An LDAP-based external authentication server
- A SAML-based identity management server

Copyright © 2025 VisionOSS Limited. All rights reserved.

User type	Description
Administrators	A user who can log in to the administrator interface. The presence of an administrator interface means that a system user instance exists.
Users	System users that have, or are linked to, user accounts in one or more UC applications. User management supports the management of UC application user accounts, which may in turn also be configured for local, LDAP, or SAML authentication.
API users	System users that connect directly to VOSS Automate, using the API. The system controls access to its service through HTTP basic authentication.

User authentication methods

VOSS Automate supports the following authentication methods for accessing the system (for administrators and end users):

- Local authentication
- LDAP Authentication
- Single-Sign-on (SSO)

The user's setup determines the type of authentication required to access the system.

The table describes the **Auth Method** settings that determine the authentication method:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Auth Method	Description
Automatic	The system setup determines the authentication method, for example, the presence and viability of LDAP servers, SSO IdPs, and so on. The scope, user type, and Auth Enabled settings on the server determines viability: • If a viable IdP server is detected, authentication defaults to SSO. Since this requires using the special SSO Login URL, login from the VOSS Automate login page will fail. • If viable LDAP servers are found, authentication is attempted against each server until one is successful or all fail. LDAP servers that have errors are skipped. • If neither of these external servers are found (IdP or LDAP), local authentication occurs. Authentication is performed in order of preference, in the user's hierarchy, or above: 1. Local user *only if* no LDAP, SSO IdP, in this hierarchy or above 2. LDAP server 3. SSO identity provider (IdP)
Local	User authentication is based on the password defined and stored locally in VOSS Automate, and the VOSS Automate credential policy defines the rules for the password (complexity, aging, etc), as well as further limits on session length, and so on. Local authentication can be done using username or email address. Local authentication is allowed if the authentication method is Local, and there are viable SSO and/or LDAP servers in scope (viable servers in the hierarchy). Users authenticated in this way are allowed to change their password once logged in. Password change is also available for Local users where such sync type CUCM-LDAP; where sync source is CUCM and user is LDAP synced.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Auth Method	Description
LDAP	The authentication method is LDAP authentication. Additional details can be provided to tie the user to a specific LDAP server or an alternate username can match to the one in LDAP (default is the VOSS Automate username). When using LDAP Authentication, the password rules that are a part of the credential policy in VOSS Automate do not apply, since the password is managed in the LDAP directory. Other credential policy rules, such as session length, are however applied, since these are managed by VOSS Automate.
SSO	The authentication method is Single Sign-on (SSO). Additional details can be provided to tie the user to a specific SSO IdP server or alternate username can match to the one in the IdP (default is the VOSS Automate username). The VOSS Automate credential policy is irrelevant, since password rules, session length, and so on are all managed by the IdP outside of Automate. Single Sign-on support is for authentication only. It does not use authorization capabilities that are possible via SAML to control the user's permissions *within* the application. No logout is supported when using SSO (single sign-out); that is, VOSS Automate will not initiate the termination of a session with the IdP (the VOSS session remains active as long as there is an active IdP session.

For SSO, see also *Single Sign On (SSO) Overview*.

Authentication method setting rules

When adding or modifying users, the user's Authentication Method is based on the **User Default Auth Method** setting in the system Global Settings, as well as on the rules outlined in the table below:

For details on these Global Settings, refer to the "Global Settings" topic in the Advanced Configuration Guide.

Action	Auth Method Setting Rule
Add user from GUI	GUI default to Global Setting, but can be changed.
Modify user from GUI	GUI default to current user Auth Method, but can be changed.
LDAP Add user sync	Automatic
LDAP modify user sync	Leave setting as is.
Unified CM add user	Apply setting from Global Settings.
Unified CM modify user	Leave setting as is.
Quick User add user	Apply setting from Global Settings.
Quick User modify user	Leave setting as is.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.3.8. Cisco Emergency Responder (CER)

Configure Cisco Emergency Responder (CER)

Tip: *Use the Action search to navigate Automate*

This procedure configures Cisco Emergency Responder (CER) on VOSS Automate.

Note: For more information on CER installation and setup, refer to the Cisco Emergency Responder Administration Guide.

1. Log in as the appropriate hierarchy administrator.
2. Set the hierarchy path to the correct level. Shared instances are created at the provider, reseller, or customer level. Dedicated instances are created at the customer level.
3. Go to the CER **Servers** page.
4. Choose an option:
   - To add a new Cisco Emergency Responder (CER) in VOSS Automate, click **Add**.
   - To modify an existing CER, click its name in the list of Cisco Emergency Responders.
5. Enter a name for the Cisco Emergency Responder in the **CER_Virtual Server Name** field.
6. If you're configuring a publisher node, select the **Publisher** checkbox.

   Note: The **Publisher** tab is populated only when the **Publisher** check box is selected.

7. Expand **Network Addresses**.
   a. Choose the SERVICE_PROVIDER_SPACE address space.
   b. Enter the IP address of the CER Server in the **IPV4 Address** field.

      Note: Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. VOSS Automate can't validate an entry that contains a blank space at the end of the hostname or IP address.

   c. The **Hostname** field is automatically populated with the CER Name. Edit it if necessary.
   d. Fill in the domain of the CER application.
   e. Provide an optional description for the network address.
8. Expand **Credentials**.
   a. Add credentials for PLATFORM and ADMIN credential types. Click + to add more credentials.
   b. Fill in the user ID and password that you configured when you installed the CER.
   c. Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
   d. Provide an optional description for the credential.

   PLATFORM and ADMIN are required for license management.

Copyright © 2025 VisionOSS Limited. All rights reserved.

9. Fill out the fields on the **Publisher** tab:

Field	Description
Version	Select the version of the CER servers in this cluster.
Multi-Tenant	Read-only. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.

10. Click **Save**.

Next Steps

- *Associate CER with Customers*

Associate CER with Customers

Tip: *Use the Action search to navigate Automate*

Prerequisites:

- Configure a customer.
- Perform this procedure at any hierarchy level at or above where the CER is configured, when you configure the VM in Cisco Unified Communications Domain Manager 10.6(x), or perform it at any time after the VM has been created.

Perform these steps:

1. Log in as a Provider or Reseller administrator.
2. Go to the CER **Servers** page.
3. Click the name of the CER cluster to associate with a customer.
4. Click the **Customer Association** tab.

   Note:

   The list of customers that appear on this tab are those at, and below your current hierarchy. For example, if you are at the Provider level, and the CER is at Reseller1, you can see all customers at the Provider level and below. An error will occur if you try to associate a customer out of the CER's scope.

5. Select the checkbox for each customer to be associated with the CER cluster.

   Note: To remove one or more customer associations from the CER cluster, clear the checkbox for each customer to be disassociated from the cluster.

6. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

View associated clusters on CER servers

Tip: *Use the Action search to navigate Automate*

Prerequisites:

- Customers must be associated with the Cisco Emergency Responder (CER) cluster in order to be viewed in this procedure, unless the CER is created at customer level.
- If the CER is created at the customer level, customer information is automatically filled in for the customer where the CER exists.

Perform these steps:

1. Log in as a Provider, Reseller, or Customer administrator.
2. Make sure that the hierarchy is set to the customer you wish to view.
3. Go to the CER **Servers** page.
4. Click the name of the CER cluster to be viewed. Information appears about the CER cluster. You can view a list of customers associated with the CER server by selecting the **Customer Association** tab.

6.3.9. Load Balancing

Introduction to load balancing

Cisco Unified Communications Manager (Cisco UCM) groups provide both call-processing redundancy and distributed call processing. You can distribute devices, device pools, and UCMs among the groups to improve redundancy and load balancing in your system.

A UCM group specifies a prioritized list of up to three UCMs. The first UCM in the list serves as the primary UCM for that group, and the other members of the group serve as secondary and tertiary (backup) UCMs.

Each device pool has one UCM group that is assigned to it. For example, Group 1 points to Device Pool 1, Group 2 points to Device Pool 2, and Group 3 points to Device Pool 3. When a device registers, it attempts to connect to the primary (first) UCM in the group that is assigned to its device pool. If the primary UCM is unavailable, the device tries to connect to the next UCM listed in the group, and so on.

Load balancing is a manual process on Cisco UCM, requiring you to perform the following tasks:

1. Add new, custom UCM groups and device pools.
2. Synchronize the groups and device pools into Automate.
3. Choose the appropriate group and device pool in the user management or phone configuration for the site. To create more than one configuration for a site, create at least two UCM groups, then associate a device pool to the appropriate UCM group.

To determine if load balancing is required for your network, you can check the current device traffic load in Cisco UCM, via System > Device Pool menu. When you click on the device configuration information for a specific device pool, the Device Pool Information field lists the number of members in the Device Pool. Compare different device pools to see if the members are evenly divided between pools.

To perform load balancing, see “Load Balancing Using Site Default Device Pool”.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Load balancing using site default device pool

Tip: *Use the Action search to navigate Automate*

This procedure load balances using the default site device pool and updates the default device pool to point to the appropriate Cisco Unified Communication Manager (Cisco UCM) group.

Note: A default device pool is created for each site when the site dial plan is deployed for the Type 1 through Type 4 dial plan schema groups.

Since you're using the default device pool, you don't need to create any additional device pools directly on CUCM. Using this configuration, redundancy is gained within a site while load balancing is gained across multiple sites. Since there is one device pool per site, all devices at a site home to the same sequence of CUCMs, providing failover redundancy. Devices in different sites home to different sequences of CUCMs, providing load balancing across the sites.

The default site device pool is not created until the Type 1 to 4 site dial plan has been deployed, which updates the Site Defaults to use the default device pool. If the site dial plan has not been deployed, you will not see a site default device pool in the form Cu<customerId>Si<siteId>-DevicePool.

In Automate you can determine the default device pool for a site in the site **Defaults** page.

Perform these steps:

1. Log in as Provider, Reseller, or Customer administrator.
2. Choose the relevant site.
3. Follow the steps outlined in *Create a Site Dial Plan* if you have not already done so; the Create a Site Dial Plan procedure creates the default site device pool instance.
4. Log in to Cisco Unified Communications Manager and create one or more UCM groups.

   Note: See Cisco Unified Communications Manager Administration Guide.

5. In Automate, perform a sync operation of the UCM via the **Data Sync** page.

   This sync updates the Automate cache and makes the UCM groups that were added directly on Cisco Unified Communications Manager available to Automate.

6. Associate a UCM group to a device pool and choose a UCM group other than the default group in the **Call Manager Group** drop-down list. See "Associate a CUCM Group to a Device Pool".

   Note: To verify that the phone or user uses the device pool as expected, open a user's settings in Automate, then select the required **Device Pool Name** setting from the drop-down under the **Phones** tab.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Associate a UCM group to a device pool

Tip: *Use the Action search to navigate Automate*

This procedure associates a Cisco UCM group with an existing device pool for each site.

This allows calls from a device that is tied to a device pool to go out on a specific UCM group based on the call type.

Note: You cannot use this procedure to add or delete device pools.

1. Log in as Provider, reseller or Customer administrator.

   Warning: When associating a UCM group, ensure that you choose a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to associate a UCM group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.

2. Go to **Device Pools**.
3. Click the device pool to be associated.
4. From the **Unified CM Group** drop-down, choose a specific CUCM group or leave the **Unified CM Group** as **Default**.
5. Save the new UCM group association.

6.3.10. VOSS Phone Server Management

Introduction to VOSS phone server

The VOSS phone server provides a method of hosting SIP compliant devices such as phones and softclients where it is not possible or desirable to connect these devices into other vendor platforms.

In an HCS environment, full integration management is provided where all trunk and dialplan related configuration is automatically applied. Other Cisco UCM dialplan designs may be utilized through the Automate dialplan additions templating feature.

The VOSS phone server provides three functions:

1. A SIP registrar allows the use of SIP devices from any compliant vendor, thereby allowing for a wide choice of phones with various feature sets, including the re-use of existing devices from systems such as Cisco Unified CM and others. Since the registrar requires only account definition per line, there is no phone concept in the Phone Server itself. Phones are represented in Automate and are a local construct only.
2. A SIP Switch handling SIP call traffic. Calls between phones hosted on the VOSS phone server are handled locally and calls to other extensions or PSTN destinations are offloaded over a SIP Trunk
3. Configuration File Management (Optional). Phone configuration files may be created and hosted in the VOSS phone server's ftp server. This allows unconfigured phones (i.e. new unused phones, or factory defaulted old phone stock) to obtain their configuration automatically when connected to the network.

   Sample configuration files for phones from SNOM, Grandstream and Cisco are included.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate utilities include:

1. System setup and Country dialplan management
2. Evaluation of the number of re-usable Cisco CUM hosted phones
3. Conversion of Cisco configuration to phone server configuration

The VOSS phone server is deployed as an OVA, typically alongside Cisco UCM Virtual Machines in an HCS/CUCM environment. Redundancy is an option, providing data replication between servers.

Managing VOSS phone servers

Adding phones requires three areas of configuration. These are all automated by Automate during the phone addition:

Set up call routing

In HCS mode, the CUCM dial plan is created to provide call routing of the chosen numbers towards VOSS phone server. This allows incoming call routing. Outbound calling Class of Service and routing are also configured to allow internal extension and E164 call routing. Number inventory and CLI management through transformation patterns are maintained.

1. Set up the VOSS phone server

   VOSS phone servers are managed on the customer hierarchy - verify that you are at the customer hierarchy.

   - **Version**: there is currently only 1.0.0 (base release version).
   - **Deployment Mode**: two options are available:
     - HCS - Automate manages the Cisco UCM dial plan and trunking, removing the need for manual integration. Use HCS to configure Unified CM call routing to the VOSS phone server. Standard Cisco dial plan integration uses a dial plan templating facility. Other dial plans may be supported by creating custom dial plan templates suitable for the dial plan in use.
     - Standalone - manual integration with other call routing devices such as SBCs or other PBX and trunking services is required.
   - If the HCS deployment mode is selected, the **HCS CUCM** must be selected.
   - **Network Addresses**:
     - The SERVICE_PROVIDER_SPACE IPv4 address is the address as viewed from Automate, so could be an address viewed through NAT.
     - The APPLICATION_SPACE IPv4 addresses is the local address of the Phone Server in the customer network.

       Both addresses are required, even where the address is the same as would be found if NAT was not in use to provide access from the service provider network.
   - **Virtual Machine**: name is optional and is used for administrator data purposes. It is not used by Automate.

2. Add country support.

   Country support must be added in HCS mode in order to integrate with the HCS dialplan. A template is required for each supported country. GBR and USA are provided by default, and other countries may be created or provided by VOSS as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

To add HCS country support, use the “phone server countries” menu item and select the template for the required country. There are no user parameters required.

3. Configure the physical phone

   In HCS mode, sites must be created with site dialplan and number inventory in the same way as when using Cisco Phones registered directly to CUCM. It is possible to host both CUCM and Phone Server phones at the same site.

   The phone itself requires configuration in order to register and handle calls.

   Soft clients will likely be manually configured locally on the hosting PC, and a “generic soft client” device type allows for locally configured devices.

   Other hardware devices such as phones from SNOM, Cisco and Grandstream may be configured using configuration files hosted on the VOSS phone server and downloaded at start up by the phone. TFTP is used to download these files. VOSS phone server hosts such files for fully automated configuration of the device.

Related topics

- *VOSS phones*
- *Add phone types* in the Core Feature Guide

Add phone types

New phone types (brands) can be created by creating a new phone type definition. This phone type defines the behavior of the Admin Portal when adding a phone, and defines sample configuration files and configuration templates to apply to this configuration file.

The sample file provides the layout of the phone configuration file but does not have values specific to each phone. Values such as the telephone number to apply are populated with a default value.

The configuration template allows access to any parameter in the sample file, and can be used to set the correct value for each phone, such as setting the telephone number. Automate ships with sample files and configuration for the SNOM D120 and D717 phones. This provides full configuration for these phones so that a new “out of the box” phone can be connected to the network and reach an operational state with no user intervention.

Adding a new phone type requires firstly creating a sample file. Many SNOM phones allow the export of the configuration which has been previously created through the phone web interface. This file can be used as the sample file, although values should be changed to make the file anonymous prior to uploading as a sample file. Once loaded, a configuration template can be created or cloned from the existing templates. This will allow modification of any value in the sample file, setting a value suitable for each phone. Using this technique, new phones types may be evaluated and added to Automate without the need for software updates or patches.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.3.11. Conferencing

Introduction to conferencing

Tip: *Use the Action search to navigate Automate*

Overview

Automate supports the following conferencing services:

- Webex
- Pexip (see *Pexip Conference Users*)
- Zoom

Site administrators manage the conferencing credentials of users if a Conferencing server is available at the site level. The Conferencing server on which users are administered can be identified with the Network Device Reference of the site, or else (according to the common reference resolution process) with the first such server in the current or higher up hierarchy level.

The default **Conferencing** page that provides the interface to Conferencing users displays the minimum of Conferencing user properties that are mandatory. The field display policies and configuration template for the **Conferencing** page can be modified according to the suggested customization procedure for policies and templates.

For Conference workflows to function, perform the following tasks at the Customer:

- Add a Conferencing server
- Add the Conferencing server to a Network Device List (NDL)
- Ensure the required site references the relevant NDL

Webex conferencing for users

If conferencing was added for a user when adding the user, the Webex ID defaults to the user ID. Note that the Webex user properties that are shown on the Users page may not correspond with those shown on the **Conferencing** page. If the Conferencing feature is to be added for an existing user, ensure that the Webex ID is the same as the user ID.

Conference workflows

Tip: *Use the Action search to navigate Automate*

User details can be added if a valid server is available.

When adding Conferencing from this input form, mandatory fields are entered on the Conferencing server.

Conferencing details can also be added as part of User Management.

Modify Conferencing details on the selected item, or also add and delete details from the User Management page.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Deleting a conference item removes details from the **Conferencing** tab of User Management.

Add a Pexip server

Tip: *Use the Action search to navigate Automate*

For an overview, see: *Pexip Conference Users*.

1. Log in as provider or reseller administrator.
2. Go to **Pexip Server**.
3. Click **Add**.
4. Complete, at minimum, the mandatory fields as in the field reference table.
5. Click **Save**.

Title	Field Type	Description
Server name*	name	The descriptive server name used to identify.
Description	description	Additional details to describe the server.
Host Name*	host	The host name or IP address of the server.
Version*	version	Version. Default: 1.0.0
User Name*	username	The administrator user name.
Password*	password	The password for the administrator.
Sync on Create/Update	sync	A full Pull Sync from the Pexip Server is run if enabled.

When a Pexip server is created, the following are also created:

- On the **Data Sync** menu:
  - A pull sync instance of data sync with the name format: *SyncPexip_<Pexip server name>*.
  - A purge sync instance of data sync with the name format: *PurgePexip_<Pexip server name>*.
- On the **Scheduling** menu:
  - An inactive schedule instance with the name format: *SchedulePexip_<Pexip server name>*.

    When the schedule is set to be active, it executes the *SyncPexip_<Pexip server name>* pull data sync.
- To test the connection to the Pexip server, choose **Test Connection** action on the menu.
- To modify the server, select it and update the fields as needed.
- To delete the server, select it from the list and then select **Delete**.

Virtual Meeting Rooms are set up as a part of User management - see:

- *Add a Pexip Virtual Meeting Room (VMR)*
- *Provision the Pexip Conference service*

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.3.12. AudioCodes

AudioCodes Devices

Overview

Tip: *Use the Action search to navigate Automate*

Administrators with the required permissions to the `relation/AudioCodesConnection` and `data/AudioCodes` models can add entries to menu layouts to expose these models and allow for the configuration of the device.

Add connection details

1. Go to the **Connection Details** page.

   Note: If the `relation/AudioCodesConnection` model is available, the **Connection Details** page form allows for the configuration of the AudioCodes device in VOSS Automate.

2. Add a descriptive **Name** for the connection.
3. Add connection details and credentials:
   - **Audio Codes Routing Manager**: IP address or a hostname
   - **Username** and **Password**: credentials for the routing manager host
   - **Authentication Method**: select the type of authentication to use with the host
4. Select **AudioCodes Connection sync on Create/Update** if an immediate data sync from the device is required.

Data syncs and schedules

When the connection details for the device is added, two default Data Sync instances and a Schedule also become available to be modified and enabled as required:

- **SyncAudioCodes__<connection-name>**
- **PurgeAudioCodes__<connection-name>**
- **ScheduleAudioCodes__<connection-name>**

The data sync workflows would then update internal number inventory entries for the **Vendor** field set as *AudioCodes* in accordance with updates to changes (add, delete, update) to AudioCodes **RegisteredUsers** (`device/audiocodes/RegisteredUsers`).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *AudioCodes device number integration*

6.4. Cisco CUC App Integration and Detailed Settings

6.4.1. Schedules

Tip: *Use the Action search to navigate Automate*

Configuring a CUC device on Automate creates a scheduled data sync to import model data from the device into Automate.

The scheduled data sync ensures that the VOSS Automate cache maintains the most current view of the configured device.

Note: If Holiday Schedules were added to CUC directly, update the default scheduled data sync instance to include the Model Type List called `CUCXN Schedules` in order to ensure that these holiday schedules are synced into VOSS Automate.

Any changes to the configuration occurring on the device, including additions, deletions, or modifications, reflect in VOSS Automate after the next data sync.

Note:

- There is no immediate data sync upon update or modification.
- Some license-related models will now be excluded from Cisco Unity Connection imports by default:
  - `device/cuc/Handler`
  - `device/cuc/GlobalUser`
  - `device/cuc/LicenseStatus`
  - `device/cuc/TenantUserLicense`
  - `device/cuc/UserLicense`

The recurring sync (disabled by default) is scheduled to occur every 14 days. You can enable the sync and modify the schedule the CUC **Schedules** page.

When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync.

You can manually run the data sync at any time, via the **Perform Publisher Actions** page or from the **Data Sync** page.

Important: Allow the initial data sync to complete before doing more configuration on Automate that requires information from CUC.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The performance of a data sync can be improved by controlling the types of data that are synced.

Related topics

- LDAP user sync in the Core Feature Guide.

6.4.2. Add greeting files

Tip: *Use the Action search to navigate Automate*

This option allows you to independently upload previously created greeting (.wav) files, which can be used when adding or updating call handlers at a hierarchy level.

Note: The Unity Connection server port that is used when uploading greeting files is the port specified during Unity Connection Publisher setup - see *CUC servers*.

1. Go to **Add Greeting Files**.
2. Click **Add**.
3. Click **Browse** to select the required greeting file from the directory in which it was saved.
4. Enter an optional description to uniquely identify the greeting file.
5. Click **Save**.

Uploaded greeting files are available to use on the **Record/Playback** and **Upload Greeting** tabs when you modify a call handler, see *Update a call handler*.

6.4.3. Call handler (auto attendant) schedule

Tip: *Use the Action search to navigate Automate*

Overview

Note: You can only manage schedules at the same hierarchy level (or lower) as your log in level. For example, if you login as a customer administrator, you can view schedules at your own customer hierarchy level, and add new schedules at (or below) your hierarchy level.

During initial installation, Automate imports two predefined schedules from Cisco Unity Connection. These are accessed via the **Schedule** page for CUC:

- **All Hours**
- **Weekdays**

Copyright © 2025 VisionOSS Limited. All rights reserved.

By default, the **All Hours** schedule is configured to be “active” 24 hours a day, 7 days a week, with no holidays. Routing rules that follow this schedule will always be active, and call handlers that use this schedule ‘as is’, will never use off hour transfer settings or play closed greetings.

The **Weekdays** schedule is configured to be active from 8 a.m. to 5 p.m. (in the time zone of the Cisco Unity Connection server) from Monday through Friday. It is also configured to observe any days and times that are set in the default Holidays schedule.

Note: By default the **Holidays** schedule is not configured for any days or times. — at a minimum you may want to add days and times to this holiday schedule when your organization will be closed.

Holidays

When a Holiday setting is in effect, holiday greetings are played (if enabled), and off hours transfer rules are observed. You can set up several years of holidays at a time. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.

Related topics

- *Add a call handler (auto attendant) schedule*
- *Update a call handler schedule*

Add a call handler (auto attendant) schedule

You may want to create a new schedule for your organization.

On the **Schedule** page (modify or add), take note of the following field:

Uses Holiday Schedule - If you want your schedule to recognize days that are included as holidays in a holiday schedule, then choose a holiday schedule from the **Uses Holiday Schedule** drop-down list. Any day included in the selected holiday schedule will be recognized as a holiday.

If you want to create a new holiday schedule:

1. Select the **Is Holiday** checkbox.
2. Click **Holiday Details +** enter the following fields:
    - **Name**
    - **Holiday Start Date**
    - **Holiday End Date**
    - **Start Time**
    - **End Time**.
3. Add more days to the holiday as required by clicking **+** next to the entered holiday, and entering new details in the fields.
4. Click **Save** when complete.

Note: Another method to create a new schedule is to:

1. Select an existing schedule from the **Schedule** list view.

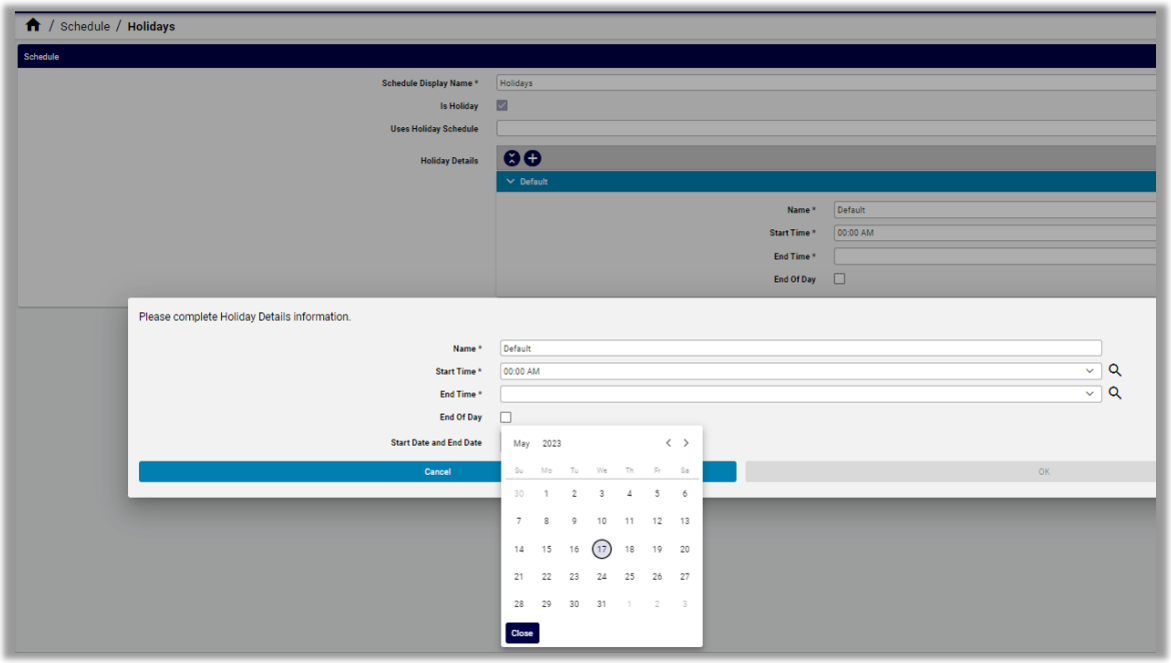
Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Clone it (**Action > Clone**) to the desired hierarchy level.
3. Edit as required.
4. Click **Save**.

Update a call handler schedule

1. In the Admin Portal, go to the CUC **Schedule** page.
2. In the **Schedule** list view, click on the schedule you wish to edit.
3. Update the relevant fields. See *Add a call handler (auto attendant) schedule*

   Note: If you're updating a *Holidays* schedule, click the Plus icon at **Holiday Details**, then fill out details for the holiday, including Name, Start Time, End Time, and select **End of Day** to define whether the schedule becomes inactive at midnight on the day of the holiday. Finally, click in the **Start Date and End Date** field to select a date for the holiday from the calendar date picker.



4. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete a call handler schedule

1. In the Admin Portal, go to the CUC **Schedule**.
2. In the **Schedule** list view, select the checkbox adjacent to the schedule you want to delete. If you want to delete more than one schedule, select multiple checkboxes.
3. Click the toolbar **Delete** icon.
4. In the dialog asking you to confirm the deletion, click **Yes**.

6.4.4. Language filters

Tip: *Use the Action search to navigate Automate*

Overview

Provider administrators or higher can manage multi-site, multi-country customers by setting geo-specific information using the Site Defaults Doc. Using this information, administrators can use custom Configuration Templates (as in the Quick Add Group for Quick Add User), to set this information on a per-site level.

Timezones and languages in Automate are populated with the required Cisco Unity Connection (CUC) timezones and languages. These are typically selected from the relevant drop-down lists as described under Modify Site Defaults.

Note: You must only add timezone and language codes in Automate that match the installed timezones and languages on the associated CUC Server. The names entered must uniquely describe the timezone and code.

Related topics

- *Timezone filters*

Add a language filter

To add a custom Cisco Unity Connection (CUC) language filter:

1. Log in as provider administrator or higher.
2. Go to **Language Filters** to see a list of language filters currently in Automate.
3. Click **Add**.
4. Configure the following:
   a. Mandatory. **Installed Language Code**. The value must match a language code installed on the associated Cisco Unity Connection Server.
   b. Mandatory. **Language Name**. The value must be a unique description for the language code.
5. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.4.5. Cisco CUC Detailed Configuration

CUC Servers and Nodes

CUC servers

Tip: *Use the Action search to navigate Automate*

Overview

Cisco Unity Connection (CUC) devices provide voicemail services and can be dedicated to a customer or shared across multiple customers.

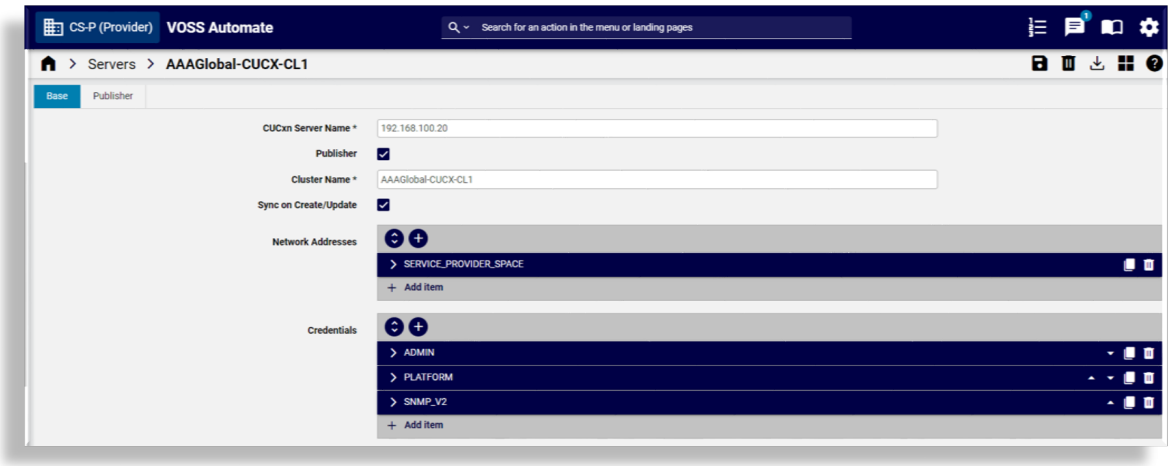
Dedicate a CUC to a single customer	Configure the CUC at the customer hierarchy node.
Share a CUC across multiple customers	Configure the CUC at a hierarchy node above the customer (reseller, provider, or intermediate node). The CUC device must be included in one or more Network Device Lists (NDLs), and the NDL must be assigned to one or more sites.

Add a CUC server

To add a CUC server:

1. Log in as the appropriate hierarchy administrator.
   - **Creating a shared instance**? Log in as provider or reseller admin.
   - **Creating a dedicated instance**? Log in as customer, provider, or reseller admin.
2. Choose the relevant hierarchy.
   - **Creating a shared instance**? Set the hierarchy to the provider or reseller level.
   - **Creating a dedicated instance**? Set the hierarchy to the customer level.
3. Go to the CUC **Servers** list view.
4. Click the Plus icon (+) to add a new server.
5. On the **Base** tab/panel, configure server details:

Copyright © 2025 VisionOSS Limited. All rights reserved.

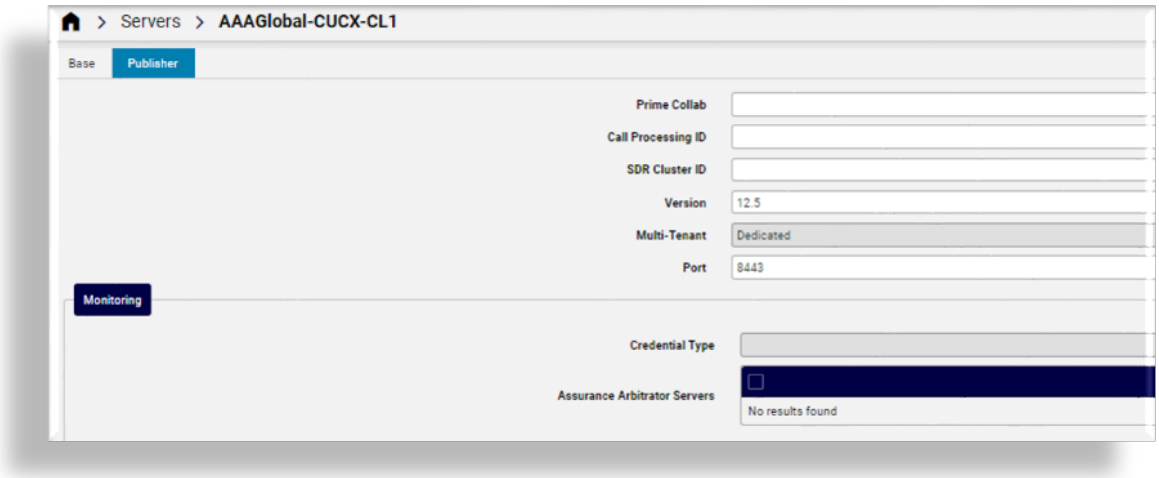


Field	Description
CUCxn Server Name	Mandatory. Fill out the Cisco Unity Connection (CUC) server name.
Publisher	Select this checkbox only if you're configuring a publisher node. **Note:** The **Publisher** tab/panel displays only when this checkbox is selected.
Cluster Name	Mandatory. Fill out the name you want to use for this cluster. The new cluster is created with this name. **Note:** If the **Publisher** checkbox is not selected, the **Cluster Name** field appears as a drop-down list so that you can choose an existing cluster.
Network Addresses	Expand this field, then: • At **Address Space**, select SERVICE_PROVIDER_SPACE. • At **IPV4 Address**, fill out the IP address of the CUC server. • The **Hostname** field is automatically populated with the CUC server name. Edit this value if necessary. **Note:** Either the hostname *or* the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Automate cannot validate an entry that contains a blank space at the end of the hostname or IP address. • At **Domain**, fill out the domain of the CUC application. • At **Description**, fill out a description for the network address. If NAT is used, also configure an APPLICATION_SPACE network address.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Credentials	Expand this field to add ADMIN credential type, fill out credential details. When done, add more credentials, if required. • Fill out the user ID and password that you configured when you installed the CUC. • Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO. • Optionally, provide a description for the credential. **Note:** • Automate uses ADMIN credentials to access the CUC REST API interface for provisioning synchronization. These credentials must be manually configured in Cisco Unity Connection, then configured in Automate, via the CUC **Servers** page, **Credentials** fields. • ADMIN is required for Service Inventory to generate reports for UC for UC applications.

6. Configure details for the **Publisher** tab/panel.



Note: This tab/panel displays *only* if you're configuring a publisher node and have selected the **Publisher** checkbox on the **Base** tab/panel.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Call Processing ID	The Call Processing ID of this cluster
SDR Cluster ID	The Shared Data Repository (SDR) CUC cluster ID.
Multi-Tenant	If creating at Provider level, this field is read-only and set to Shared. If creating at Customer level, you can choose between Dedicated and Partitioned.
Version	Select the version of Cisco Unity Connection Servers in this cluster.
Port	The port on the CUC server to connect to. The default is 8443.
Monitoring	For new servers and if Arbitrator servers are available, monitoring can be enabled for this CUC server on Insights. The Arbitrator server checkboxes can be selected to add the server as an asset. The Arbitrator server will be updated. Existing servers can be managed from the Onboard Assets and Offboard Assets menus under Insights. The Arbitrator checkboxes will then reflect the asset status.

Note: For more information around monitoring and Insights, see *Introduction to Insights monitoring*.

7. Save your changes.

Delete a CUC server

Deleting a Cisco Unity Connection (CUC) server in Automate also deletes local data that has been synced to it from the CUC server, including:

- Users
- Configuration parameters
- Dial Plan information (if applicable)

CUC Routing

Class of Service (User)

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Customer administrators and higher level administrators can create and maintain a Class of Service (CoS) that applies to users.

A CoS specifies the Cisco UCM and Calling Search Spaces (CSS) for a user's line, thereby indicating whether local, national, and international numbers can be called.

An administrator can create a CoS at a customer level hierarchy. A UCM is specified. A drop-down list of those available at the customer level is shown.

Optional device and line CSSs can also be added - either selected from those existing on the UCM, or else added. Macros can also be used when adding new CSSs, for example, `CSS-Gold-{{macro.SITENAME}}`.

When a CoS is modified, the UCM can't be modified. To refer to another UCM, either clone an existing CoS, else, delete it and re-add it.

Add a Class of Service (user)

1. Log in as a Customer administrator or higher.
2. Choose the relevant customer hierarchy.
3. Go to **Class of Service**.
4. Click **Add**.
5. From the **CUCM** drop-down, choose the relevant UCM.
6. Fill out a name for the CoS.
7. From the **Device CSS** and **Line CSS** drop-downs, choose the relevant CSS types to be associated to this CoS.

   Note: The value can also be a macro that evaluates to a valid CSS type that already exists on the selected UCM. Blank values are also allowed.

8. Save your changes.

   You can view transaction progress and details in the Transaction Logs (when adding, updating, or deleting a user's CoS).

Related Topics

- Transaction Logging and Audit in the Core Feature Guide
- Class of Service (Site) in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call handler

Tip: *Use the Action search to navigate Automate*

Overview

A Cisco Unified Communications Manager (Cisco UCM) auto-attendant call handler transfers incoming calls to the extension of a user or department without the intervention of an operator, via a system of voice menus that the caller interacts with, using their telephone keypad or voice commands.

Note: Auto-attendant is a comprehensive service that provides for the provisioning, configuration, and management of call handlers, greetings, schedules, and related dialplan components in Cisco Unity Connection (CUC) and Cisco UCM.

Some call handler systems are comprised of message-only information menus and voice menus, which allow organizations to provide business information such as hours, directions to their premises, or to answer other frequently-asked questions. Once the message plays, the caller can be forwarded to an operator, or they can choose to return to the main menu.

Call handlers can be created at the customer hierarchy or the site hierarchy in Automate:

Where created	Choosing a NDL
Created at customer	You must select a Network Device List (NDL), which then instructs the workflow which UC application servers to provision.
Created at site	The NDL associated to the site is chosen automatically.

Related topics

- Manage greeting files in the Core Feature Guide
- Call handler (auto-attendant) schedule in the Core Feature Guide
- Add a timezone filter in the Core Feature Guide
- *Number status and usage*
- See “System Call Handlers” in the “Cisco Unity Connection System Administration Guide for more information about Call Handlers.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call handlers and shared numbers

Automate allows you to share the same directory number (DN) between a call handler and one or more device types (phone, SNR, EM), provided you're using different line partitions between the call handler and the device types.

Note: SNR is short for "Single Number Reach" device. EM is short for "Extension Mobility" device. Device can include, for example, desk phone, BOT.

Shared number scenarios for call handler

Overview

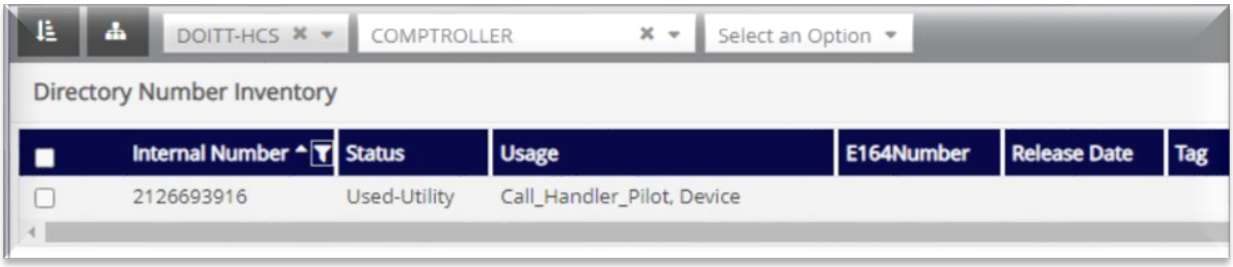
This section describes scenarios for number sharing between call handler and one or more device types and how this changes the status and usage values for the number in the number inventory.

The following scenarios are described:

- *Add devices to a number with an existing call handler*
- *Add a call handler to a number with existing devices*
- *Remove call handler from a number previously shared between call handler and devices*
- *Remove devices from a number previously shared between call handler and devices*

Note: Status defines whether the number is available to be assigned (or shared) between call handler and one or more devices. Usage value is added to the line details in the directory number inventory.

When adding a call handler, all numbers available for the call handler (whether shared or not) display in the **Pilot** drop-down. See *Manage auto-attendant and call handlers*



When a number is currently used exclusively by call handler (not shared with a device), the status and usage detail for that number is as follows:

Status	Usage
Used-Utility	Call_Handler_Pilot

When a number is currently used exclusively by a device (not shared with call handler), the status and usage detail for that number is as follows:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Status	Usage
Used	Device

Add devices to a number with an existing call handler

In this scenario, call handler is added first and is assigned to a number. Then you can add additional devices (e.g. desk phone, BOT, EM, SNR) with the same number.

Scenario	Before adding devices	After adding devices
Add devices to a number already assigned to call handler	• Status: “Used-Utility” • Usage: – “Call_Handler_Pilot”, or – “Call_Handler_Pilot, Device”	• Status: “Used” • Usage: “Call_Handler_Pilot,Device”

Add a call handler to a number with existing devices

In this scenario, one or more device types (device, EM, SNR) were added first to a number, then you add the same number to call handler.

Scenario	Before adding Call Handler	After adding Call Handler
Add call handler to a number already assigned to devices Scenario also applies if call handler was added with with a different number, then you change the call handler number to one that is used by devices.	• Status: “Used” • Usage: “Device”	• Status: “Used-Utility” • Usage: “Call_Handler_Pilot,Device”

Remove call handler from a number previously shared between call handler and devices

In this scenario, you have a number that is currently shared between call handler and one or more devices. Now you remove call handler from the number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Scenario	Existing Status / Usage	Updated Status / Usage
Where call handler was added first, and then devices were added. Now you delete the call handler or change the number it uses.	• Status: “Used” • Usage: “Call_Handler_Pilot,Device”	• Status: “Used” • Usage: “Device”
Where devices were added to a number first, and then call handler was added. Now you delete call handler or change the number it uses.	• Status: “Used-Utility” • Usage: “Call_Handler_Pilot,Device”	• Status: “Used” • Usage: “Device”

Remove devices from a number previously shared between call handler and devices

In this scenario, call handler was added first, then you added devices (one or more) to that number. Now you remove devices.

In this case, number status and usage depends on whether there was only one device and you remove it, or whether there are multiple devices, and you remove one device from the number shared with call handler.

Scenario	Existing Status / Usage	Updated Status / Usage
Call handler was added first. One device (e.g. a phone) shares a number with call handler. You delete that one device, or you update that device to remove the number (e.g. update phone to use a new line, or remove line from phone).	• Status: “Used” • Usage: “Call_Handler_Pilot,Device”	• Status: “Used-Utility” • Usage: “Call_Handler_Pilot”
Call handler was added first. Two or more devices are then added to the shared number (e.g. two phones using the same number). One device is deleted (e.g. delete phone), or you update one device to remove the number (e.g. update phone to use a new line, or remove line from phone).	• Status: “Used” • Usage: “Call_Handler_Pilot,Device”	• Status: “Used” • Usage: “Call_Handler_Pilot,Device”

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manage auto-attendant and call handlers

This section describes how to add, update, or delete an auto-attendant call handler in Automate and CUC.

Note: Some of the configuration parameters required to provision the call handler are defined via the configuration templates and are not exposed in the user interface. For example, the following settings are hardcoded in the **AddCucmRoutePatternForCallhandlerCFT** configuration template:

- Provide Outside Dial Tone = False
- Call Classification = OnNet

To change these settings or any other values defined via the configuration template, clone the template (via the **Configuration Templates** page) to the relevant hierarchy level, and edit the fields as required.

Add a call handler

This procedure adds a call handler.

Before you start:

- The relevant call handler template must have been synced in to Automate from CUC.

1. Log in to the Admin Portal as Provider, Reseller, or Customer administrator.
2. Choose the relevant hierarchy, either customer or site.
3. Go to **Add Cisco Auto Attendant**.

   Note: When adding a new record, only the **Call Handler Basics** tab displays until you fill out the basic details and save. Once you save, the other tabs display, where you can complete the configuration. See *Update a call handler*

4. Mandatory. At **Network Device List**, if you're at the customer level, select the network device list (NDL).

   Note: This field is auto-populated and read-only if you're adding the call handler at site level.

5. Mandatory. At **Name**, enter a name for the new call handler.
6. Mandatory. At **Call Handler Template**, choose the CUC call handler template. Options depend on the selected NDL.

   Note: For more information about the call handler template, see the "Call Handler Templates" section of the "Call Management" chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x.

7. At **Pilot**, choose a directory number to associate with the call handler.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: The drop-down displays the list of directory numbers available at the selected hierarchy. This can include numbers already assigned to one or more device types, since Automate allows sharing of numbers between call handler and multiple device types. See *Call handler*

8. At **Do not add Route Pattern** define whether to remove the mandatory requirement for adding a route list (if you've chosen a pilot).

   Note:

   - When enabled, (checkbox selected), choosing a route list (route pattern) is optional.
   - When disabled (default), choosing a route list (route pattern) is mandatory.

   This setting is relevant when adding or updating a Call Handler.

9. At **Route List**, choose a Cisco UCM route list for the new call handler.

   Note:

   - Optional when **Do not add Route Pattern** is enabled.
   - The NDL determines the route lists available in this drop-down. If the NDL is updated, route list options are updated.

10. Click **Save**.

    Note:

    - Adding a call handler through Automate also adds a route pattern on the Cisco UCM designated in the NDL (if **Do not add Route Pattern** is disabled, and you've chosen a route list and a pilot for the Call Handler). The pattern is the value of the pilot (directory number) you choose.
    - A configuration template (which can be cloned and modified) defines the rest of the pilot configuration (including partition).
    - A direct routing rule is also created on the CUC designated in the NDL. This rule accepts inbound calls into CUC, and routes them to the relevant call handler.

Update a call handler

To update a call handler:

1. Log in as Provider, Reseller, or Customer administrator.
2. Choose the relevant hierarchy.
3. Go to (CUC) **Call Handler**.
4. In the list view, click the relevant call handler to open the **Call Handler** page.
5. Click through the following tabs, and update settings as required:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Tab	Description
Call Handler Basics	Only this tab is enabled when adding a Call Handler. All tabs are available when updating a Call Handler. • **Do not add Route Pattern** (disabled by default) defines whether to remove the mandatory requirement for choosing a route list (if you've chosen a pilot). – When disabled, you must choose a route list if you've selected a pilot – When enabled, choosing a route list is hidden and no longer required (even if you've chosen a pilot) • **Call Handler Owner** - choose the CUC user to associate with the owner of the Call Handler.
Transfer Rules tab	Enables/disables transfer rules. • The **Standard** transfer rule can't be disabled. • By default, **Transfer Call To** is set to **Greeting**. When changing this setting to **Extension or URI**, you can specify an extension number or URI, and a transfer type (either *Release to Switch* or *Supervise Transfer*)
Caller Input tab	Configures the default caller. Additional settings become available as you choose options on this tab. For example, choosing **User with Mailbox** (from the **Action** drop-down in **Callhandler Menu Entry**) displays the **Transfer**/**Greeting** drop-down.
Greetings tab	Configures greeting settings.
Record/Playback tab	Configures the greeting you want to record and playback on the chosen extension. You can trigger a call to a physical device, which allows for recording or playback of a greeting. The extension to dial must be an accessible extension for the administrator (or user) to answer and record or listen to greetings • At **Extension**, choose an extension, or manually type in the number of the device you want to call to record or listen to a greeting. • To record or playback a greeting for a specific purpose, select the **Specific Greeting** checkbox; else, the action applies to the main Call Handler. • At **Duration (seconds)**, specify a time period (in seconds) that the system allows for recording a greeting. This time duration does not apply when playing back a recording. Ensure you set this timer appropriately. Setting it too low may result in an incorrect configuration. • Before saving the settings on this tab, go to **Record Greeting** or to **Playback Greeting** (as applicable) to record or playback the greeting you wish to use.
Upload Greeting tab	At **Greeting File**, choose the greeting file (.wav) to upload to the Call Handler. Then configure the specific greeting (if required).

6. Click **Save**.

   Changes are saved to the call handler in Automate and in Cisco Unity Connection (CUC).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete a call handler

To delete a call handler, click on the call handler you want to delete; then, click **Delete**. On the pop-up, click **Yes** to confirm.

If this call handler is using a number shared with one or more additional device types, see *Call handler* to understand how the status and usage description of the number may change when you delete the call handler.

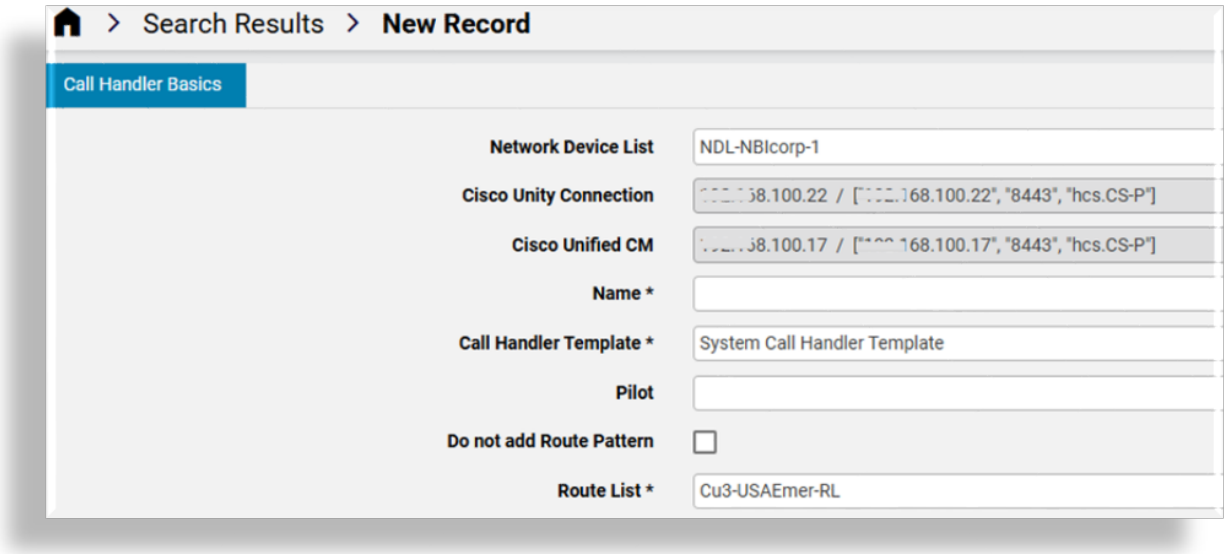
Call Handler settings

This section provides more information about the information required in the tabs and fields when adding or editing a Call Handler.

Call Handler Basics tab/panel

This tab configures base information for the call handler.

Note: When adding a call handler you'll need to fill out and save details on this tab before the other tabs display.



Copyright © 2025 VisionOSS Limited. All rights reserved.

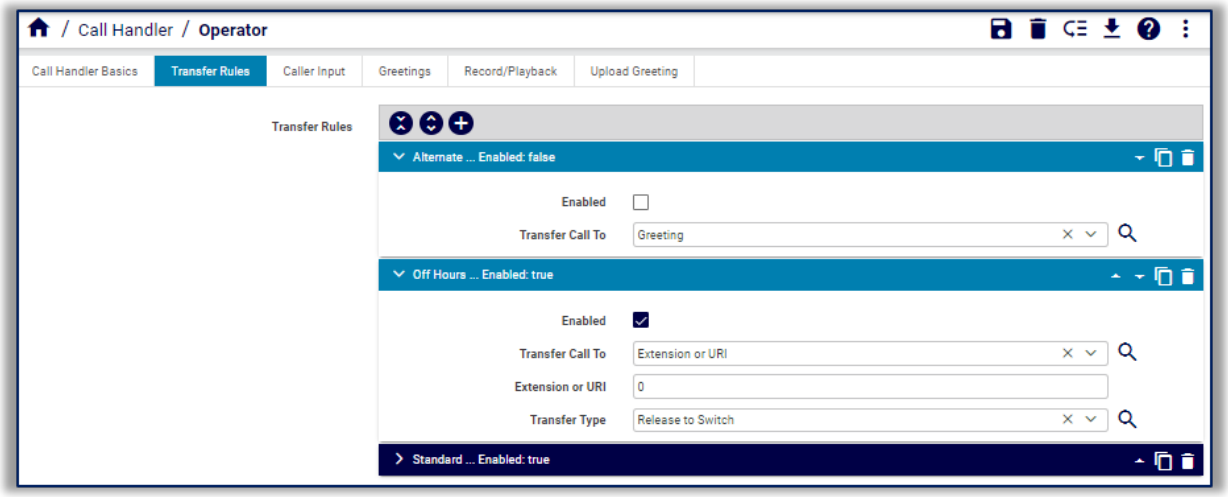
Title	Field Name	Description
Network Device List *	HF.target_ndl	Mandatory input-field for the **option** (if hierarchy is at Site-node, however, this value is derived automatically). The workflow (and GUIRules) will target the UC devices that is linked to this Network Device List (NDL). In the Mod use-case, this should also be derived automatically and can thus be omitted from Updates.
Cisco Unity Connection	HF.cuc_info	Informative (non-input) field. Indicates the target CUCx host/IP, which is automatically derived from the input NDL.
Cisco Unified CM	HF.cucm_info	Informative (non-input) field. Indicates the target CUCM host/IP, which is automatically derived from the input NDL.
Name *	DisplayName	The text name of the handler to be used when displaying entries in the administrative console, e.g. Cisco Unity Connection Administration. For example, the display name for the default opening greeting Call Handler is "Opening Greeting."
Route List	route_list	The CUCM Route List to use. The valid options are dependent on the selected NDL/CUCM. console, e.g. Cisco Unity Connection Administration. For example, the display name for the default opening greeting Call Handler is "Opening Greeting."
Pilot	DtmfAccessId	The DTMF access id (i.e., extension) for the call handler. The dialable number. When adding a call handler, all numbers available for the call handler (whether shared or not) display in the Pilot drop-down. Removing a pilot number from a call handler changes the number's status to *Available* in the Internal Number Inventory (INI).
Call Handler Template	cuc_template	Mandatory. The CUC call handler template for the call handler.

Note: If the pilot number is shared between the call handler and one or more additional device types, see *Call handler* to understand the status of numbers available to assign to the call handler.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Transfer Rules tab/panel

This tab configures transfer rules for the call handler, for example, the system behavior to transfer a call to an alternative number.



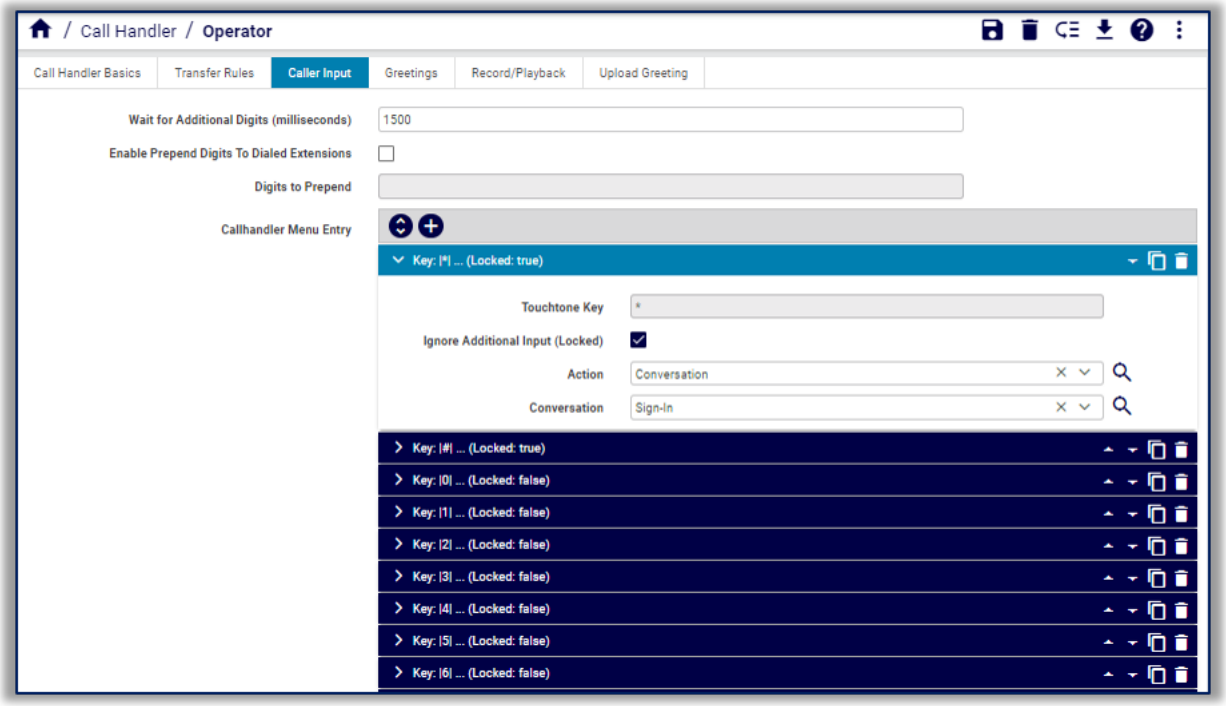
Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
Message	callerInput_tab_message	Caller Input
Callhandler Menu Entry	CallhandlerMenuEntry.[n]	
Touchtone Key	TouchtoneKey	The character on the touch-tone keypad that this menu entry corresponds to (* , #, 0,1. . . 9).
Ignore Additional Input (Locked)	Locked	A flag indicating whether Cisco Unity Connection ignores additional input after callers press this key. Values: 0: Additional input accepted 1: Additional input ignored; Cisco Unity Connection performs the action assigned to the key.
Call Action	Action	The type of call action to take, e.g., hang-up, goto another object, etc.
Extension or URI	TransferNumber	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Description	DisplayName	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Transfer Type	TransferType	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Rings to Wait for	TransferRings	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Target Conversation	TargetConversation	The name of the conversation to which the caller is routed.
Target Handler	TargetHandlerObjectId	The unique identifier of the specific object to send along to the target conversation.

Caller Input tab/panel

This tab defines the call handler behavior for caller input and navigation.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes fields on this tab:

Field	Description
Wait for Additional Digits (milliseconds)	The amount of time (in milliseconds) that Cisco Unity Connection (CUC) waits for additional input after a caller presses a single, unlocked key. If there's no input within this time, CUC performs the action assigned to the key.
Enable Prepend Digits to Dialed Extensions	Defines whether to prepend digits when dialing an extension number to transfer to.
Digits to Prepend	The touch-tone digits to prepend to the extension when dialing the transfer number.

Note: These fields are exposed automatically in the default FDP for relation/CallhandlerREL. If the FDP has been customized, you'll need to expose these fields manually by exposing the following field names: OneKeyDelay, EnablePrependDigits, PrependDigits

The table describes options in the **Call Handler Menu Entry** fieldsets:

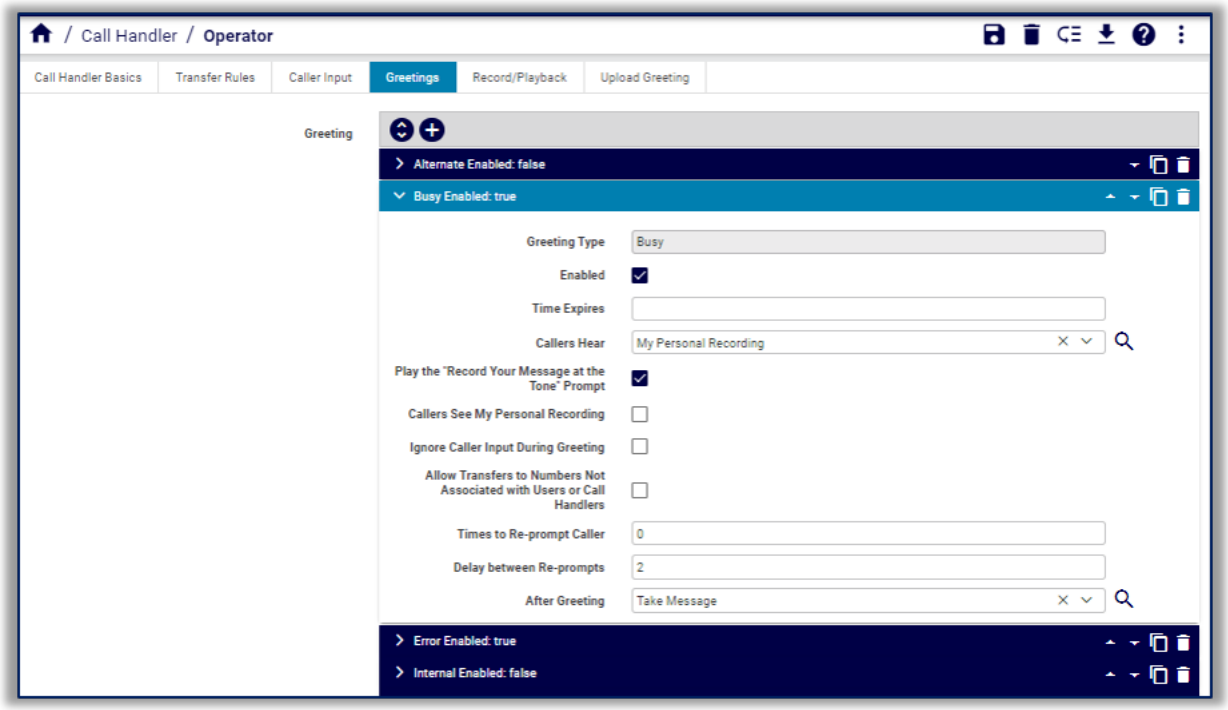
Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
Message	callerInput_tab_message	
Callhandler Menu Entry	CallhandlerMenuEntry.[n]	
Touchtone Key	TouchtoneKey	The character on the touch-tone keypad that this menu entry corresponds to (* , #, 0,1. . . 9).
Ignore Additional Input (Locked)	Locked	A flag indicating whether Cisco Unity Connection ignores additional input after callers press this key. Values: 0: Additional input accepted 1: Additional input ignored; Cisco Unity Connection performs the action assigned to the key.
Call Action	Action	The type of call action to take, e.g., hang-up, goto another object, etc.
Extension or URI	TransferNumber	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Description	DisplayName	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Transfer Type	TransferType	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Rings to Wait for	TransferRings	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Target Conversation	TargetConversation	The name of the conversation to which the caller is routed.
Target Handler	TargetHandlerObjectId	The unique identifier of the specific object to send along to the target conversation.

Greetings tab/panel

This tab configures the behavior and type of greetings enabled in the call handler.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.

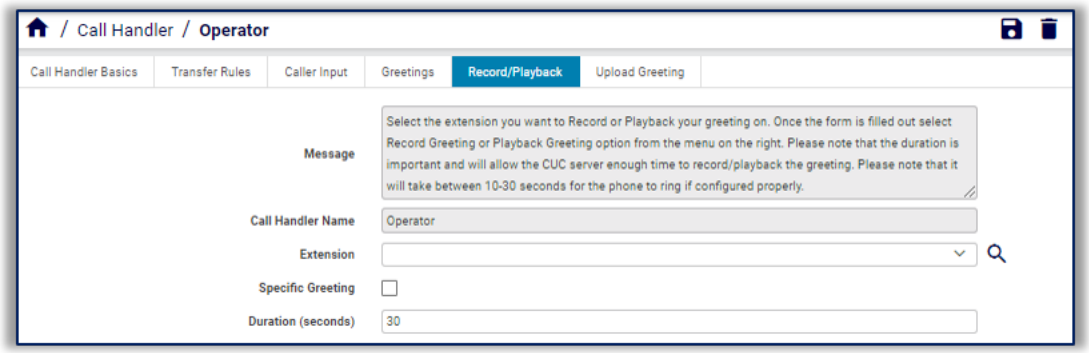
Title	Field Name	Description
Message	greetings_tab_message	
Greeting	Greeting.[n]	
Greeting Type	Enabled	The type of greeting, e.g. “Standard,” “Off Hours,” “Busy,” etc.
Enabled	Enabled	If TimeExpires is set, this field is ignored.
Time Expires	TimeExpires	The date and time when the greeting rule expires. The greeting rule is considered not expired (enabled), if the value is NULL or a future date. The greeting rule is considered expired (disabled), the value is in the past.
Callers Hear	PlayWhat	The source for the greeting when this greeting is active.
Play the “Record Your Message at the tone” Prompt	PlayRecordMessage Prompt	A flag indicating whether the “Record your message at the tone?” prompt prior to recording a message.
Callers See My Personal Recording	EnablePersonal Video-Recording	It will Enable the Personal video Recording in CUCA.
Callers See Play the “Record Your Message at the Tone” Prompt	PlayRecordVideo MessagePrompt	A flag indicating whether the “Record your message at the tone?” prompt prior to Video recording a message.
Ignore Caller Input During Greeting	IgnoreDigits	A flag indicating whether Cisco Unity Connection takes action in response to touchtone keys pressed by callers during the greeting.
Allow Transfers to Numbers Not Associated with Users or Call Handlers	EnableTransfer	A flag indicating when an extension is dialed at the greeting and the extension is not available whether to transfer to another extension.
Times to Re-prompt Caller	Reprompts	The number of times to reprompt a caller. After the number of times indicated here, Cisco Unity Connection performs the after-greeting action.
Delay between Re-prompts	RepromptDelay	The amount of time (in seconds) that Cisco Unity Connection waits without receiving any input from a caller before Cisco Unity Connection prompts the caller again.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
After Greeting	AfterGreetingAction	The type of call action to take, for example, hang-up, goto another object, etc.
After Greeting Target Conversation	AfterGreetingTarget Conversation	The name of the conversation to which the caller is routed.
After Greeting Target Handler Object Id	AfterGreetingTarget HandlerObjectId	The unique identifier of the specific object to send along to the target conversation.
Callhandler URI	CallhandlerURI	
Greeting Stream Files URI	GreetingStreamFilesURI	
Greetings Type	GreetingType	The type of greeting, e.g. “Standard,” “Off Hours,” “Busy,” etc.
URI	URI	

Record/Playback tab/panel

This tab configures message recording and playback for the call handler.

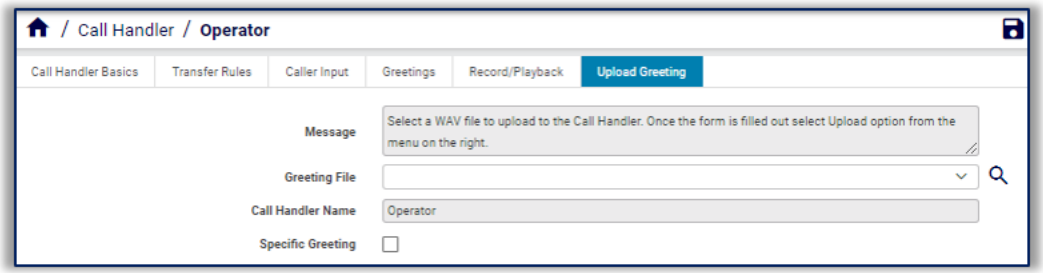


Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
Message	RecordPlayback.note	A special interface, which allows administrators to trigger a call to a physical device, which allows for recording or playback of a greeting. The extension to dial must be an accessible extension for the admin (or user) to answer and record or listen to greetings.
Call Handler Name	RecordPlay-back.call_handler	Call Handler Name.
Extension	RecordPlay-back.extension	Extension to Record message on.
Specific Greeting	RecordPlay-back.specific_greeting	The unique identifier of the Call Handler object to which this menu entry belongs.
Greetings	RecordPlayback.greeting	Greetings.
Duration	RecordPlayback.duration	Duration to allow enough time to make recording/playback.

Upload Greeting tab/panel

On this tab you can upload a greeting for the call handler.



Title	Field Name	Description
Message	note	Upload a greeting to the selected Call Handler.
Greeting File	Upload.filename	Call Handler Name.
Call Handler Name	Upload.call_handler	Call Handler Name.
Specific Greeting	Upload.specific_greeting	Specific Greeting.
Greetings	Upload.greeting	Greetings.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Cisco Unity SIP Integration

Introduction to Unity SIP integration

Overview

The Unity SIP integration tooling provisions complete SIP integration between redundantly deployed Cisco Call Managers (CUCM) and Cisco Unity Connection (CUC) servers. This integration tooling can be used to define the primary only integration that the legacy Voicemail Service provides.

The integration tooling provides a repeatable process to manage the integration of CUCM and CUC, while also providing the ability to:

- Define the dial plan used for integration so that the administrator deploying the integration does not need to have dial plan knowledge.
- Override the dial plan input mechanism mentioned above for advanced deployment.
- Deploy CUCM and CUC SIP integration in full redundancy supporting optional tenants.

Important: Contact your dedicated VOSS support representative for details on how to set up and configure the Unity SIP Integration feature.

Note: If this feature is not exposed in the Admin Portal menu layout, refer to “Unity SIP Integration - Menu Layout Changes and Access Profile Changes”.

Unity SIP integration scope

The Unity SIP integration tooling provides support for:

- Dual trunks to Unity publisher/subscriber
- Multiple SIP server destinations to CUCMs (SIP redundancy)
- Specifically defined number of Unity port build per Unity node
- Dynamic creation of CUCM route list/route group or the ability to update if they already exist
- Creation of Unity tenants for shared architectural deployments
- Creation of Unity integration utilizing tenants
- Support for multi-cluster deployments

Configure the Unity SIP Integration menu layout

Tip: *Use the Action search to navigate Automate*

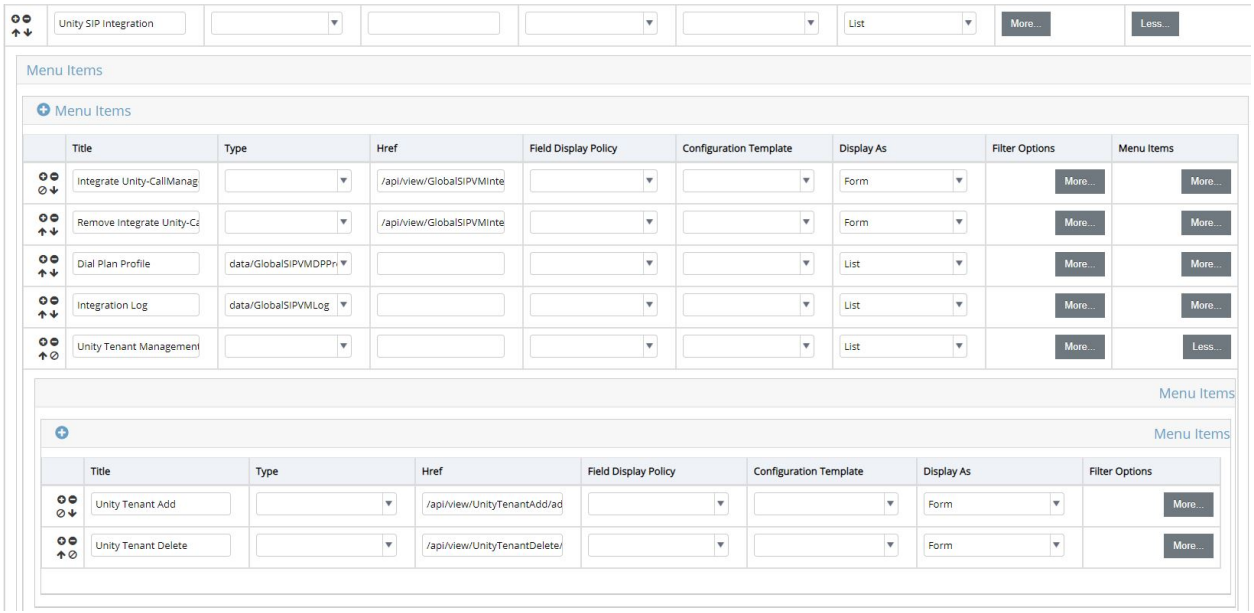
1. Log to Automate with sufficient rights to change menu layouts.
2. Go to **Menu Layouts**.
3. Select menu you wish to configure.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. Configure the menu layout as shown below under **Unity SIP Integration**.
5. Click **Save**.

Title	Type	Href	Display As
Unity SIP Integration			List
Integrate Unity-CallManager		/api/view/GlobalSIPVMIntegration/add	Form
Remove Integrate Unity-Call Manager		/api/view/GlobalSIPVMIntegrationDelete/add	Form
Dial Plan Profile	data/GlobalSIPVMDPProfile		List
Integration Log	data/GlobalSIPVMLog		List
Unity Tenant Management			List
• Unity Tenant Add		/api/view/UnityTenantAdd/add	Form
• Unity Tenant Delete		/api/view/UnityTenantDelete/add	Form

See also **Unity SIP Integration Menu Layout** illustration:



Copyright © 2025 VisionOSS Limited. All rights reserved.

Access profile changes

Tip: *Use the Action search to navigate Automate*

1. Log in to Automate as an administrator with sufficient rights to change access profiles.
2. Go to **Access Profiles**.
3. Select the required administrator name, for example ProviderAdminAP.
4. Configure the provider access profiles as shown in step 5.
5. Under **Type Specific Permissions** add the following new **Permitted Type** entries and **Permitted Operations**:
   - Permitted Type: view/UnityTenantAdd
   - Permitted Operations: Create
   - Permitted Type: view/UnityTenantDelete
   - Permitted Operations: Create
   - Permitted Type: view/GlobalSIPVMIntegration
   - Permitted Operations: Create, Field Display Policy, Read, Tag
   - Permitted Type: view/GlobalSIPVMIntegrationDelete
   - Permitted Operations: Create
   - Permitted Type: data/GlobalSIPVMDPProfile
   - Permitted Operations: Create, Delete, Read, Tag, Update
   - Permitted Type: data/GlobalSIPVMLog
   - Permitted Operations: Read, Tag
6. Click **Save**.

Unity SIP Integration

Tip: *Use the Action search to navigate Automate*

The Unity SIP Integration feature can be used in place of your existing voicemail service. A list of menus items is available to carry out the Unity SIP Integration tasks. Unity SIP Integration provides SIP integration for both CUCM and CUC.

A typical workflow would be that one or more integration dial plan profiles are set up for use, and then a SIP Unity Integration is pushed to CUCM and CUC.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Menu	Description
Integrate Unity-CallManager	The main tool used to push integration between CUCM and CUC.
Remove Integrate Unity- Call-Manager	This allows you to remove the complete integration out of the target CUCM and CUC.
Dial Plan Profile	This allows an advanced administrator to define all of the dial plan elements that make up the CUC integration, for example device pools, route group, route list, CSSs, and so on.
Integration Log	This log is populated with information about when the integration was pushed, as well as other details, so that it can be pulled back out again.
Unity Tenant Management	A “tenant” is basically a small voicemail setup for a sub-company within your larger Connection server. In other words if you had companies sharing a single connection server for voicemail services, you can set each one up as a separate “tenant” in your install which effectively isolates them from one another. Note that a Unity server containing user data without tenants cannot have tenants added after the fact.
Unity Tenant Add	This allows you to add a unity tenant to the Unity server.
Unity Tenant Delete	This allows you to remove a unity tenant from the Unity server.

Integrate Unity-Call Manager

Tip: *Use the Action search to navigate Automate*

Overview

Integrate Unity-Call Manager is the main tool used to push integration between CUCM and CUC, allowing you to create a SIP integration between Cisco Unified Call Manager (CUCM) and Cisco Unity Connection (CUC).

You can select the following tabs on the **Integrate Unity-CallManager** page:

- UC Publisher Application Selection
- Deployment Options
- CUCM Global
- Unity Port Group
- Unity Ports
- CUCM Voicemail Pilot
- CUCM Voicemail Profile
- CUCM Route List
- CUCM Route Group
- CUCM to CUC Publisher SIP Trunk

Copyright © 2025 VisionOSS Limited. All rights reserved.

- CUCM to CUC Subscriber SIP Trunk

Configure the Integrate Unity-CallManager

1. In the Automate Admin portal, go to **Integrate Unity-CallManager**.
2. Fill out the following fields to auto-populate initial key values:
   - On the **UC Publisher Application Selection** tab/panel:
     - Mandatory. Select an option at **Provisioning Target Call Manager**.
     - Mandatory. Select an option at **Provisioning Target Unity**.
   - On the **Deployment Options** tab/panel:
     - Mandatory. Select an option at **Voicemail Service Dial Plan Profile**.
3. Mandatory. On the **Deployment Options** tab/panel, fill out values for the following:
   - At **Dial Plan Advanced Mode**:
     - Select this checkbox to unlock the fields for dial plan elements. You then have the ability to update those values 'live'.
     - Clear this checkbox to return the dial plan elements to the default voicemail dial plan profile values.

     Note: You can choose to hide this checkbox from lower level administrators.

   - At **Provision CUCM-Unity in Redundant Mode**:
     - Clear this checkbox to allow this feature to function in single mode; that is, to operate in a similar way to the original voicemail service (Publisher only and no Subscriber trunk).
     - Select this checkbox to provision in redundant mode. In this mode, you can configure ports on both the Publisher and Subscriber Unity nodes, as well as build a trunk to both Publisher and Subscriber.

   Note: The **Unity Tenant(s) Present** checkbox is selected by default if the *Provisioning Target Unity* server you selected on the **UC Publisher Application Selection** tab/panel contains tenants.

4. View auto-populated settings on the **CUCM Global** tab/panel - these values auto-populate based on options selected for **Voicemail Service Dial Plan Profile** on the **Deployment** tab/panel:
   - The value for **SIP Profile**, which assigns the configured settings in this SIP profile to the associated device.
   - The value for **SIP Trunk Security Profile**, which assigns a single security profile to multiple SIP trunks in order to apply the configured settings to the SIP trunks.
5. Complete at minimum the mandatory values on the following tabs:
   - *Unity Port Group tab/panel*
   - *Unity Ports tab/panel*
   - *CUCM Voicemail Pilot tab/panel*
   - *CUCM Voicemail Profile tab/panel*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *CUCM Route List tab/panel*
- *CUCM Route Group tab/panel*
- *CUCM to CUC Publisher SIP Trunk tab/panel*
- *CUCM to CUC Subscriber SIP Trunk tab/panel*

Unity Port Group tab/panel

Complete, at minimum, the mandatory fields on this tab/panel:

- **Phone System** - Choose from the drop-down. The phone system settings identify the phone system with which Unity Connection integrates and regulate certain phone system features (integration configuration settings are located in the port groups that belong to the phone system.)
- **SIP Server Authentication Username** - Enter the user name that Unity Connection uses to authenticate with the SIP server (SIP integrations only).
- **SIP Server Authentication Password** - Enter the password that Unity Connection uses to authenticate with the SIP server (SIP integrations only.
- **Repeat SIP Server Authentication Password** - Repeat the SIP Server Authentication Password entered above.
- **SIP Security Profile (IP Port)** - Select the SIP security profile that Unity Connection uses. Default setting = 5060.
- **Primary CUCM IPv4 Address or Host Name** - Enter the IP address (or host name) of the PIMG/TIMG unit that the port group connects to.
- **Redundant SIP Servers**
  - **Call Manager Server IP or Host Name** -

Unity Ports tab/panel

Complete, at minimum, the mandatory fields on this tab/panel:

- **Publisher Server**

  This field is auto populated based on the **Provisioning Target Unity** chosen under **Deployment Options**.
- **Publisher Port Count**
- **Subscriber Server**
- **Subscriber Port Count**

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Voicemail Pilot tab/panel

Complete, at minimum, the mandatory fields on this tab/panel:

- **Pilot Number** - Enter a number to identify the voicemail pilot number.
- **Calling Search Space** - Enter an appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this pilot number.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Default Voice Mail Pilot for the System** - Select this check box if you want to replace the current default pilot number, and make this pilot number the default Voice Mail Pilot for the system.

CUCM Voicemail Profile tab/panel

Complete the following fields, as required:

- **Name** - Enter a name to identify the voicemail profile.
- **Description** - Enter the description of the profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (), angle brackets (<>), dollar sign ($), single-quote(‘), open parenthesis [(], close parenthesis [)], slash (/), colon (:), semi-colon (;), equal sign (=), at sign (@), tilde (~), brackets ({ }), or apostrophe (‘).
- **Pilot** - Choose the appropriate voicemail pilot number that is defined in the Voice Mail Pilot Configuration or Use **Default**. This field is auto populated based on the **Pilot Number** entered under **CUCM Voicemail Pilot**.
- **Voice Mail Box Mask** - Specify the mask that is used to format the voice mail box number for auto-registered phones. When a call is forwarded to a voice-messaging system from a directory line on an auto-registered phone, CUCM applies this mask to the number that is configured in the Voice Mail Box field for that directory line.
- **Make this the default Voice Mail Profile for the System** - Select this check box to replace your current default profile, and make this the default profile name.

CUCM Route List tab/panel

Complete the following fields as required:

- **Name** - Enter a name for this route list. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Run On All Active Unified CM Nodes** - Select this check box to enable the active route list to run on every node.
- **Call Manager Group** - Choose a CUCM group. The route list registers with the first CUCM in the group, which is its primary Cisco Unified CM.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Route Group tab/panel

Complete the following fields as required:

- **Name** - Enter a name for this route group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.

- **Distribution Algorithm** - Choose a distribution algorithm from the drop-down:
  - **Top Down** - If you choose this distribution algorithm, CUCM distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member.
  - **Circular** - If you choose this distribution algorithm, CUCM distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which CUCM most recently extended a call. If the nth member is the last member of a route group, CUCM distributes a call starting from the top of the route group.

  Default = Circular.

CUCM to CUC Publisher SIP Trunk tab/panel

Complete, at minimum, the mandatory fields on this tab/panel:

- **Device Name** - Enter a device name.
- **Trunk Device Pool** - This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Destination IP Address** - Choose from the drop-down list.

CUCM to CUC Subscriber SIP Trunk tab/panel

Complete, at minimum, the mandatory fields on this tab/panel:

Note: This tab displays only if you've selected the **Provision CUCM-Unity in Redundant Mode** checkbox on the **Deployment Options** tab/panel.

- **Device Name** - Enter a unique device name.
- **Trunk Device Pool** - This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Destination IP Address** - Choose from the drop-down list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add or delete a Unity tenant

Tip: *Use the Action search to navigate Automate*

Overview

The ability to add or delete Unity tenants assists in creating groups of objects in Unity Connection that provide a basic “tenant services” application. It allows you to create a tenant, which includes numerous interrelated database objects in Connection that work together to provide basic directory segmentation features to allow for isolated groups of users and handlers within your Connection server.

Add a Unity tenant

Note: The description, alias and SMTP Domain name must all be unique among tenants in your system.

1. Go to **Unity Tenant Add**.
2. Complete, at minimum, the following mandatory fields:
   - **Target Unity Server**
   - **Unity Tenant Name (Alias)** - the alias is used as a prefix for all objects created in the tenant; used to ensure all objects in Connection are uniquely named
   - **SMTP Domain** - a unique SMTP domain name
   - **Tenant Description**
3. Save your changes.

Delete a Unity tenant

Note: When deleting a tenant, ALL OBJECTS associated with that tenant are deleted as well. This means all users, call handlers, interviewers, schedules, COS etc. are deleted. There is NO UNDO for this. Make sure you really want to remove a tenant and all its objects before doing so.

1. Go to **Unity Tenant Delete**.
2. At **Unity Tenant Name (Alias)**, select the tenant to delete.
3. Click **Save** to remove the tenant.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial plan profile

Tip: *Use the Action search to navigate Automate*

On the **Dial Plan Profile** page, an advanced administrator can define all of the dial plan elements that make up the CUC integration.

Note: You can only add a SIP integration once a dial plan profile is configured.

You will need to complete at least the following mandatory fields:

- Profile Name
- SIP Profile
- SIP Trunk Security Profile
- Device Pool
- Route Group
- Route List
- SIP Trunk Inbound CSS
- Call Manager Group
- Voicemail Pilot CSS

You can configure details on this page with static (exact) values if you wish to deploy these same values over and over at store level. Typically, this option is not used.

At the Provider hierarchy, macros are used to make the profile portable across several customers. For example, if you had two or three different versions of dial plans, then you would have two or three versions of this profile. The lower level administrators could then apply the profiles as required.

Integration log

Tip: *Use the Action search to navigate Automate*

On the **Integration Log** page you can view all details relevant to the SIP integration, including when the integration was pushed, and other details so that the integration can be pushed back out again, if required.

Remove Integrate Unity-CallManager

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

The *Remove Integrate Unity-CallManager* tool takes the complete selected SIP integration back out of the Cisco Unified Call Manager (CUCM) and Cisco Unity Connection (CUC).

Remove an integration

1. Go to **Remove Integrate Unity-CallManager**.
2. At **Integration Label**, select the integration that you want to remove.
3. Save your changes.

Cisco Voicemail Services

Voice mail services

Tip: *Use the Action search to navigate Automate*

Add voice mail service

This procedure adds a voice mail service, associates the service with a Cisco Unity Connection (CUC) server, and integrates it with a Cisco Unified Communications Manager (UCM) and/or Cisco Webex DI (Dedicated Instance).

Prerequisites

- To associate the voice mail service with a UCM, ensure you know the SIP trunking endpoint information between the voice mail server and the UCM.
- A CUC server must be configured.

Perform these steps:

1. Log in as provider or reseller administrator.
2. Set the hierarchy to the correct provider or reseller node.

   Note: The voice mail service is always added above the customer level, so either at provider level or reseller level, and is associated to the customer.

   ---

3. Go to **Voice Mail Service**.
4. Click the Plus icon (+) to add a voice mail service.
5. On the **New Record** page, fill out details for the new voice mail service:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Voice Mail Service Name	The voice mail service name. Ensure there are no spaces in the name.
Cisco Unity Connection Cluster	Mandatory. The name of the CUC server for the voice mail service. **Note:** • The CUC server must have been added at the Provider level. • This is also where the voice mail server in a multi-tenant environment is categorized as *Dedicated* or *Partitioned*, which defines the elements available to the voice mail server, for example, whether another tenant should be created on the voice mail server.
Integrate with Cisco Unified CM	Defines whether to integrate the voice mail service with UCM (UCM will manage the voice mail service). The default is False (unchecked). When choosing **Integrate with Cisco Unified CM**, the **Cisco Unified CM Cluster** drop-down displays.
Cisco Unified CM Cluster	The UCM cluster associated with the voice mail service. This drop-down displays only if you've selected **Integrate with Cisco Unified CM**. From this drop-down, select the UCM to be paired with the CUC server. **Note:** The UCM must have been added and configured at the Provider level (via the **CUCM** page).
Integrate with Cisco Unified CM Webex DI	Defines whether to integrate a voice mail Webex Dedicated Instance with UCM. When choosing **Integrate with Cisco Unified CM Webex DI**, the rest of the fields on this form are hidden, and the the **Voice Mail Trunk Address** drop-down displays. In a UCM Webex DI environment, the routing rules in the Automate provisioning workflow uses the calling search space (CSS) for Webex DI to allow for adding multiple voice mail services for Webex DI.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Voice Mail Trunk Address	This drop-down displays only if you've selected the **Integrate with Cisco Unified CM Webex DI** checkbox. The drop-down displays available existing entries on the selected UCM cluster, which will be associated with the Route Group as a part of the Route List and Route Group provisioning.
Cisco Unity Connection Server Address	The hostname or IP address of the voice mail server. This field is hidden on the form if you've selected **Integrate with Cisco Unified CM Webex DI**. This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).
Cisco Unity Connection Server Port	The voice mail server port number (1 to 65535). **Note:** Do not use port 5061, which is reserved for secure SIP. This field is hidden on the form if you've selected **Integrate with Cisco Unified CM Webex DI**. This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).
Cisco Unified CM Server Address	The hostname or IP address for the voice mail server to reach the UCM. This field is hidden on the form if you've selected **Integrate with Cisco Unified CM Webex DI**. This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).
Cisco Unified CM Server Port	The UCM port number. **Note:** • Do not use port 5061, which is reserved for secure SIP. • Only one UCM and one CUC can be specified here. To support redundancy and failover in a multinode configuration, the trunk information must be manually updated on the UC apps. This field is hidden on the form if you've selected **Integrate with Cisco Unified CM Webex DI**. This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Voice Messaging Ports	Mandatory. Fill out the number of voice messaging ports to be created for the voice mail service and associated with the appropriate Port Group on CUC when the voice mail service is associated to a customer. Valid values are 1 - 250. The default = 3. **Note:** The number of voice messaging ports you add can't bring the total number of voice messaging ports for all port groups to more than the maximum number of voice messaging ports that are enabled by the CUC license files. If the license files don't enable the total number of ports, you won't be able to add the new ports. This field is hidden on the form if you've selected **Integrate with Cisco Unified CM Webex DI**. This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).

6. Save your changes to add the new voice mail service.

   Once a shared voice mail service is created, if you have enabled **Integrate with Cisco Unified CM**:

   - In UCM, cluster-level SIP trunk and route group is provisioned for the shared voice mail service.
   - In CUC, cluster-level port group appears on the PhoneSystem for the shared voice mail service.

Next steps

- *Associate or disassociate voice mail services to a customer*

Delete voice mail service

1. Log in to the Automate Admin Portal as Provider administrator.
2. Go to **Voice Mail Service**.
3. From the list of voice mail services, select the checkbox for the voice mail service you want to remove.
4. Click **Delete**, then click **Yes** to confirm.

   Once the transaction completes, the voice mail service is removed from the list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Pilot numbers

Tip: *Use the Action search to navigate Automate*

Add a pilot number

This procedure creates one or more voicemail pilot numbers for voicemail services that have previously been associated with the customer.

Prerequisites:

- Create the voicemail service.
- Associate voicemail service with the customer.

Note: In Automate, you can select the voice mail pilot number from a list of available DN inventory.

Perform these steps:

1. Log in as provider or customer administrator.
2. Set the hierarchy to the customer or site that you are defining a Voice Mail Pilot Number for.
3. Go to the CUC **Pilot Numbers** page.
4. Click **Add** to associate a pilot number with the voice mail service that has been associated with the customer.
5. From the **Voice Mail Service** drop-down, select the appropriate Voice Mail Service from the list of Voice Mail Services associated with the customer.
6. From the **Voice Mail Pilot Number** drop-down, select a Pilot Number from the list of your available DN inventory, or type the Pilot Number you want to use in the field. This is the internal Voice Mail Pilot Number that can be dialed from site.

   Note: You can add one or more pilot numbers for a single voice mail service.

7. Click **Save** to create the pilot number.

   The Pilot Number appears in the list. When a Pilot Number is created for a Voice Mail Service and the **Integrated with CUCM** checkbox was selected for the Voice Mail Service, the following is provisioned based on the deployment mode of the Voice Mail server:

Voice Mail Deployment Mode	Cisco Unified Communications Manager
Dedicated	At customer level: Route List, Route Pattern, CSS, Voice Mail Pilot, Voice Mail Profile
Partitioned	At customer level: Route List, Route Pattern, CSS, Voice Mail Pilot, Voice Mail Profile

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete a voicemail pilot number

1. Log in as the Customer Administrator. For a list of the roles and tasks that can be done at each level, see *Dial plan roles and privileges*.
2. Go to the CUC **Pilot Numbers** page.
3. From the **Pilot Numbers** list view, select the number to be deleted.
4. Click **Delete** to delete the Voice Mail Pilot Number.
5. From the popup window, click **Yes** to confirm the deletion.

   When the delete action is complete, the Voice Mail Pilot Number disappears from the list.

Associate or disassociate voice mail services to a customer

Tip: *Use the Action search to navigate Automate*

Associate voice mail services to customer

Prerequisites

- Create the voice mail service. See *Voice mail services*.
- If you've selected the **Integrate with Cisco Unified CM** checkbox when creating the voice mail service, create a customer dial plan and a site dial plan before attempting to associate the voice mail service with the customer, else, the association will fail.

Note: If you've selected the **Integrate with Cisco Unified CM Webex DI** checkbox when creating the voice mail service, the selected **Cisco Unified CM Cluster** provides the **Voice Mail Trunk Address** selection.

Perform these steps:

1. Log in as provider or reseller administrator.
2. Set the hierarchy path to the customer where you want to associate the voice mail service.
3. Go to the **Associate Voice Mail Service to Customer** page.
4. Click **Add** to associate voice mail service to the customer.
5. From the **Voice Mail Service** drop-down, choose the name of the voice mail service that has been defined by the provider and available to this customer.
6. Click **Save**. The voice mail service is now associated with this customer and appears in the list.
   - When the voice mail service is associated with a customer and the **Integrate with Cisco Unified CM** checkbox was selected for the voice mail service, the following is provisioned based on the deployment mode of the voice mail server:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Voice Mail Deployment Mode	Cisco Unified Communications Manager	Cisco Unity Connection
Dedicated	Creates integration at customer level: SipTrunk, Route Group, AllowVm route partition	Creates customer-specific Port Group, ports (3), route partition, calling search space and user template
Partitioned	Creates integration at customer level: SipTrunk, Route Group, AllowVm route partition	Creates new tenant (partition), port group, ports (3), route partition, calling search space and user template

Note: The deployment mode for the voice mail service is determined by the mode selected when the Cisco Unity Connection is first added to Automate via the **CUC** page.

- When the **Integrate with Cisco Unified CM Webex DI** checkbox was selected for the voice mail service, the **Voice Mail Trunk Address** selected from the selected **Cisco Unified CM Cluster** - is associated with the route group as a part of the route list and route group provisioning.

Disassociate voice mail services from customers

1. Log in as the Provider Administrator.
2. Set the hierarchy path to the customer from which you want to disassociate the Voice Mail Service.
3. Go to **Associate Voice Mail Service to Customer**.
4. From the list of associations, choose the Voice Mail Service customer association to be disassociated, by clicking the check box in the leftmost column.
5. Click **Delete** to disassociate the Voice Mail Service from the customer.
6. From the popup window, click **Yes** to confirm the change. When the delete action is complete, the Voice Mail Service association to the customer disappears from the list.

Associate or disassociate pilot number and site

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Associate pilot number to site

This procedure associates an existing voicemail pilot number to a site.

Prerequisites

- Add the voicemail pilot number. See *Pilot numbers*

> **Note:** In Automate, the event related to SIP Local Gateway may be generated as a result. Also you can select an E164 number to associate with the Pilot Number.

Perform these steps:

1. Log in as a Customer or Provider administrator.
2. Set the hierarchy to the relevant site.
3. Go to **Associate Pilot Number to Site**.
4. Click the Plus icon (+) to add the pilot number to site association.
5. At **Voice Mail Service** (mandatory), choose the voicemail service to associate with the site.
6. At **Voice Mail Service Pilot Number** (mandatory), choose the pilot number for the voicemail service you selected.
7. At **E164 Number** (optional), choose a E164 number from your site's inventory to associate with the pilot number, or type the E164 number you want to use.

   > **Note:** You must choose (or specify) an available E164 number. The transaction will fail if you choose an E164 number that is already assigned.

8. Click **Save**.

   The voicemail service pilot number is associated with the site:

   - The association appears in the list. When a pilot number is associated to a site, **CUC Defaults** are updated so that the user management templates can take advantage of this new voicemail service for the site.
   - If the site has one or more SIP Local Gateways associated with it and an E164 number has been specified, the `HcsSipLocalGwAddVoiceMailPilotNumberEVT` is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Disassociate pilot number from a site

> **Note:** In Automate, the event related to SIP Local Gateway is generated as a result.

Perform these steps:

1. Log in as the Customer administrator. For a list of the roles and tasks that can be done at each level, see *Dial plan roles and privileges*.
2. Go to **Associate Pilot Number to Site**.
3. From the list of associations, select the pilot number association to be disassociated.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. Click **Delete** to disassociate the Pilot Number from the site.
5. From the popup window, click **Yes** to confirm the change.
   - When the delete action is complete, the Pilot Number association to the site disappears from the list.
   - If the site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwDelVoiceMailPilotNumberEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Cisco Unity Connection Localization

Timezone filters

Tip: *Use the Action search to navigate Automate*

Add a Timezone filter

To add a custom Cisco Unity Connection timezone filter:

1. Log in as provider administrator or higher.
2. Go to **TimeZone Filters** to view a list of timezone filters currently in VOSS Automate.
3. Click **Add**.
4. Configure the following:
   a. TimeZone Code. Mandatory. The value must match a timezone code installed on the associated Cisco Unity Connection (CUC) server.
   b. TimeZone Name. Mandatory. The value must be a unique description for the timezone code above.
5. Click **Save**.

6.5. Additional Apps - App Integration and Detailed Settings

6.5.1. LDAP Server Settings

Setup LDAP server integration for sync and/or authentication.

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP server

Tip: *Use the Action search to navigate Automate*

Add LDAP server

This procedure adds and configures the LDAP server for integration with Automate.

Note: When integrating with a eDirectory LDAP server, OpenLDAP configuration options are followed, except for the primary key configuration options.

1. Log in as Provider, Reseller, or Customer administrator.
2. Set the hierarchy node to the node where you want to sync in users from LDAP to Automate.
3. Go to **LDAP Server**.
4. Click **Add**.
5. Configure the LDAP server. See *LDAP server configuration settings* for details.
   - Fill out the fields on the **Base** tab/panel.
   - Optionally, on the **Sync List** tab/panel, if you choose LDAP sync list option *Create sync list from template*, you can choose a LDAP sync list template (based on the server type) - either of these:
     - Ldap Sync List Microsoft Active Directory
     - Ldap Sync List Open Ldap

     You can choose a template when adding the LDAP server, or update your choice after saving. If you don't choose a template, LDAP sync is not affected by this list. See the tab description, and:
     - *LDAP user sync*
     - *LDAP schedule*
6. Click **Save**.
7. Test the connection to the LDAP server.

   If the authentication credentials or search base DN are invalid, the system displays an error, for example:

   Error encountered while processing your request

   caught exception: [Helper] validation failed; Invalid search base db.

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP server configuration settings

This topic is a field reference guide for the fields on the **LDAP Server** when adding or updating an LDAP server.

You can select the following tabs on the **LDAP Server** page:

Note: Use the toolbar tab/panel button to toggle between displaying these fields in tabs or panels.

- Base
- Sync List

Base tab/panel

Field	Description
Description	Defaults to the current hierarchy level.
Host Name *	Mandatory. Hostname or IP address of the LDAP server.
Port	Port number for LDAP traffic. Defaults to 389.
User DN *	Mandatory. The User Distinguished Name of an admin user that has access rights to the Base DN on the LDAP server. Examples: • Administrator@stb.com • OU=LDAP0,DC=stb,DC=com
Admin Password *	Mandatory. Admin password associated with the user.
Search Base DN *	Mandatory. Base Distinguished Name for LDAP search. This should be a container or directory on the LDAP server where the LDAP users exist, such as an Organization Unit (OU). For example, to search within an OU called CUS01 under a domain called GCLAB.COM, the Search Base DN would be OU=CUS01,DC=GCLAB,DC=COM. Note that the search will traverse the directory tree from this point down and will include any sub OU's which have been added within the OU.
Search Filter	An RFC 2254 conformant string used to restrict the results returned by list operations on the LDAP server.
Server Type *	Either **Microsoft Active Directory** or **OpenLDAP**. For AD LDS (ADAM), choose **Microsoft Active Directory**.
AD Sync Mode *	Defaults to Direct.
Enable Write Operations	This check box is only shown for Microsoft Active Directory servers (**Server Type** is **Microsoft Active Directory**) when **Encryption Method** is "Use SSL Encryption (ldaps://)" (port is `636`). When enabled, Automate user management allows for the management of users on the LDAP server (add, modify, delete).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
CUCM LDAP Directory Name	Optional. The name of the LDAP Directory configured on CUCM that we want this user to be considered synced from. The LDAP Directory must be configured on CUCM already. While this parameter is optional, note the following when this parameter is *not* set: • In a top-down scenario, users are added to CUCM as Local Users • In a bottom-up sync scenario, users won't be able to log on to Automate
Encryption Method	Choose between **No Encryption**, **Use SSL Encryption (ldaps://)**, or **Use StartTLS Extension**. • No Encryption - default port for LDAP is port 389 • Use SSL Encryption (ldaps://)a - uses port 636 and establishes TLS/SSL upon connecting with a client. • Use StartTLS Extension - to transition to a TLS connection after connecting on port 389
Server Root Certificate	If **Trust All** is unchecked, the LDAP server's SSL certificate is validated against this root certificate. If no **Server Root Certificate** is specified, validation is done against any existing trusted CA certificates. Use this option for custom root certificates in *.pem* format. See "SSO Certificate Management" for more information.
Trust All	Defines whether to disable certificate validation.
Primary Key Attribute	The attribute value used to uniquely identify and search for records on an LDAP server. For example, `uid` is the attribute when using a 389-Directory Server and `entryUUID` when using an OpenLDAP server. The attribute must be unique, should not change over time and should not be location specific. If no attribute is entered, `entryUUID` is used for an OpenLDAP server and `ObjectGUID` if the LDAP server is Microsoft Active Directory. **Note:** From v21.4-PB5, Automate introduced support for syncs from an eDirectory LDAP server configured as an OpenLDAP server type, and allows the use of an OctetString-formatted `GUID` primary key (pk) instead of the `entryUUID` attribute.
Authentication Scope	Hierarchical scope this server applies to: Local authentication or Full tree authentication.[1]
User sync type	Choose the type of users that can authenticate against this server - options are: • All users - all users can authenticate against this server • Synced users only (default) - only users synced in from LDAP can authenticate against this server
Authentication enabled	Defines whether the server is available for authentication. Default is True.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Search Filter examples:

- `(telephoneNumber=919*)`: all telephone numbers starting with 919
- `((&(OfficeLocations=RTP)(|(department=Engineering)(department=Marketing)))`: office is located in RTP and department is either Engineering or Marketing
- `(&(MemberOf=cn=Admin,ou=users,dc=foo,dc=com)(!(c=US)))`: all Admins except those in the U.S.

User lookup for LDAP authentication is restricted to the `device/ldap` model specified in the **Authentication Attribute**: **Model Type**. For example, if this attribute was `device/ldap/user`, the LDAP user authentication is restricted to `(objectClass=user)`.

Related Topics

Sync List tab/panel

A sync list improves performance, and limits sync attributes to those relevant to your scenario.

On this tab you can choose a LDAP sync list option, when adding a new LDAP server or when updating an existing LDAP server (one that was added prior to release 19.3.4).

Important: The following attributes are always synced in, regardless of the sync list option you choose:

- sAMAccountName
- userPrincipalName
- mail
- cn
- uid
- description

The table describes the LDAP sync list options you can choose on this tab:

[1] For details around authentication scope, see *User login options by auth method and server auth scope*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP Sync List Option	Description
No sync list - all fields will be synced	LDAP sync is not driven by a LDAP sync list. All fields are imported (as they were before release 19.3.4).
Create sync list manually	The fields to sync can be added or modified manually. For list override precedence and other considerations, see *LDAP sync lists*.
Create sync list from template	Displays an additional field on the tab (LDAP Sync List Template) and allows you to choose a sync list from a predefined configuration template (CFT). Automate provides default Sync List CFTs for the following: • Microsoft AD servers • OpenLDAP servers These CFTs contain LDAP attributes that are typically required to be synced with LDAP. Once you've applied the template, or if a template is not used, a sync list is visible and configurable directly on a saved LDAP server's **Sync List** tab. See *LDAP sync lists*.

LDAP authentication

Overview

Automate supports LDAP authentication and can be used either standalone (LDAP-authentication-only) or in conjunction with LDAP syncing of users:

LDAP sync and authentication	• Users are synced in from LDAP. • LDAP authenticates these users. • LDAP user sync is available for Active Directory (AD) and OpenLDAP.
LDAP authentication-only (standalone)	• Users are added locally or are synced in from CUCM. • LDAP authenticates these users. • Not available for OpenLDAP. • Requires Automate version 10.6(3) or later.

Note:

- Automate provides LDAP server support for case-insensitive search base DNs. For example, on an LDAP server, the following search base DNs are equal:
  - CN=Users,DC=example,DC=com
  - cn=Users,dc=example,dc=com

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP authentication workflow

1. User provides their credentials in the Automate system Login page.
2. Authentication request is sent to the relevant LDAP server(s), based on the user's authentication setup:

Default authentication setup	Matching username and password • Automate username and password must match the username and password in the LDAP server (based on the LDAP field chosen for *username*). • Once authenticated, the LDAP username is mapped to Automate user to determine access, role, and so on.
Alternative authentication setup	Non-matching username and password Automate supports authentication for mapping non-matching usernames. This is useful where the username in Automate and the UC apps is different to the username in LDAP. For example, if the LDAP username is bobsmith but the username in Automate is bsmith, then choose LDAP as the authentication type and set the LDAP username (bobsmith in this case) to match the username of bsmith in Automate. You would do this via the LDAP authentication attribute, such as sAMAccountName, mail, or userPrincipalName (which define the field where the username is sourced from, and which is used to authenticate the user.)

Note: For LDAP authentication, the password rules of the Automate credential policy don't apply as the password is managed in the LDAP directory. Other credential policy rules are applied (such as session length), as these are managed in Automate.

Related topics

- *LDAP user sync*
- *Configure LDAP authentication-only (standalone)*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Write-back to Active Directory LDAP

Tip: *Use the Action search to navigate Automate*

Overview

For Microsoft Active Directory LDAP servers, Automate provides an option to enable write-back as a part of Quick Add User, for both Cisco UCM Quick Add User and Microsoft Quick Add User.

Prepare for write-back to Active Directory LDAP servers

Before using write-back for Microsoft Active Directory LDAP servers, you'll need to set up the environment as follows:

1. At the required hierarchy for the **LDAP Server**:
   a. **Server Type** is `microsoft_active_directory`.
   b. **Port** is 636.
   c. **Encryption Method** is `Use SSL Encryption`.
   d. **Enable Write Operations** is enabled.
2. Add an **LDAP User Sync** instance at the required hierarchy:
   a. Select the relevant **LDAP Server**.
   b. Select a **LDAP Write Back Template** - see: *LDAP write-back template*.
   c. If the **LDAP Write Back Only** checkbox is enabled, users are *only* synced in for write-back purposes and other user updates are not carried out.

      This should only be used for a Microsoft-only type scenario where users are being synced in initially from MS365 or MSTeams and the LDAP Write Back option is configured to write back to Active Directory for the purpose of syncing to Azure.

   At the end of the Quick Add User workflow, write-back is then carried out for target model type `device/ldap/user` using this **LDAP User Sync** instance.
3. When saving **LDAP User Sync**, a data sync instance is created that applies when a sync is carried out from **Sync & Purge > LDAP Users**.
4. When Quick Add User or Microsoft Quick User is run, the LDAP user is updated in accordance with the LDAP write-back template.

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP write-back template

An LDAP Write Back template is a configuration template for target model type `device/ldap/user` that contains named macros that will be applied during write-back when the Quick Add User or Microsoft Quick User task is carried out.

For example, the following macros can be used in the configuration template selected in **LDAP Write Back Template**.

- LDAP username: `{{macro.DISPLAY_GET_USERNAME}}` - writes back username
- LDAP user first name: `{{macro.DISPLAY_NAME_GET_FNAME}}` - writes back user first name
- LDAP user last name: `{{macro.DISPLAY_NAME_GET_LNAME}}` - writes back user last name
- **Telephone Number**: `{{macro.DISPLAY_GET_FIRST_LINE}}` - write back the first line added to a user when running Quick Add User.
- **Telephone Number**: `{{macro.DISPLAY_GET_FIRST_LINE_E164}}` - write back the first E164 line added to a user when running Quick Add User.

Note:

- When writing back to Active Directory for the purpose of syncing to Microsoft Entra ID for Microsoft Teams provisioning, the LDAP authentication attribute on the LDAP user configuration must be to `userPrincipalName` and the username mapping on the **User Field Mapping** page must be set to `userPrincipalName` for the specific LDAP server.
- The configuration template is automatically created for each LDAP server; at the same level of the hierarchy as the LDAP server when **Enable Write Operations** is set to True. There can only be one Write Back configuration template per LDAP server.

6.5.2. LDAP Users Activities

Configure and execute LDAP user sync and authentication setup.

LDAP user sync

Tip: *Use the Action search to navigate Automate*

Overview

You'll need to set up an LDAP user sync in order to sync in users from a specified LDAP directory into Automate.

Users synced in from LDAP appear at the hierarchy node where the LDAP user sync object exists. Once synced in, you can manage these users in Automate (via the User Management menu). For example, you may want to move users to other hierarchies, or to push users to CUCM.

When syncing in from LDAP, some fields are always imported into Automate, while others are excluded. For details, see *LDAP authentication*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete or retain associated accounts at user sync

You can configure (via *Global settings*) the LDAP user sync to delete or retain Cisco (CUCM) subscriber voicemail and Webex accounts when running syncs after deleting a subscriber.

- On the **Webex App** tab of the Global Settings, choose whether to retain or delete the Webex app account
- On the **Voicemail** tab of the Global Settings, choose whether to retain or delete the voicemail account.

Related Topics

- For details around LDAP server setup and authentication settings, see *LDAP server*
- *Global settings*

Add LDAP sync

This procedure adds a LDAP sync to prepare for syncing users in from LDAP to Automate.

1. Log in as Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node of the LDAP server you want to sync users from.
3. Go to the **LDAP User Sync**.
4. Click **Add**.
5. Fill out details for the sync:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
LDAP Server	Mandatory. The LDAP server you're syncing from.
LDAP Authentication Only	This setting is available only in Automate, and is disabled by default. Leave unchecked (clear) to sync in users from LDAP (from a predefined LDAP directory). In this case, the user passwords are authenticated against this LDAP directory. Select this checkbox (enable) to prevent user sync from the predefined LDAP directory. In this case: • Only the users passwords are authenticated against the LDAP directory • You can add users manually via the GUI, API, bulk load, or sync users in from CUCM.
User Model Type	Defines the LDAP object (from the configured LDAP server), and is used to import and authenticate users. • When LDAP server is Microsoft Active Directory, the default is `device/ldap/user`. • When LDAP server is AD LDS (ADAM), set to `device/ldap/userProxy`. • When LDAP server is OpenLDAP, the default is `device/ldap/inetOrgPerson`. Contact the LDAP server administrator if you need to identify a non-default User Model Type to use.
LDAP Authentication Attribute	The attribute used for creating an LDAP user. When Server Type is Microsoft Active Directory, options are: `employeeNumber`, `mail`, `sAMAccountName`, `telephoneNumber`, `userPrincipalName`. When Server Type is OpenLDAP, options are: `employeeNumber`, `mail`, `telephoneNumber`, `uid`. Custom values for a deployment are also allowed.
Attribute	This value is used for LDAP authentication against LDAP when **LDAP Authentication Only** is enabled.

Copyright © 2025 VisionOSS Limited. All rights reserved.

User Entitlement Profile	Choose the User Entitlement Profile that specifies the devices and services to which users synced in from the LDAP server are entitled. The chosen entitlement profile is assigned to each synced in user. It is checked during user provisioning to ensure the user's configuration does not exceed the allowed services and devices specified in the entitlement profile.
User Role (default)*	The default role to assign to the synced user (if no other LDAP custom role mappings are applicable for the synced user, then this fallback/default role will be applied). Mandatory.
User Move Mode	Defines whether users are automatically moved to sites based on the filters and filter order defined in **Manage Filters**
User Delete Mode	Defines whether users are automatically deleted from Automate if they are deleted from the LDAP directory. If set to automatic, all subscriber resources associated with the user, such as a phone, are also deleted. **Warning:** Setting this option to *Automatic* will delete *all* users from the LDAP server (in Automate and in the UC apps, phones, services, and so on).
User Purge Mode	Defines whether users are automatically deleted from Automate if they are purged from the LDAP device model. An administrator can remove the LDAP user from the device layer even if the user has not been removed from the LDAP directory. **Warning:** Setting this option to *Automatic* will delete *all* users from the LDAP server (in Automate and in the UC apps, phones, services, and so on).

6. Inspect the default mappings and modify if required, see *User field mapping*.
7. Click **Save** to add the LDAP sync.

   Note: By default, the new LDAP sync is initially inactive. See *LDAP schedule*.

8. In the Global Settings, define whether to retain or delete associated webex and/or voicemail accounts in the user sync that runs after deleting a subscriber. See topic Global Settings (Webex App tab, Voicemail tab)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- Global Settings in the Core Feature Guide

LDAP sync scenarios (top-down and bottom-up)

The table summarizes the two LDAP user sync scenarios that Automate supports:

- Top-down
- Bottom-up

Note: Although you can have different LDAP sync types at different parts of the hierarchy, it is recommended that you run either top-down or bottom-up LDAP syncs.

Sync scenario	Description
Top-down	Users are synced *directly* from the LDAP directory. User data is sourced from one or more LDAP directories. This setup defines how users are matched to be pulled in (for example, OU definition, LDAP filter, field filters, etc). Recommended for flow-through provisioning.
Bottom-up	Users are synced *indirectly* from the LDAP directory, that is, where applications are integrated and syncing the users from the LDAP directory. For example, the system syncs via the CUCM, which is syncing to LDAP.

Note: In a top-down or bottom-up LDAP sync, a system configuration template sets the CUCM (LDAP) user's identity field (`userIdentity`) to the user principal name (UPN), `userPrincipalName`, if it exists; otherwise it uses the email address. This is useful where a user has a different email address to the UPN and needs to be correctly mapped following a LDAP sync, and then the user is moved to a site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP sync lists

The table describes, for LDAP sync, LDAP sync lists, arranged in override order:

1. *Always synced list*	Fields required to list LDAP Users on the GUI
2. *Drop Field List*	Fields never imported from LDAP
3. *Data Sync Blacklist* (denylist)	A change in these fields does not trigger an update
4. *Model Type List*	From the LDAP data sync. Set up and used in scheduled syncs
5. *LDAP Sync List* (manual or from CFT)	Fields to be imported from LDAP as set up with the LDAP server

Always synced list

The following fields are always synced in an LDAP sync as their values are required to list LDAP users on the GUI:

Column Name	Field Name
Cn	`cn`
Uid	`uid`
Description	`description`
Mail	`mail`
User Principal Name	`userPrincipalName`
SAM Account Name	`sAMAccountName`

Drop field list

Any items in the LDAP Sync List from `DROP_FIELD_LIST` are excluded from the sync. This list is read-only.

```
DROP_FIELD_LIST=[
    'photo',
    'jpegPhoto',
    'audio',
    'thumbnailLogo',
    'thumbnailPhoto',
    'userCertificate',
    'logonCount',
    'adminCount',
    'lastLogonTimestamp',
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
    'whenCreated',
    'uSNCreated',
    'badPasswordTime',
    'pwdLastSet',
    'lastLogon',
    'whenChanged',
    'badPwdCount',
    'accountExpires',
    'uSNChanged',
    'lastLogoff',
    'dSCorePropagationData'
    ]
```

Data sync denylist

See Settings (Data Sync Workflow Execution Control) in the Advanced Configuration Guide.

An LDAP sync list won't override any of the Data Sync Denylist attributes (default or custom) in `data/Settings`. That is, for fields that appear in both the LDAP Sync List and in the Data Sync Denylist, where the field value is different on the LDAP server, the LDAP sync won't trigger any update for the LDAP entity during a sync.

Model type list

Given an existing LDAP server with a LDAP Sync List configured, when executing a data sync against the LDAP server, the *existing Model Type List functionality* from the LDAP data sync is maintained and takes precedence over the LDAP Sync List.

See:

- *Create a targeted MTL*
- *Model Type Lists (MTL)*

LDAP sync list

A new LDAP server or one that existed in the system prior to release 19.3.4 allows you to choose the **LDAP Sync List Option**:

- No sync list
- Create sync list manually
- Create sync list from template

The configuration template (CFT) can also be created and applied to a server. See *LDAP sync list configuration templates*.

Important: Besides the sync override order indicated above, manual or template sync lists are bound by the following considerations:

- If no sync list is set up, LDAP sync is not affected by this list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- When updating the default sync list (or any sync list you choose), a full sync is required (during the next scheduled, or a manual sync). See the **Sync and Purge** menu, and for more information about data sync and data sync cache, see *Data sync types*.

  Until a full LDAP user import is performed, user details are updated in the local cache (when opening a management page).

  For these reasons, it is recommended that such updates and syncs should be scheduled for off-peak times, particularly where a large number of users requires a large sync.

- For users targeted for Cisco-based services, a field must be mapped to the surname field for users. It is therefore important to include a field in the Sync List that is mapped to the 'surname' field, typically `sn`.

For details on the LDAP Sync List on the LDAP server, see: *LDAP server*.

Note: By default LDAP user details shown on the GUI display all `device/ldap/user` fields. It is recommended that you create a FDP for `device/ldap/user` to contain *only* the fields from your LDAP Sync List in order to view LDAP user details according to your configuration.

LDAP sync list configuration templates

Administrators can clone the default sync list Configuration Templates (CFTs) to a hierarchy, and modify them for use during initial LDAP server setup. Modified CFTs are available at the hierarchy on the **Sync List** tab (from the **LDAP Sync List Template** drop-down).

Two default CFTs are provided. Both can be cloned:

- **Ldap Sync List Microsoft Active Directory**
- **Ldap Sync List Open Ldap**

The table describes the default CFT fields:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Ldap Sync List Microsoft Active Directory **Model Type:** `device/ldap/user`	**Ldap Sync List Open Ldap** **Model Type:** `device/ldap/InetOrgPerson`
sAMAccountName	uid
mail	mail
givenName	givenName
sn	sn
title	title
department	departmentNumber
displayName	displayName
employeeNumber	employeeNumber
employeeType	employeeType
homePhone	homePhone
ipPhone	
telephoneNumber	telephoneNumber
mobile	mobile
otherMailbox	
facsimileTelephoneNumber	facsimileTelephoneNumber
l	l
c	
streetAddress	
st	street
postalCode	postalCode
physicalDeliveryOfficeName	physicalDeliveryOfficeName
manager	manager
memberOf	memberOf
objectClass	objectClass
o	o
ou	ou

If new LDAP attribute names are added to the cloned CFT and modified on the GUI, type the names in. Initially, all attribute names are imported. The full attribute list and naming is available on the GUI **Sync List** tab from the default sync list for the server. See: *LDAP server*.

Enter a descriptive name for the cloned CFT, which will then show in the hierarchy on the drop-down list of **Sync List** CFTs that are available when you modify an LDAP server or create a new server.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Multiple LDAP organization units per hierarchy

Large corporations and institutions with multiple domains or agencies may require more than one LDAP Organizational Unit (OU) to be configured at a hierarchy.

Automate allows for multiple LDAP OUs at a hierarchy by providing for a *unique combination* of the following LDAP server properties at the hierarchy:

- IP address
- Port
- search base DN

Multiple search base DNs can therefore be configured at the *same hierarchy* for different organizations within the same company, so that administrators and self-service users can successfully authenticate. For example:

LDAP server setup:

IP	Port	Search base DN	Hierarchy
1.2.3.4	389	ou=SharedOUA,dc=voss-solutions,dc=com	Provider.Customer
1.2.3.4	389	ou=SharedOUB,dc=voss-solutions,dc=com	Provider.Customer

Users:

- userA: ou=SharedOUA,dc=voss-solutions,dc=com
- userB: ou=SharedOUB,dc=voss-solutions,dc=com

Configure LDAP authentication-only (standalone)

This procedure sets up LDAP for authentication-only, in VOSS Automate.

Note: Users can be added locally or synced from CUCM:

Scenario where LDAP authentication is the default	When users are LDAP synced in CUCM and then synced into VOSS Automate
Scenario where LDAP authentication is not the default	• When users are manually configured in CUCM and then synced into VOSS Automate • When users are manually configured in VOSS Automate

You can change the default behavior, as described in *View and Update LDAP Authentication Users*.

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

To set up LDAP for authentication-only . . .

1. Log in as Provider, Reseller, or Customer administrator.
2. Choose the hierarchy where you have the LDAP server set up (the server you're using to authenticate users).
3. Go to **LDAP User Sync**.
4. Click **Add**.
5. Fill out the relevant details:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
LDAP Server	Choose the LDAP Server where you are authenticating users.
LDAP Authentication Only	Disabled by default, which means users will be synced from the configured LDAP directory and their passwords are authenticated against that LDAP directory. When enabled: • The LDAP server is used only to authenticate users. • Only available at hierarchy nodes with an LDAP server, so not available for users created at sites. • Fill out the **CUCM LDAP Directory Name** for the LDAP server. When more than one LDAP server sync is created and you don't provide this detail, no LDAP users are created and the transaction log shows a warning. • Users won't be synced from the configured LDAP directory but their passwords are authenticated that LDAP directory. • You can manually add users from the GUI or API, bulk load them, or sync them from CUCM.
User Model Type	Read-only. Identifies the LDAP object (defined in the configured LDAP server), used to authenticate users.
LDAP Authentication Attribute	Mandatory. Choose the LDAP Attribute for authenticating users. Options are: • sAMAccountName (only option for AD, and the default for AD) • uid (only option for OpenLDAP, and the default for OpenLDAP) • mail • employeeNumber • telephoneNumber • userPrincipalName (AD or hybrid, for MS) These are the same values CUCM uses for LDAP Attribute for User ID. Active Directory (AD) only: For these user types, don't choose **userPrincipalName**, unless the **userPrincipalName** value was set as the Username when the user was created: • Users created using the VOSS Automate GUI • Users created using the VOSS Automate API • Users bulk loaded into VOSS Automate • Users manually created in Unified CM and synced into VOSS Automate For users synced from LDAP into CUCM and then into VOSS Automate: Caveats (AD and OpenLDAP) For users synced from LDAP into CUCM and then into VOSS Automate: • We strongly recommend selecting the same LDAP Authentication Attribute as Unified CM uses for LDAP Attribute for User ID. • If you sync users into Unified CM using attributes other than sAMAccountName/uid, do not choose sAMAccountName/uid. If you sync users from LDAP into CUCM using employeeNumber, choose employeeNumber for the LDAP Authentication Attribute. However, to get the LDAP Authentication to work properly, one of these conditions must be met: • Before syncing users from CUCM to VOSS Automate, set the Employee Number field on CUCM Server FieldMapping tab to userid • Define the LDAP for Authentication Only sync before syncing users from CUCM into VOSS Automate

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Click **Save**.

   All users with `SyncToHierarchy` set to the hierarchy of the LDAP server now use the LDAP server for authentication. Users are added to the LDAP Authentication Users list.

Sync or purge LDAP users

This procedure syncs or purges (deletes) users that were synced from an LDAP server.

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, select the hierarchy where the LDAP server exists.
2. Go to **LDAP Users**.
3. Configure the following:

Setting	Description
Remove Log Messages	Defines whether to remove user management logs before syncing or purging.
Remove Log Direction	Displays only when **Remove Log Messages** is enabled. Choose an option: • Local - removes logs at the hierarchy of the LDAP server. • Down - removes logs at and below the hierarchy of the LDAP server.
LDAP Server	Mandatory. Choose the organization unit of the LDAP server from which you need to sync or purge the users.
LDAP Action	Mandatory. Select an option from the drop-down to run either a sync or purge: • Synchronize users from LDAP • Purge local LDAP device resources

Warning: If you're choosing to run a purge, a system message displays onscreen to warn you that purging will result in the loss of data. All LDAP users imported from the selected LDAP server will be removed.

It is recommended that you consider this warning carefully, and the consequences of a purge:

- If "purge" mode on the LDAP user sync configuration is set to *Manual*, any subscribers associated with these LDAP users will be retained and converted to local subscribers.
- If "purge" mode on the LDAP user sync configuration is set to *Automatic*, any subscribers associated with these users, as well as their devices and services, will be deleted.

4. Save your changes.

   The transaction is triggered. View transaction progress and details in the Transaction Logs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide.

LDAP custom role mappings

Overview

LDAP custom role mapping allows you to apply (in top-down deployments only) customized roles, to LDAP synced and moved users. The default roles are overwritten.

The table describes how LDAP custom role mapping works for LDAP user sync and LDAP user move:

Action	Description
LDAP user sync	• By default, users synced in from LDAP are assigned the role configured in 'User Role(default)', in the LDAP user sync. • The role specified in the custom role mapping takes precedence over the 'User Role(default)', when both of the following conditions are met: – The user's **Active Directory Group** Membership matches a group configured in the custom role mapping – The hierarchy of the LDAP user sync matches the **Target Role Context**
LDAP user move	• By default, users moved manually to a hierarchy (using 'Move Users') are assigned the role specified in 'Set Default Role'. • The role specified in the custom role mapping takes precedence over the 'Set Default Role' chosen in 'Move Users', when both of the following conditions are met: – The user's **Active Directory Group** matches a group configured in the custom role mapping. – The user's destination hierarchy type matches the **Target Role Context**. • By default, a user moved to a hierarchy automatically (using a filter), is assigned the role specified in the filter in 'Set Default Role'. • The role specified in the custom role mapping takes precedence over the 'Set Default Role' defined in the filter, when both of the following conditions are met: – The user's **Active Directory Group** Membership matches a group configured in the custom role mapping. – The user's destination hierarchy type (specified in the filter), matches the **Target Role Context**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add LDAP custom role mapping

Tip: *Use the Action search to navigate Automate*

In top-down deployments only, this procedure applies customized roles to LDAP synced and moved users, and overwrites default roles.

1. Log in as Provider or Reseller administrator.
2. Set the hierarchy to where the LDAP custom role mapping must be added.
3. Go to **LDAP Custom Role Mappings**.
4. Click **Add**.
5. Fill out the fields (all are mandatory):

Field	Description
Active Directory Group	The user's Active Directory group, derived from 'memberOf', from the LDAP Schema. This must be an exact match of the value defined in Active Directory, for example, CN=Administrators,CN=Builtin,DC=test,DC=net.
Target Role Context	The hierarchy for which the custom role mapping will be applied. This must match the hierarchy type where the users are synced, or their destination hierarchy when moved. For example, if a user is assigned a 'CustomerAdmin' role, and the LDAP user sync is configured at Customer level, then the **Target Role Context** must be set to Customer. If a user is assigned a 'SiteAdmin' role, and is being moved (manually or automatically) using 'Filter to a Site', then **Target Role Context** must be set to Site.
Target Role	The role to apply to the user if their **Active Directory Group** and **Target Role Context** are matched. This must be a valid role at the user's destination hierarchy. This can be defined at a specific role or as a macro. For example, if the user is assigned a 'SiteAdmin' role, the role can be defined as the exact name of the role or defined as a macro, which allows re-use for any site name e.g. {{macro.SITENAME}}SiteAdmin.

6. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP schedule

Tip: *Use the Action search to navigate Automate*

Overview

You can sync users in to Automate from LDAP in any of the following ways:

- Activate a scheduled sync
- Run a manual sync

Activate LDAP scheduled sync

This procedure activates a LDAP sync from a schedule.

Prerequisites

- LDAP server must be present

Perform these steps:

1. Go to **LDAP Schedule**.
2. Click on a LDAP schedule.
3. On the **Base** tab, select the **Active** checkbox.
4. Click **Save**.

   The system attempts to sync users from the LDAP server. It may take a few minutes for the users to show up in Automate.

   Note: You can't cancel a sync once it's running, and you can't delete an LDAP server while a sync is in progress.

5. Once the sync completes, verify that users are synced in:
   - Navigate to the LDAP server hierarchy to view the lists on the **LDAP Users** menus.
   - Verify that users are synced in from LDAP, via the **Users** page.

Related Topics

- For details around running a manual LDAP sync, see *Sync or purge LDAP users*.
- For details on sync lists and scenarios, see *LDAP authentication*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.5.3. Insights

Actions for orchestration of configuration into the Insights product.

Introduction to Insights monitoring

Tip: *Use the Action search to navigate Automate*

Overview

Users with both Automate and Insights deployed can enable monitoring of UC applications via the Automate Admin Portal, from an Insights Arbitrator server integrated with Automate.

Note: For details around integrating Automate with the Insights Arbitrator server, see *Insights Assurance Arbitrators*

Once the integration is set up, you onboard customer server clusters, comprising one or more Cisco Unified Communication Manager (UCM) CallManager servers and/or Cisco Unity Connection (CUC) servers, to an Arbitrator server for monitoring, from within the Automate Admin Portal.

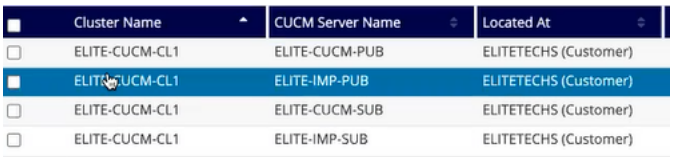
The following servers are supported:

- Cisco Unity Connection (CUC) servers
- Cisco UCM servers

  Provisioning is supported for these UCM server types:

  - Voice (VOICE_VIDEO)
  - IM and Presence Service (IM_P)

Note: The image displays a customer with four Cisco UCM servers that are part of the same cluster. The cluster is onboarded to the Arbitrator server for monitoring purposes.



Cluster Name	CUCM Server Name	Located At
ELITE-CUCM-CL1	ELITE-CUCM-PUB	ELITETECHS (Customer)
ELITE-CUCM-CL1	ELITE-IMP-PUB	ELITETECHS (Customer)
ELITE-CUCM-CL1	ELITE-CUCM-SUB	ELITETECHS (Customer)
ELITE-CUCM-CL1	ELITE-IMP-SUB	ELITETECHS (Customer)

This feature provides the following functionality in the Admin Portal:

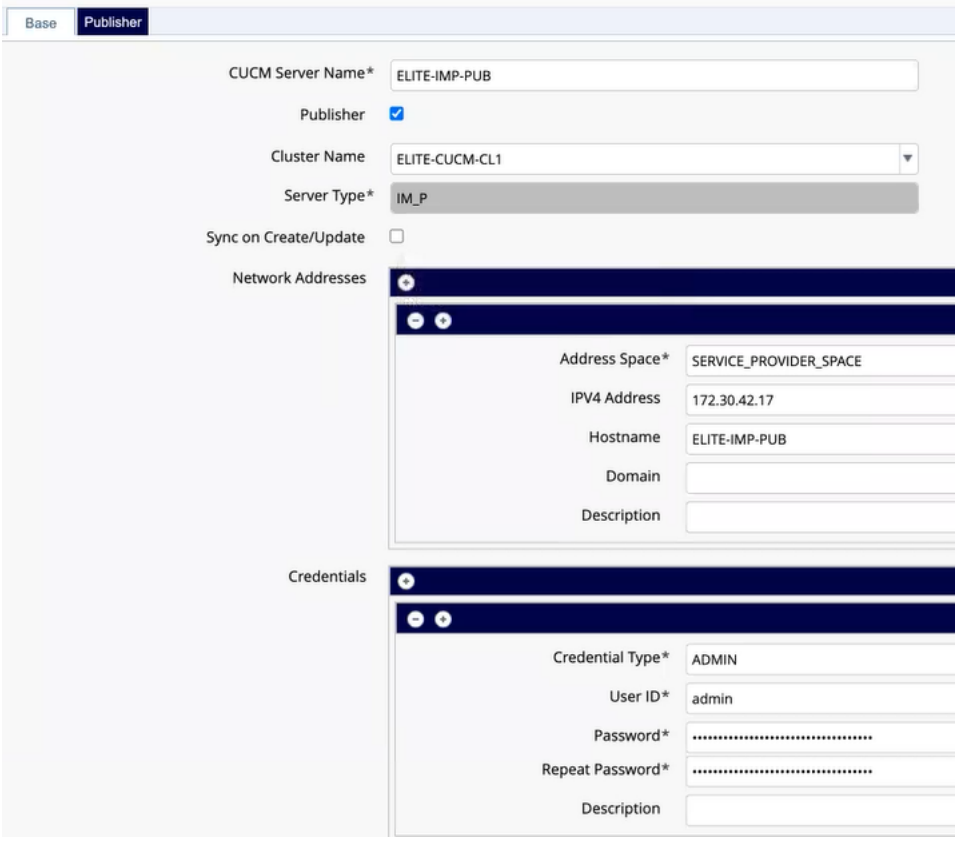
- Integrate Arbitrator servers, and view existing integrations, via the Insights **Arbitrators** page in Automate. See *Insights Assurance Arbitrators*

  Note: The Arbitrator server should be at version SP23 or higher.

- View currently configured monitoring set up for server clusters, if any:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- For UCM servers, go to the **Servers** page (for UCM), then click on a cluster to view the following:
  - On the **Base** tab, view the cluster name and server type (VOICE_VIDEO or IM_P), and whether the server is a Publisher server or a Subscriber server.
  - On the **Publisher** tab, view monitoring details, including the monitoring Arbitrator server, if any.



  - For CUC servers, go to the CUC **Servers** page, then click on a cluster to view monitoring details, including the monitoring Arbitrator server, if any.

- When adding new UCM or CUC server in a cluster, you can choose an Arbitrator to monitor the servers (via the Monitoring fields for Cisco Publisher servers)

Note: At the time of writing (Automate v21.3), modifying any existing monitoring setup on UC apps is not supported. However, deleting a UC app on Automate will remove the asset and related configuration from all corresponding Insights Arbitrator servers.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Onboarding provisioning

The onboarding process triggers a workflow that finds all the servers in the cluster, then provisions all required monitoring elements (which differ depending on whether the server is UCM or CUC, Publisher or Subscriber, or CUCM server type VOICE_VIDEO, or IM_P).

Note: You can view all workflow provisioning steps via the transaction log in the Admin Portal.

Sub Transactions

Action	Status	Transaction	Submitted Time	Detail
Create Onboard Assurance Asset CUCM Server	Success	Link	April 5, 4:55:55 AM	Onboard ELITE-IMP-SUB CUCM Server onto PROBE
Create Onboard Assurance Asset CUCM Server	Success	Link	April 5, 4:55:31 AM	Onboard ELITE-CUCM-SUB CUCM Server onto PROBE
Create Onboard Assurance Asset CUCM Server	Success	Link	April 5, 4:54:56 AM	Onboard ELITE-IMP-PUB CUCM Server onto PROBE
Create Onboard Assurance Asset CUCM Server	Success	Link	April 5, 4:52:46 AM	Onboard ELITE-CUCM-PUB CUCM Server onto PROBE

The table describes the onboarding provisioning that occurs for the server types supported for Arbitrator monitoring:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Server in the cluster	Onboarding Provisioning
CUCM VOICE Publisher (PUB)	Provisioning on Arbitrator: 1. Creates the asset on Arbitrator. 2. Adds the asset into an asset group on Arbitrator (or updates the asset group if it already exists) 3. Creates a credential for the server. 4. Creates a server-specific probe and probe group combination. 5. Creates five Arbitrator monitoring profiles, which define the schedule for the probe to run on the asset (for example, every 5 minutes, or once a day): • A server-specific PERFMON CUCM group profile that associates the probe and probe group combination with the asset and the credential. • Four profiles that associate static probes (which are always on the Arbitrator) with the asset: RIS, PING Monitor, Version, RTMT The static probes must exist on the Arbitrator for Arbitrator monitoring to work. The static probes are associated with new assets, using the profiles. Provisioning on the CallManager: • Creates the application user. When onboarding multiple servers, you can ignore a *fail* status at this step `Create Cucm App User`, since duplicate user creation is ignored. • Updates service parameters
CUCM VOICE Subscriber (SUB)	Provisioning on Arbitrator: 1. Creates the asset on Arbitrator. 2. Adds the asset into an asset group on Arbitrator (or updates the asset group if it already exists) 3. Creates a credential for the server. 4. Creates one Arbitrator monitoring profile (ping test only).
CUCM IM_P Publisher (PUB)	Provisioning on Arbitrator: 1. Creates the asset on Arbitrator. 2. Adds the asset into an asset group on Arbitrator (or updates the asset group if it already exists) 3. Creates a credential for the server. 4. Creates a server-specific probe and probe group combination. 5. Creates two Arbitrator monitoring profiles, which define the schedule for the probe to run on the asset (for example, every 5 minutes, or once a day): • A server-specific PERFMON CUCM group profile that associates the probe and probe group combination with the asset and the credential. • A PING Monitor profile

Copyright © 2025 VisionOSS Limited. All rights reserved.

Server in the cluster	Onboarding Provisioning
CUCM IM_P Subscriber (SUB)	Provisioning on Arbitrator: 1. Creates the asset on Arbitrator. 2. Adds the asset into an asset group on Arbitrator (or updates the asset group if it already exists) 3. Creates a credential for the server. 4. Creates one Arbitrator monitoring profile (ping test only).
CUC Publisher (PUB)	View the transaction and sub-transaction log for details.
CUC Subscriber (SUB)	View the transaction and sub-transaction log for details.

For details, see *Onboard assets*

Note: All provisioned elements can be viewed on the Insights Arbitrator dashboard. For details, see the Insights documentation.

Probe groups, profiles, and asset onboarding

The table describes the probe groups and profiles that are added to the Insights Arbitrator server when assets are onboarded, and removed when assets are off-boarded.

PERFMON CUCM Group Profile	
Probe name	`axlGetPerfmonCounters_CUCM_INTF (<CUCM Cluster name>)`
Probe Group Name	`<customer_name>-CUCM Perfmon AXL (<CUCM Cluster name>)`
Frequency	600 sec (10 min)
For Publisher Server	Yes
For Subscriber Server	No

Copyright © 2025 VisionOSS Limited. All rights reserved.

PERFMON CUC Group Profile	
Probe name	axlgetperfmon (<CUCxn Cluster name>)
Probe Group Name	<customer_name>-Cisco Unity AXL (<CUCxn Cluster name>)
Frequency	300 sec (5 min)
For Publisher Server	Yes
For Subscriber Server	No

RIS Group Profile	
Probe Group Name	1-Cisco CUCM RIS CmDevice_creds
Frequency	300 sec (5 min)
For Publisher Server	Yes
For Subscriber Server	No

PINGMON Group Profile	
Probe Group Name	1b-PING Monitor
Frequency	300 sec (5 min)
For Publisher Server	Yes
For Subscriber Server	Yes

VERSION Group Profile	
Probe Group Name	4-Cisco CUCM Version
Frequency	86400 sec (24 hr)
For Publisher Server	Yes
For Subscriber Server	No

RTMT Group Profile	
Probe Group Name	5-Cisco RTMT
Frequency	1800 sec (30 min)
For Publisher Server	Yes
For Subscriber Server	No

Copyright © 2025 VisionOSS Limited. All rights reserved.

Offboarding assets

Should you wish to disable monitoring and remove data from the Arbitrator server, you can offboard these assets (and their related configuration) from the Arbitrator server. For details see *Offboard assets*

Insights Assurance Arbitrators

Tip: *Use the Action search to navigate Automate*

Overview

Managing Insights Arbitrators in Automate requires the following:

- A License Mode for Insights Collaboration Assurance - see: *Manage your Automate product license*.
- Set up Arbitrators
- Set up host connection details and credentials (the admin user and password from the Arbitrator)

Note: See the Insights documentation for Arbitrator setup.

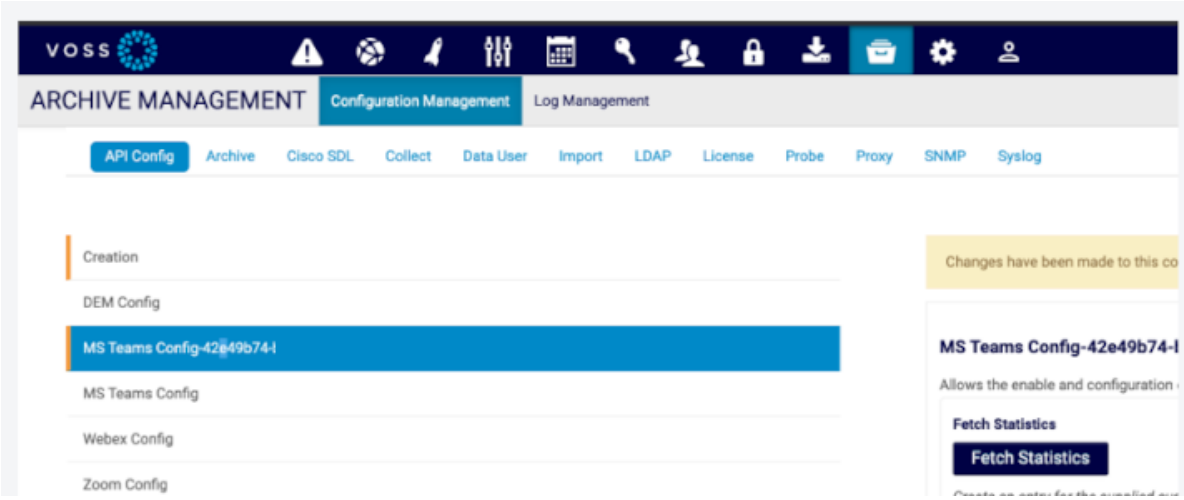
Add a connection to the Arbitrator server

This procedure provides connection details to the Arbitrator server to integrate Automate with the Arbitrator server.

Note: Once the integration is complete:

- The Arbitrator is available to onboard and offboard assets that are added or are available in Automate.

  For example, if a MS Tenant is managed in Automate (*Microsoft tenant setup*), the corresponding MS tenant is shown and managed on the associated Arbitrator. The image shows an example where a tenant displays on the Arbitrator (API Config tab):



Copyright © 2025 VisionOSS Limited. All rights reserved.

Also verify that the MS Tenant configuration includes a secret set up - see *Microsoft tenant setup*.

- If **Assurance** is selected as **Data Source** to manage dashboard widgets, options are available to choose it as a **Data Source Instance**, since multiple instances can be configured. See: *Chart widgets* and *Table widgets*.

Add a connection to the Insights Assurance Arbitrator:

1. In the Automate Admin Portal, go to **Insights Assurance Arbitrators**.
2. Click the Plus icon (+) to add an Arbitrator.
3. Fill out Arbitrator details:

Server Name	Name of the Insights Arbitrator server in Automate. Alphanumeric characters, allows spaces, dashes, underscores (for example, *ARB-US-001*).
Description	Optional. Provide a description.
Host Name	Host name or IP address of this Arbitrator server, which is used to connect to the Arbitrator.
API Username	Username for a valid admin account; an admin user allowed to log in to the Arbitrator server.
API Password	Password credential of a valid admin account; an admin user allowed to log in to the Arbitrator server.
Database Password	The Arbitrator database password (this password can be changed from the default on the Arbitrator CLI -
Data Center	The name of the data center where the Arbitrator server is deployed. Used as the location when Arbitrator assets are created.
Sync on Create/Update	When enabled (selected) Arbitrator server (based on **Host Name**) data is synced in to Automate (pull sync).

4. Click **Save**.
   - A data sync instance is created: `SyncAssuranceArbitrator__<arbitrator-name>`
   - A data sync instance is created: `PurgeAssuranceArbitrator__<arbitrator-name>`
   - A test connection is automatically carried out when saving the arbitrator details and it can also be used to manually verify input details and connection to the Arbitrator host (via the **Action** menu).
   - The new Arbitrator server is added to the list of Arbitrators displayed on the **Arbitrator** summary list view.

Note:

- The Arbitrator default database password for Automate can be managed from the Arbitrator on the **Change Passwords** CLI menu on the Arbitrator. For details on the Arbitrator command line menus, refer to the Arbitrator Install Guide and Dashboard and Arbitrator Maintenance and Upgrade Guide.

  To carry out this task, choose: **Change Automate Public Database Password** from the menu.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- If **Global Settings**, **Enabled Services** shows **Enable Microsoft** as true, then Microsoft Tenant hierarchies can be synced in to the Arbitrator hierarchy via the **Sync in Microsoft Tenants** menu. Such a sync would then also allow for **Digital Experience Monitoring (DEM)** from the **Microsoft Insights** menu / dashboard. This sync should be repeated for any new Microsoft Tenants added under the hierarchy. For details, refer to *Digital Experience Monitoring (DEM)* in *Introduction to Microsoft Insights*.

Next Steps

- CUCM and CUC servers can now be onboarded and enabled for monitoring. See *Onboard assets*.

Related topics

- *Onboard assets*
- *Offboard assets*
- *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

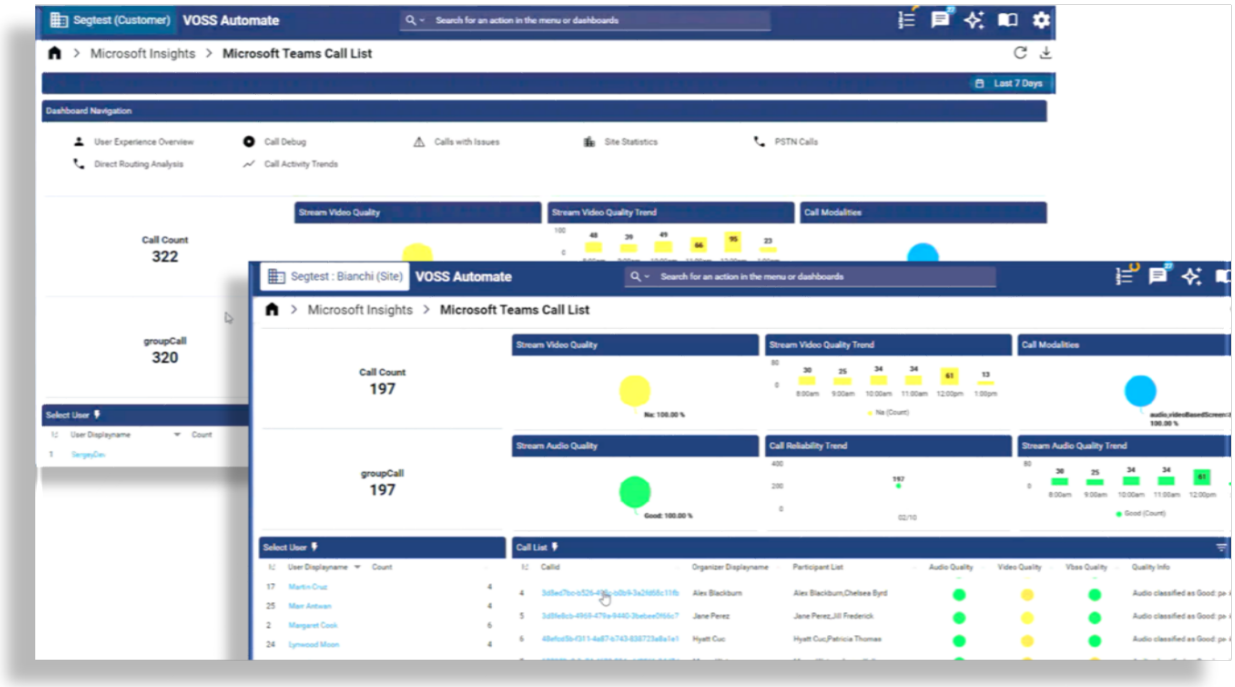
Push hierarchy details to Arbitrator's call data

This procedure pushes Automate's user hierarchy paths into Arbitrator's call records from the Microsoft tenant on Automate to update the Arbitrator.

Pushing Automate's user hierarchy paths into Arbitrator, particularly when new sites are added, allows new calls to be stamped with the correct hierarchy, enabling segmentation of Microsoft Teams call data, role based access control (RBAC), and filtering in Insights dashboards.

Microsoft Teams call data (collected by Arbitrator) is segmented to match the user hierarchies defined in Automate so that admins can view this data in the correct business context. This allows the Microsoft Insights dashboards in Automate to display accurate call details at selected hierarchies, at a particular customer or site for example.

Existing call records are excluded. New calls (after the update) will have their hierarchy stamped - based on their user principal name (UPN) in the call record, matched to the correct hierarchy - as they're brought into Automate from Microsoft.



Prerequisites:

- Microsoft tenant set up and added to the *Network Device List* (NDL)
- Arbitrator connection set up in Automate.

Note: The Microsoft tenant pushes its configuration data (including hierarchy information) to the Arbitrator so that you won't need to add these details for the tenant on the Arbitrator. The call records on Arbitrator can then be stamped with hierarchy details from the tenant.

You will need to perform this procedure whenever you're adding a new tenant at the Provider level so that the Arbitrator is updated with data from all Microsoft tenants.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Push hierarchy paths to Arbitrator

1. In the Admin Portal, go to **Insights Assurance Arbitrators**.
2. Click on the arbitrator.
3. From the overflow Action menu, select **Update Microsoft Tenants to Arbitrator** to push tenant configuration data to the Arbitrator.

Note: If you're at Provider level, tenant config data from all tenants at this hierarchy is pushed to Arbitrator.

Related topics

- See *Insights Analytics (sync-check-arbitrator)* in the Platform Guide
- Network device lists in the Core Feature Guide
- Microsoft tenant setup in the Core Feature Guide.

Remove an Arbitrator server

This procedure removes an Arbitrator server from the list of Arbitrator servers configured for integration with Automate.

1. In the Automate Admin Portal, go to **Arbitrator** (Insights).
2. View the summary list of available Arbitrators set up for integration with Automate.
3. Select the relevant Arbitrator, then click **Delete**.
   - The Arbitrator server is removed from Automate app servers (Unified CM, Unity Connection).
   - The integration details for this Arbitrator server is removed from Automate.
   - On the **Monitoring** group of the UC app server publisher form, the **Insights Arbitrator** checkbox is removed.
   - Created pull/purge data syncs on Automate are removed.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Onboard assets

Tip: *Use the Action search to navigate Automate*

If Insights Arbitrator servers are configured at a hierarchy, you can manage the clusters and Arbitrator servers in a batch, for existing UC app clusters (CUCM and CUC) in Automate.

Note: Modification of any existing monitoring on UC Apps is not supported. However, once a Cisco UCM or CUC server is created, use the Onboard/Offboard Asset tools to enable/disable monitoring.

1. In the Automate Admin Portal, go to **Onboard Assets** (Insights).
2. Choose a Customer hierarchy.
3. From the **Credential Type** drop down, keep the default, `ADMIN`, or choose a different credential type.

   Note: This field defines the credential type of the UC server to use for asset configuration on the Arbitrator.

4. View available CUCM and CUC clusters and Arbitrators, then select options in the **Available** fields and move these to the **Selected** fields in the relevant transfer boxes.
5. Click **Save**.
   - You can inspect the onboarding workflow transaction log to view the updates and import of the CUCM and CUC server service parameters and all provisioning workflow steps. See *Onboarding provisioning*
   - All servers (assets) in the selected cluster are onboarded (created on Arbitrator). Servers that are already onboarded are skipped.
   - One asset group is created per customer (required by Arbitrator).
   - For details on probe groups, see *Probe groups, profiles, and asset onboarding*
   - Credentials created on Arbitrator use the chosen credential type user credentials you chose. These credentials are used to make the request to the asset, for example AXL user for CUCM.
   - For CUCM, service parameters are updated for each server:
     - Setting up remote syslog
     - Enable CDR and related settings
     - Create the application user, if this is a Publisher
   - If an existing CUCM is updated, it is updated to show it is monitored by the Arbitrator.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Probe groups, profiles, and asset onboarding*
- *Cisco UCM servers*
- *CUC servers*

Additional onboarding tools for single clusters and servers

Automate provides a number of additional *views* that are not, by default, exposed in the default menus, but which have access profiles enabled for Provider and higher-level administrators. These views allow you to onboard single assets.

You can add these views to the menus, if required:

- Onboard Insights Asset CUCM Server
- Onboard Insights Asset CUC Server
- Onboard Insights Asset CUCM Cluster
- Onboard Insights Asset CUC Cluster

These tools do not direct you to a particular hierarchy and the views allow you to carry out the tasks on the page by selecting the following:

- Credential Type
- CUCM/CUC Server or cluster
- Arbitrator Server

The views offer the same functionality as the transfer boxes available via the **Onboard Assets** and **Offboard Assets** pages. However:

- You won't be forced to choose a particular hierarchy.
- Tasks can be carried out for a shared architecture; for example, if the cluster is located at a reseller hierarchy.

Offboard assets

Tip: *Use the Action search to navigate Automate*

Overview

Cisco UCM and CUC server clusters that have been integrated with Insights Arbitrator servers can be offboarded in two ways:

- Offboard the asset
- Delete the UC app

Note: While an asset can be offboarded, the feature does not currently allow for the *modification* of any existing monitoring on UC Apps.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics:

- *Introduction to Insights monitoring*
- *Arbitrators*
- *Onboard assets*

Offboard assets

This procedure allows a batch removal of the clusters associations by Arbitrator server.

1. In the Automate Admin Portal, choose the relevant customer hierarchy.
2. Go to **Offboard Assets**.
3. On the **Offboard Assets** page, choose relevant options:
   - From the **Arbitrator Server** drop-down, choose the Arbitrator server where you wish to remove (offboard) an asset.
   - In the **Available** field, select assets to remove (which are currently associated with the Arbitrator), and click the right-pointing arrows to move these items to the **Selected** field.
4. Click **Save**.

Note:

- View the transaction log to ensure assets are off-boarded as required.
- Automate makes the following updates on the associated Arbitrator when a Cisco UCM or CUC server (asset) is unassociated from an Insights Arbitrator:
  - Removes asset (the server)
  - Removes or refreshes asset group
  - Removes probe (performance monitoring)
  - Removes probe group (customer specific). See *Probe groups, profiles, and asset onboarding*
  - Removes relevant credentials on Arbitrator (by default the ADMIN user credentials set up on Automate)
  - Removes profiles in Insights Arbitrator (**Probe Group** > **Templates**/**Profiles**). See *Probe groups, profiles, and asset onboarding*
  - For CUCM, removes the application user, if this is a Publisher.

Note: Off-boarded CUCM and CUC servers in a cluster remain, and show **Monitoring** details with specific **Assurance Arbitrator Server** instances disabled.

The UC app server add/update page displays the unchecked (removed) Arbitrators. See the **Monitoring** section on the **Publish** page (for CUCM or CUC > Server).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete a UC app to offboard the asset

When a CUCM or CUCM server or cluster that was integrated with an Insights Arbitrator server is deleted, the asset, customer-specific probes, profiles, credentials, and related data are removed from the Arbitrator.

The Insights Arbitrator data syncs for the UC app are also removed.

Additional offboard tool for single servers

Automate provides a *view* that is not, by default, exposed in the default menus, but which has access profiles enabled for Provider and higher-level administrators. This view allows off-boarding of a single asset.

You can add this view to the menus, if required:

- Offboard One Assurance Asset

This tool allows you to select the following on the page to perform off-boarding:

- Assurance Arbitrator Server
- Asset: Cisco UCM/CUC Server

6.5.4. Microsoft Operator Connect for Providers

Set up provider Operator Connect integration and management.

Microsoft Operator Connect management in Automate

Tip: *Use the Action search to navigate Automate*

Overview

This feature provides support for Microsoft Operator Connect in Automate, allowing service providers to manage the numbers that customers can order from them, from within Automate.

Data is synced between Automate and the service provider's Operator Connect portal to automate the process of setting up customers, and the ordering and assignment of numbers.

Service provider customers log in to their Operator Connect portal to order numbers. These requests are sent to the service provider's Operator Connect portal as *Customer Consents*, which are synced in to Automate via the service provider's Operator Connect tenant that is set up in Automate.

Automate supports the following MS Operator Connect management features:

- Customer onboarding
- Pushing numbers via the service provider's Operator Connect APIs to their customer tenants and into the service provider's Session Border Controller (SBC) infrastructure
- Removing numbers
- Removing customers

Copyright © 2025 VisionOSS Limited. All rights reserved.

Providers use the MS Operator Connect functionality in Automate only when they're providing Operator Connect numbers to customers. Operator Connect support in Automate is intended as an additional feature, alongside the MACDs and other Microsoft capabilities, for those service providers offering additional services.

The workflow for MS Operator Connect is as follows:

1. The admin user adds an Operator Connect tenant at the Provider level, which also creates a number of default syncs in the Admin Portal.
2. The admin user initiates a test connection on the Operator Connect tenant.
3. The admin user can initiate a sync on the Operator Connect tenant to import data from the Operator Connect tenant.

   Imported data is automatically moved from Provider level to Customer level:

   - When the imported data is added (based on the Tenant ID configured for each Customer in `relation/MicrosoftTenant`)
   - When imported data is updated (based on the Tenant ID configured for each Customer in `relation/MicrosoftTenant` for any data that was previously at the Provider level).

MS Operator Connect functionality in Automate:

- View and update the partner consent status, at Provider or Customer level. See *Partner operator consent*
- View a list of calling profiles at the Provider level. See *Calling profiles*
- View a list of number usage capabilities at the Provider level. See *Number usage capabilities*
- View a list of previously ordered numbers, at Provider or Customer level. See *Number order history*
- View a list of previously released numbers, at Provider or Customer level. See *Number release history*
- Add or remove numbers and number ranges, at the Customer or Site level. See *Upload number range* and *Numbers (for MS Operator Connect Tenants)*

Related Topics

- *Operator Connect tenant*
- *Partner operator consent*
- *Numbers (for MS Operator Connect Tenants)*
- *Number order history*
- *Onboard customers for Operator Connect using the Customer Build Tool*

Operator Connect tenant

Creating an Operator Connect tenant in Automate allows for syncing of data between the service provider's Operator Connect tenant on their Operator Connect portal, and Automate.

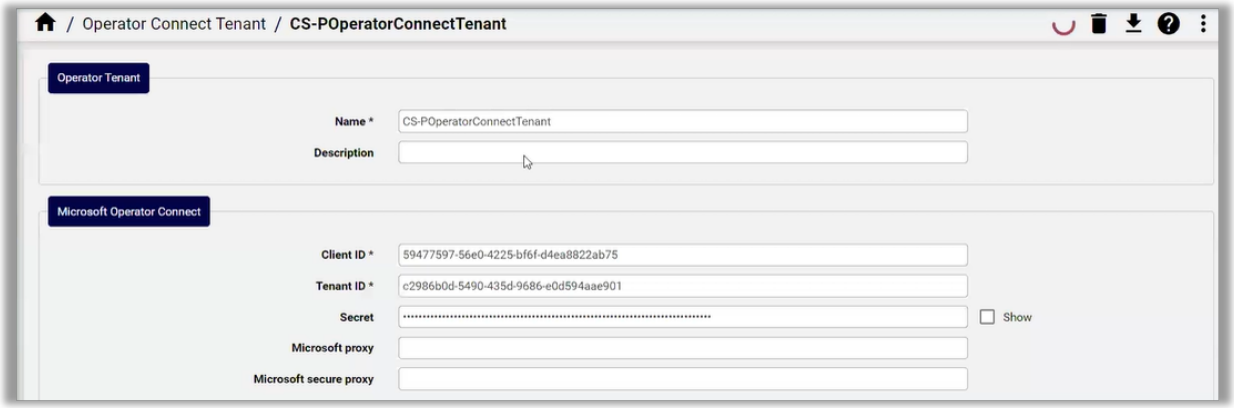
As a service provider, you can create an Operator Connect tenant in Automate at the Provider level in the hierarchy, and add the details to connect to your Operator Connect tenant.

Once you've added the tenant, you can test this connection, then initiate a sync to import data, using the default data sync that is created when saving the new Operator Connect tenant in the Automate Admin Portal.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Default syncs are created in Automate for adding and updating data from your Operator Connect tenant on the Operator Connect portal. See *Operator Connect default data syncs*

Imported data is automatically moved from the sync-in level (Provider) to the Customer level when data is added or updated, based on the Tenant ID configured for each customer in `relation/MicrosoftTenant`. For updated data, this is also based on any data that was previously at the Provider level.



Related topics

- *Microsoft Operator Connect management in Automate*
- *Operator Connect default data syncs*
- *Partner operator consent*

Add an Operator Connect tenant

This procedure adds the Operator Connect tenant and creates the default data syncs.

1. In the Automate Admin Portal, log in as Provider admin, then go to the **Operator Connect Tenant** page.
2. Choose the Provider hierarchy.

   Note: You can only add a tenant for Operator Connect at the Provider level.

3. In the list view, click the Plus icon (+) to add an Operator Connect tenant, then fill out the following details for the new tenant:
   - Fill out a name (mandatory), and a description (optional).
   - (Mandatory) Fill out the client ID (application ID) from the Azure AD app registration portal.
   - (Mandatory) Fill out the tenant ID (directory ID) from the Azure AD app registration portal.
   - (Optional) Fill out the client secret previously created in the Azure AD app registration portal.
   - (Optional) Fill out the details of the Microsoft proxy and the Microsoft secure proxy.
5. Click **Save** to add the new tenant, and wait for the transaction to complete.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Click **Action > Test Connection** to verify that the tenant can connect to Azure.
7. Click **Action > Sync** to import data.
   - Default syncs are added.
   - Imported data is automatically moved from the Provider level to the Customer level (based on the tenant ID configured for each customer (in `relation/MicrosoftTenant`).

Note: In subsequent syncs, previously imported data may be updated based on the tenant ID configured for each customer (in `relation/MicrosoftTenant`), for any data that was previously at the Provider level.

Operator Connect default data syncs

When adding an Operator Connect tenant, a number of default data syncs are added to Automate for retrieving data from the Operator Connect tenant.

To view these data syncs, go to the **Data Sync** page.

Note: In the **Data Sync** list view, type all or part of the phrase *Operator Connect* in the **Name** column or the **Device Type** column to filter the list for only the data syncs relevant to Operator Connect.

The default data syncs for Operator Connect simplify scheduling; that is, you can add a schedule at any time, and use the default data syncs.

The table describes the default data syncs for Operator Connect:

OperatorConnect Sync Type	Description
`SyncMSOperatorConnect`	A full pull sync that syncs in all data.
`SyncMSOperatorConnectNumber`	Contains a model type list that syncs in just numbers.
`SyncPartnerOperatorConsents`	Syncs in new or updated partner consents.
`PurgeMSOperatorConnect`	A purge sync that removes all locally synced data from the Automate database.

Partner operator consent

Partner operator consents define the progress of a service provider's relationship with their customer. For example, when the customer first contacts the service provider, the partner consent status is set to *Customer Contacted*.

You can view and manage partner consent statuses for your customers (at Provider or Customer level), via the **Partner Operator Consent** page.

Provider or customer-level partner operator consents are initially synced in from the MS Operator Connect portal to Automate once you add the Operator Connect tenant and run a full pull sync. Thereafter, you can run a `SyncPartnerOperatorConsents` sync to sync in only new or updated partner consents.

Copyright © 2025 VisionOSS Limited. All rights reserved.

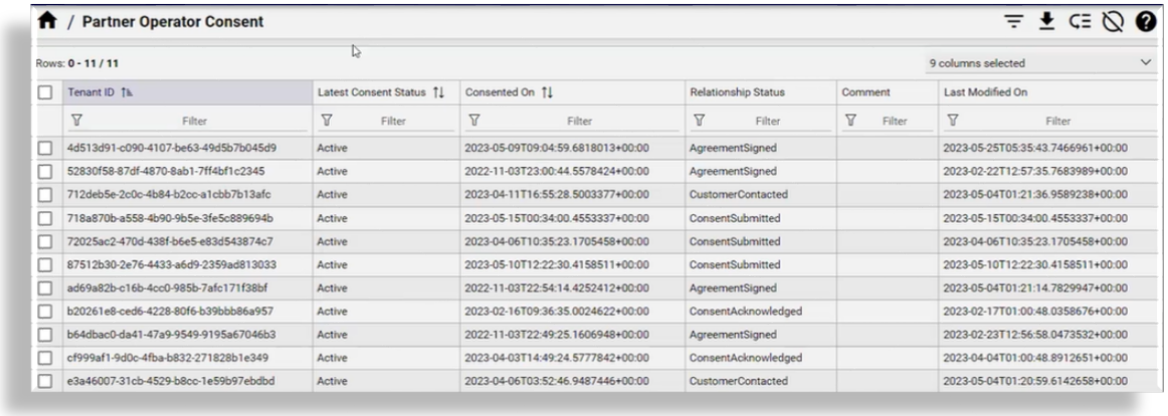
Related topics

- *Microsoft Operator Connect management in Automate*
- *Operator Connect tenant*
- *Operator Connect default data syncs*

View partner operator consents

1. Log in to the Admin Portal at the Provider or Customer level hierarchy.
2. Go to the **Partner Operator Consent** page.
3. In the summary list, view the list of existing partner operator consents:

Note: The list of partner operator consents can also be viewed via the MS Operator Connect portal.



/ Partner Operator Consent

Rows: 0 - 11 / 11

9 columns selected

Tenant ID	Latest Consent Status	Consented On	Relationship Status	Comment	Last Modified On
4d513d91-c090-4107-be63-49d5b7b045d9	Active	2023-05-09T09:04:59.6818013+00:00	AgreementSigned		2023-05-25T05:35:43.7466961+00:00
52830f58-87df-4870-8ab1-7ff4bf1c2345	Active	2022-11-03T23:00:44.5578424+00:00	AgreementSigned		2023-02-22T12:57:35.7683989+00:00
712deb5e-2c0c-4b84-b2cc-a1cbb7b13afc	Active	2023-04-11T16:55:28.5003377+00:00	CustomerContacted		2023-05-04T01:21:36.9589238+00:00
718a870b-a558-4b90-9b5e-3fe5c889694b	Active	2023-05-15T00:34:00.4553337+00:00	ConsentSubmitted		2023-05-15T00:34:00.4553337+00:00
72025ac2-470d-438f-b6e5-e83d543874c7	Active	2023-04-06T10:35:23.1705458+00:00	ConsentSubmitted		2023-04-06T10:35:23.1705458+00:00
87512b30-2e76-4433-a6d9-2359ad813033	Active	2023-05-10T12:22:30.4158511+00:00	ConsentSubmitted		2023-05-10T12:22:30.4158511+00:00
ad69a82b-c16b-4cc0-985b-7afc171f38bf	Active	2022-11-03T22:54:14.4252412+00:00	AgreementSigned		2023-05-04T01:21:14.7829947+00:00
b20261e8-ced6-4228-80f6-b39bbb86a957	Active	2023-02-16T09:36:35.0024622+00:00	ConsentAcknowledged		2023-02-17T01:00:48.0358676+00:00
b64dbac0-da41-47a9-9549-9195a67046b3	Active	2022-11-03T22:49:25.1606948+00:00	AgreementSigned		2023-02-23T12:56:58.0473532+00:00
cf999af1-9d0c-4fba-b832-271828b1e349	Active	2023-04-03T14:49:24.5777842+00:00	ConsentAcknowledged		2023-04-04T01:00:48.8912651+00:00
e3a46007-31cb-4529-b8cc-1e59b97ebdbd	Active	2023-04-06T03:52:46.9487446+00:00	CustomerContacted		2023-05-04T01:20:59.6142658+00:00

The table describes the columns on the **Partner Operator Consent** page list view:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Tenant ID	Unique tenant IDs for each of the end customers. Once the tenant ID is matched to a customer, all new or updated details for the consent is moved to the relevant customer. Each of the service provider's customers are associated with a unique tenant ID that displays in both the VOSS Automate Admin Portal and on the MS Operator Connect portal. This is the tenant belonging to the end customer, and you can use this tenant ID to onboard the customer with the Customer Build tool in VOSS Automate, and add the tenant ID to the tenant so that when you sync in data, the system associates the data with the customer's tenant ID so that the data is moved to the appropriate customer.
Latest Consent Status	Status of the latest consent.
Consented On	Date of latest consent.
Relationship Status	The currently configured relationship status, in the order history, for the consent (last synced in from the API), for example: • Consent Acknowledged • Customer Contacted - the first time the customer contacts you • Agreement Signed • Consent Declined • Contract Terminated
Comment	Notes for the consent.
Last Modified On	The last time the consent was updated.
Product Context	The product associated with the partner consent.
Located At	The hierarchy level, either Provider or Customer. Since the tenant is first added at Provider level, the first sync pulls in the consents initially to the Provider level. Once you start provisioning and adding customers, the consents are moved to the relevant customer level.
Device	

4. Click on a row in the list view to view more details for the customer and the associated partner consent.

Note: The only change you can make to a partner consent in the management page is to update the relationship status. See *Update partner operator consent*.

All other values are read-only on this page.

Copyright © 2025 VisionOSS Limited. All rights reserved.

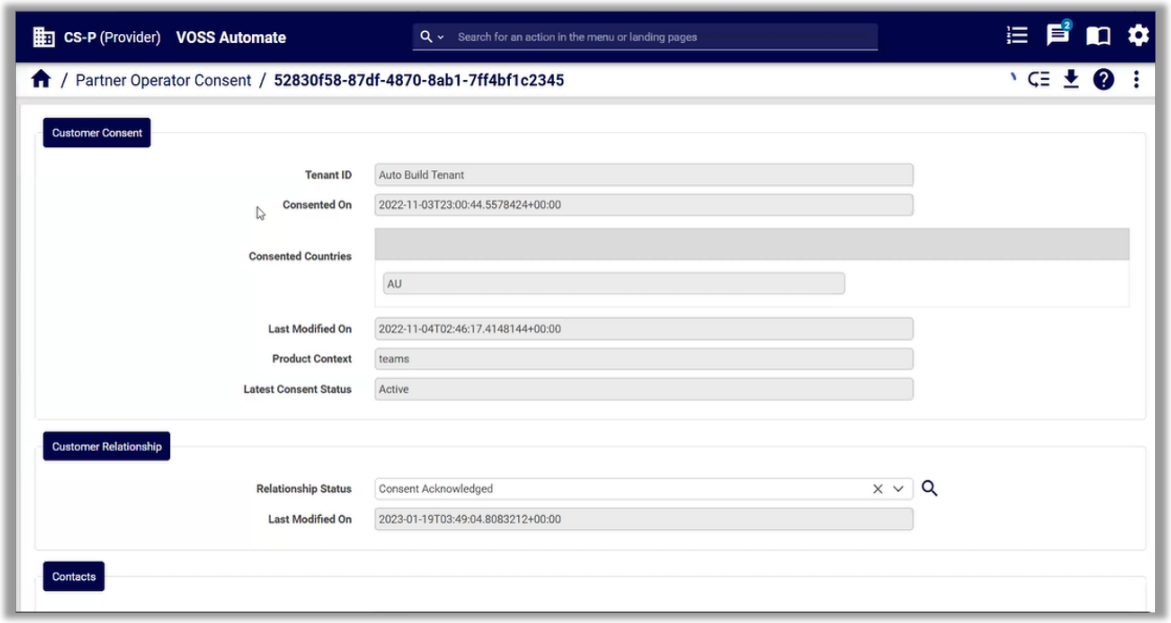
Related topics

- *Onboard customers for Operator Connect using the Customer Build Tool*

Update partner operator consent

The only change you can make to a partner consent in the Admin Portal's **Partner Operator Consent** management page is to update its relationship status.

1. Log in to the Admin Portal at the Provider or Customer hierarchy.
2. Go to **Partner Operator Consent**.
3. In the summary list, click on a relevant row.



4. Click the down-arrow at **Relationship Status**, then select a new value.
5. Save your change.

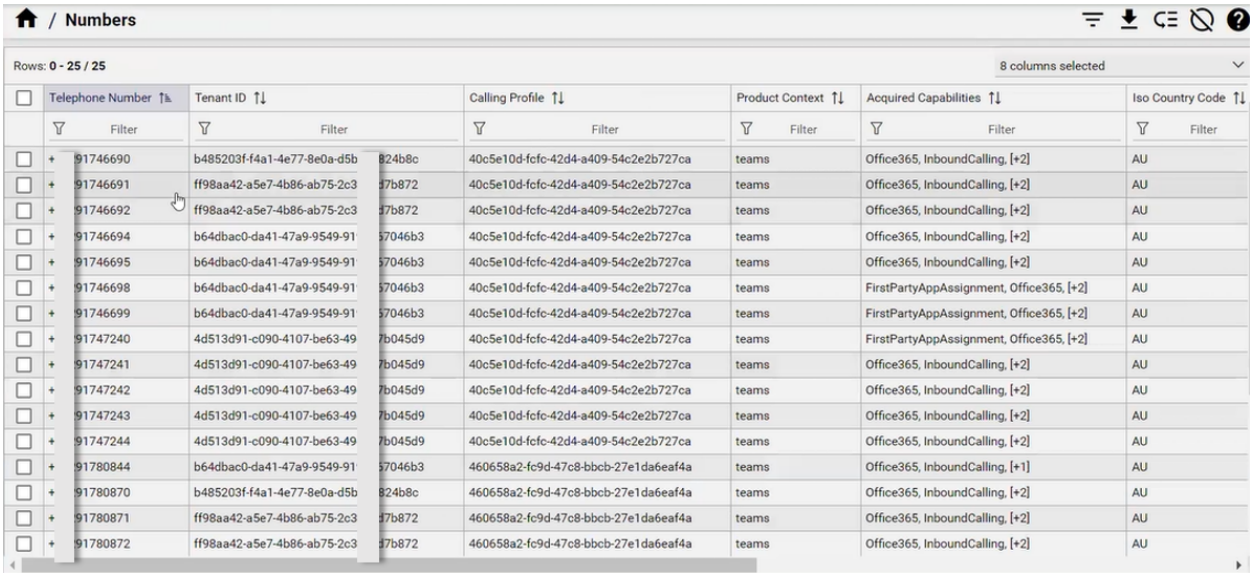
Numbers (for MS Operator Connect Tenants)

Numbers belonging to your customers are initially synced in to Automate, from the Operator Connect portal, at the Provider level. Once you add customers and start start provisioning and syncing, the numbers are moved to the relevant customers, based on their unique tenant IDs.

You can view the numbers associated with your Operator Connect customers, including the level where the numbers exist (Provider or Customer level) via the Operator Connect **Numbers** page.

Note: Automate supports import up to a maximum of one thousand (1000) numbers in total from the Operator Connect tenant.

Copyright © 2025 VisionOSS Limited. All rights reserved.



/ Numbers

Rows: 0 - 25 / 25

8 columns selected

Telephone Number	Tenant ID	Calling Profile	Product Context	Acquired Capabilities	Iso Country Code
91746690	b485203f-f4a1-4e77-8e0a-d5b824b8c	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91746691	ff98aa42-a5e7-4b86-ab75-2c37b872	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91746692	ff98aa42-a5e7-4b86-ab75-2c37b872	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91746694	b64dbac0-da41-47a9-9549-91 57046b3	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91746695	b64dbac0-da41-47a9-9549-91 57046b3	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91746698	b64dbac0-da41-47a9-9549-91 57046b3	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	FirstPartyAppAssignment, Office365, [+2]	AU
91746699	b64dbac0-da41-47a9-9549-91 57046b3	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	FirstPartyAppAssignment, Office365, [+2]	AU
91747240	4d513d91-c090-4107-be63-49 7b045d9	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	FirstPartyAppAssignment, Office365, [+2]	AU
91747241	4d513d91-c090-4107-be63-49 7b045d9	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91747242	4d513d91-c090-4107-be63-49 7b045d9	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91747243	4d513d91-c090-4107-be63-49 7b045d9	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91747244	4d513d91-c090-4107-be63-49 7b045d9	40c5e10d-fcfc-42d4-a409-54c2e2b727ca	teams	Office365, InboundCalling, [+2]	AU
91780844	b64dbac0-da41-47a9-9549-91 57046b3	460658a2-fc9d-47c8-bbcb-27e1da6eaf4a	teams	Office365, InboundCalling, [+1]	AU
91780870	b485203f-f4a1-4e77-8e0a-d5b824b8c	460658a2-fc9d-47c8-bbcb-27e1da6eaf4a	teams	Office365, InboundCalling, [+2]	AU
91780871	ff98aa42-a5e7-4b86-ab75-2c37b872	460658a2-fc9d-47c8-bbcb-27e1da6eaf4a	teams	Office365, InboundCalling, [+2]	AU
91780872	ff98aa42-a5e7-4b86-ab75-2c37b872	460658a2-fc9d-47c8-bbcb-27e1da6eaf4a	teams	Office365, InboundCalling, [+2]	AU

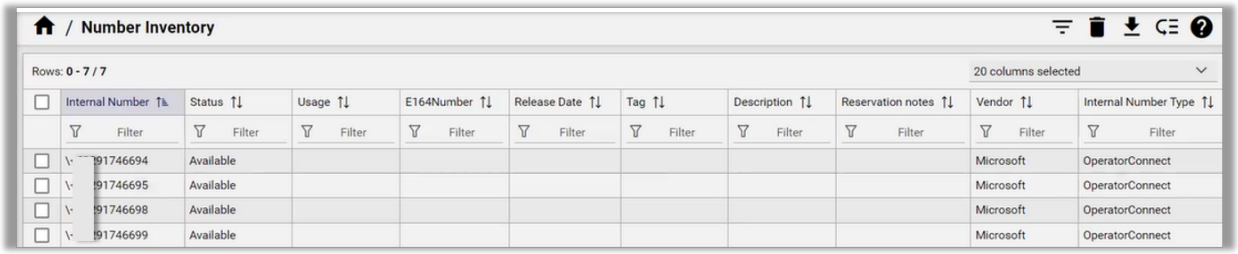
Once numbers are synced in, a number inventory entry is added to the Automate **Number Inventory**.

When adding a new number or number range (via the *Upload number range* menu) from the Operator Connect tenant, at the customer or site level:

- An inventory instance is added to the Automate number inventory (`data/InternalNumberInventory`) for each number in the range.
- If this is a new number, *or* if the number already exists in the number inventory, the internal number type on the directory number is set to “OperatorConnect”.
- No SBC provisioning occurs.

When removing a number or number range from a customer or site (via *Release number range*):

- The inventory instance for each number is removed from the number inventory, if the number is in state, *Available*.
- If the directory number is not being deleted, then “Operator Connect” is removed as its internal number type .
- No SBC provisioning occurs.



/ Number Inventory

Rows: 0 - 7 / 7

20 columns selected

Internal Number	Status	Usage	E164Number	Release Date	Tag	Description	Reservation notes	Vendor	Internal Number Type
\- 91746694	Available							Microsoft	OperatorConnect
\- 91746695	Available							Microsoft	OperatorConnect
\- 91746698	Available							Microsoft	OperatorConnect
\- 91746699	Available							Microsoft	OperatorConnect

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Upload number range*

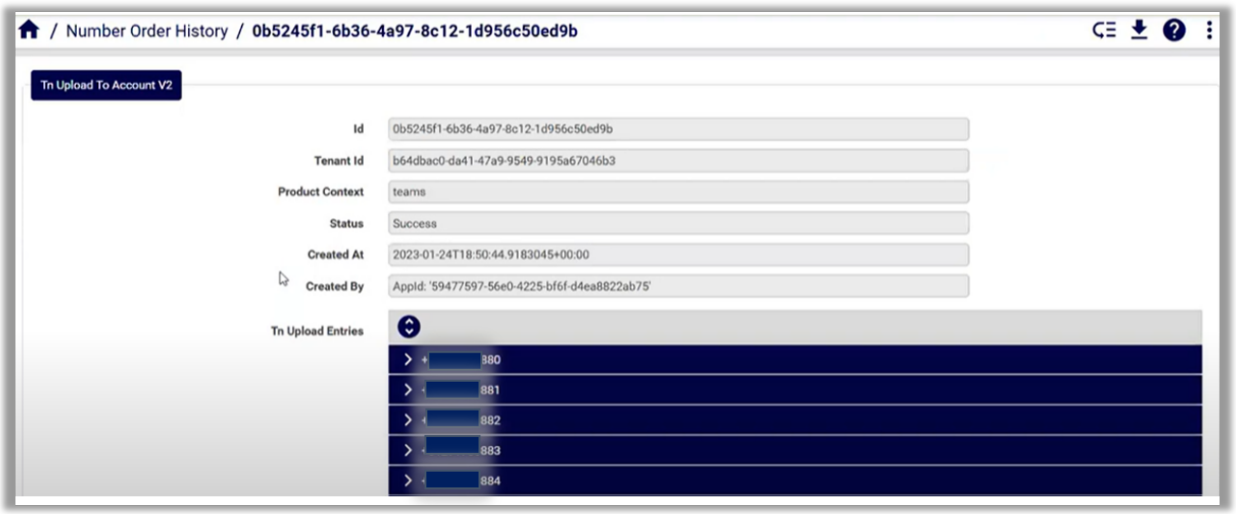
Number order history

The **Number Order History** page displays a record of the number ranges and individual numbers your customers have ordered.

You can view the number order history via the **Number Order History** page, then click on a number to view its order history details.

Note:

- In the list view, numbers are sorted in the list view from earliest to latest.
- The value for **Product Context** is read-only.



Number release history

The **Number Release History** page displays the history of numbers that have previously been released. Number release history is synced in at the Provider level until you've added customers, and started syncing and provisioning. The release history can be viewed at the relevant customer level once you add the customer and make changes in the provisioning.

You can view the number release history via the **Number Release History** page, then click on a number to view its release history details.

Note:

- In the list view, numbers are sorted in the list view from earliest to latest.
- The value for **Product Context** is read-only.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Upload number range

The **Upload Number Range** feature allows you to add a new number or new number range.

Note: Data is provided via a view that is integrated with the customer build tool. The customer build step calls the **Upload Number Range** tool to perform provisioning and ordering, and adds or updates directory numbers based on the specified range values so that SBC provisioning forms part of the customer build tool. See *Onboard customers for Operator Connect using the Customer Build Tool*.

Note: Once you start ordering numbers, you can edit the number range, if required.

Upload a number or number range

This procedure uploads a new number or a new number range.

1. In the Admin Portal, go to the **Upload Number Range** page.
2. Set the hierarchy to the relevant customer or site.
3. At the **Tenant** field, choose the customer name.

   Note: At the time of writing (for 21.4-PB2), since you're at the relevant customer level, the customer's name is the only available value to select from the drop-down. Auto-populating the **Tenant** field with the customer name is reserved for future development, so for now, you'll need to select the customer name from the drop-down.

4. Choose a calling profile.
5. At **Usage**, select the calling user assignments (one or more).

   Note: Once the number is provisioned to the end-customer, this value restricts or defines how the number can be used, for example, *Mobile* and/or *InboundCalling*, and/or *OutboundCalling*.

6. At **Start Telephone Number**, fill out the number that should be ordered, for example, *+91868416580*. If you're ordering a range of numbers, the starting telephone number should have an *X* at the end, for example, *+9186841658X*
7. At **Type of Service**, select the type of service. Options are:
   - Geographic
   - Toll Free
   - Mobile
   - No Selection
8. At **Range**, fill out the range value.

   Note: To order just one number, use *1*, or for a range of 10 numbers, beginning with the first number you specified in the previous step, use *10*, and so on.

Copyright © 2025 VisionOSS Limited. All rights reserved.

You can specify a range from 1 to 1000. For example, to order a range of 10 numbers with starting telephone number, *+9186841658X*, fill out a range value of 10, to order numbers from *+91868416580* to *+91868416589* (0-9).

9. If you're using civic addresses (for emergency calling), you can select the civic address specified on the Operator Connect tenant. Choosing a civic address associates the number with the civic address.

   Note: By default, **Allow Tenant Address Update** is enabled (set to True), which means you won't need to select a civic address ID.

   The drop-down contains valid addresses (for emergency numbers), imported from the MS Operator Connect portal for the associated tenant.

10. Save your changes to order the number/s.

    Note: The number/s you ordered:

    - Will be available on the Operator Connect portal.
    - Will display in the Automate Number Inventory, as described in *Numbers (for MS Operator Connect Tenants)*
    - Will display in the **Number Order History** list view (see *Number order history*), from where you can track it.

Related topics

- *Numbers (for MS Operator Connect Tenants)*
- *Number order history*

Release number range

The **Release Number Range** page allows you to remove a number or range of numbers.

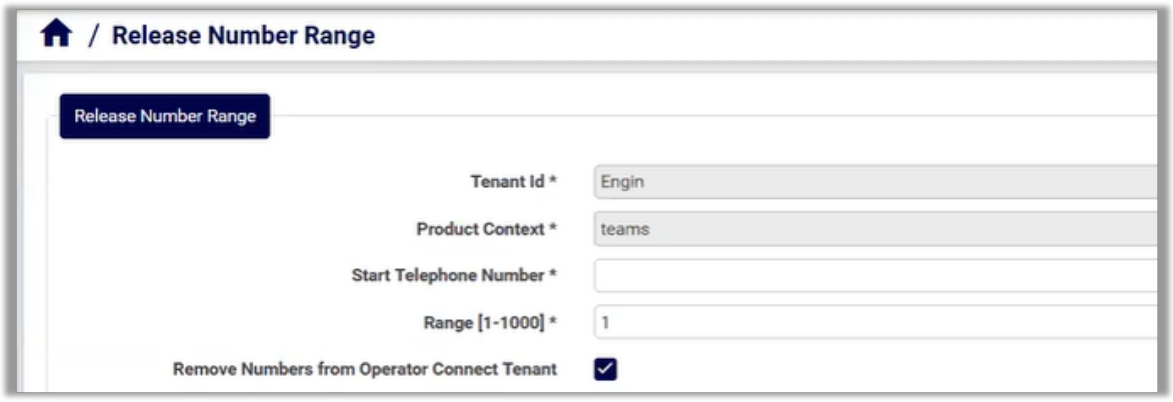
Note: Data is provided via a view that is integrated with the customer build tool. Refer to *Onboard customers for Operator Connect using the Customer Build Tool*.

Remove a number or range of numbers

This procedure removes a number or a range of numbers from a customer.

1. In the Admin Portal, go to the **Release Number Range** page.
2. Set the hierarchy to the relevant customer.

Copyright © 2025 VisionOSS Limited. All rights reserved.



3. Choose the customer name from the drop-down.
4. Fill out the telephone number you wish to remove, and the range.

Note:

- To remove one number, fill out the number, and specify range as *1*.
- To remove a range of numbers, fill out the starting telephone number, and specify a range from 1 to 1000.

---

5. At **Remove Numbers from Operator Connect Tenant**, define whether to also remove the number or number range from the Operator Connect tenant.

Note: By default, **Remove Numbers from Operator Connect Tenant** is enabled (True). When set to *False* (unchecked), the provisioning workflow skips the step to remove numbers from the Operator Connect tenant. This is required where, for example, a customer cancels their contract and is off-boarded, and their numbers no longer exist on the Operator Connect tenant. In this case, if **Remove Numbers from Operator Connect Tenant** is enabled, the transaction will fail if the workflow attempts to remove numbers that no longer exist on the tenant.

---

6. Save your changes.

   When removing a number or number range from a customer:

   - The inventory instance for each number is removed from the number inventory, if the number is in state, *Available*.
   - If the directory number is not being deleted, then “Operator Connect” is removed as its internal number type .
   - No SBC provisioning occurs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Numbers (for MS Operator Connect Tenants)*

Calling profiles

MS Operator Connect calling profiles are synced in from the Operator Connect portal, and an admin user can view the list of calling profiles at the Provider level in the Admin Portal.

Note: Calling profiles are always at the Provider level since they're associated with the service provider and not with a specific customer.

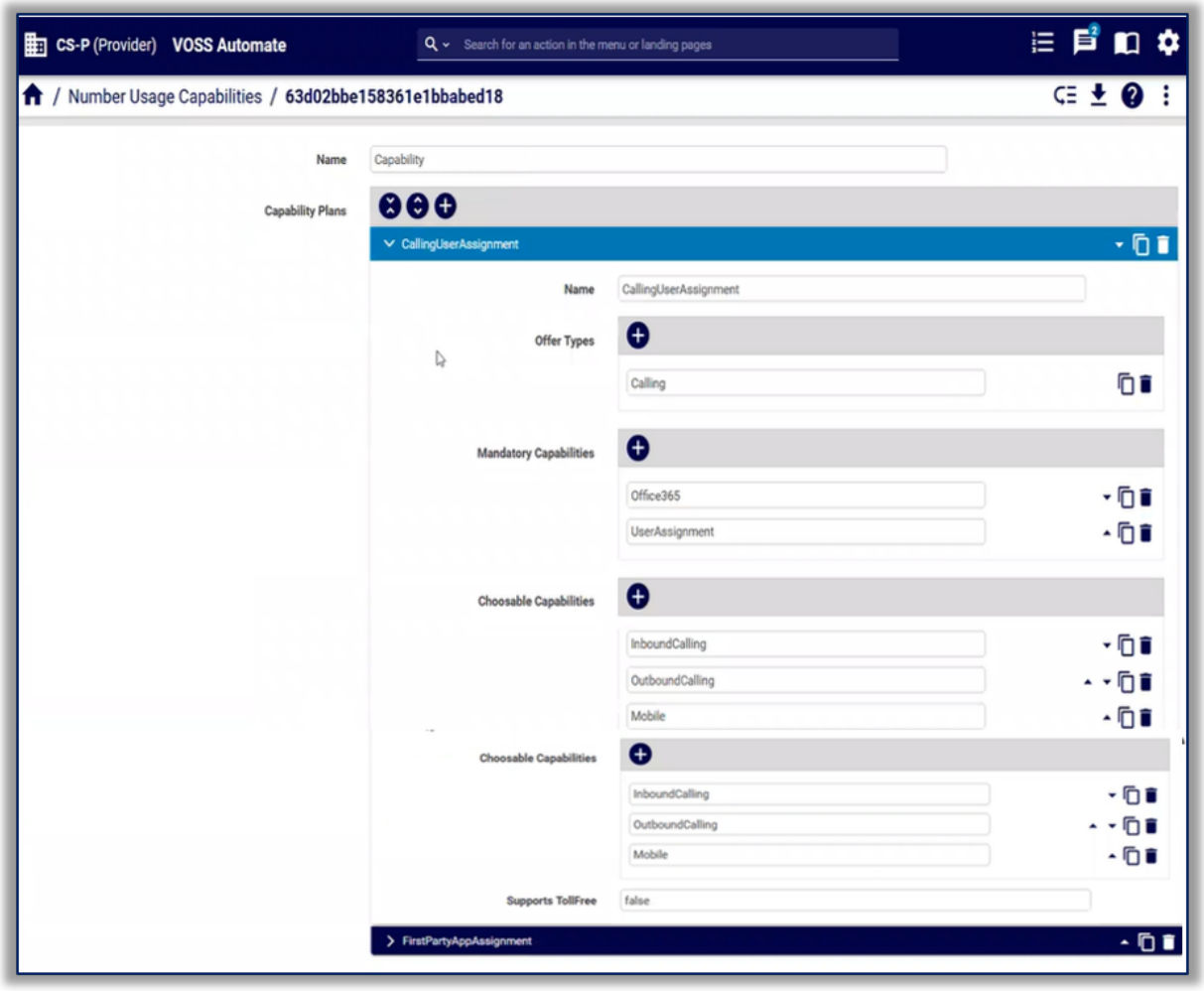
To view the calling profiles, go to the **Calling Profiles** page, then click on a calling profile in the list to view its details.

Number usage capabilities

Automate queries the Operator Connector portal to retrieve and display number usage capabilities, which are imported to, and remain at, the Provider level.

To view imported number usage capabilities, go to the **Number Usage Capabilities** page, then click on an item in the list view to inspect its details.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Onboard customers for Operator Connect using the Customer Build Tool

You can add customers for Operator Connect using the Customer Build template tool.

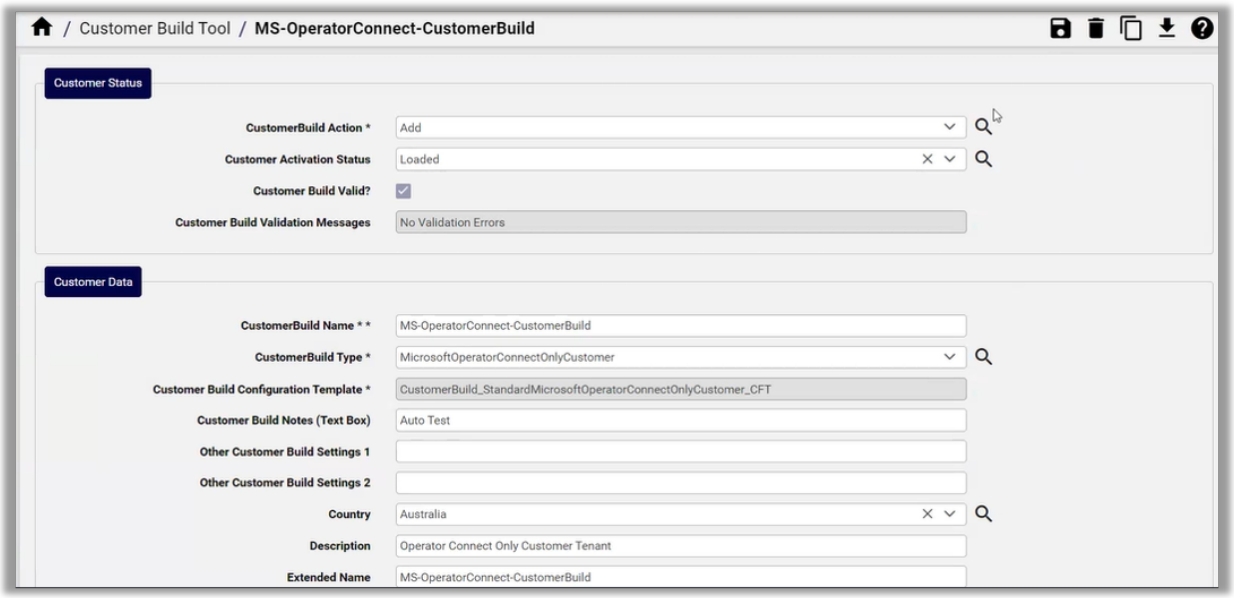
Note: Automate's Customer Build tool allows you to add and onboard customers (and their sites, if provided), with defined number ranges, or to update or delete a customer.

Using this tool, you can create a re-usable template of a customer, with all of the provisioning steps required for adding a customer, modeled in the tool. You can set up one or more customer build tools for different types of customers, depending on the provisioning requirements and the type of customer, for example, whether managed or not, or whether they're Cisco-only, Microsoft-only, hybrid, or just require number management, such as Operator Connect customers.

In the Customer Build tool, you can choose the type of customer you wish to build, fill out minimum details for this type of customer, and set up the workflow steps for provisioning.

Please contact VOSS support services if you wish to use the tool and have it exposed in your menus.

Copyright © 2025 VisionOSS Limited. All rights reserved.



To create and onboard a customer for Operator Connect:

1. Log in to the Admin Portal, and set the hierarchy to *Reseller*.
2. Go to **Customer Build**.
3. Fill out the tenant ID.
4. Select the customer build type used for Operator Connect (`MicrosoftOperatorConnectOnlyCustomer`).

   Note: The Operator Connect build type allows you to add Operator Connect-only customers, which don't need to be managed since you're only managing numbers.

   In this case, you only need to provide the Microsoft tenant name and the tenant ID (customer secrets are not required).

   If you wish to use the Customer Build tool for managed customers (direct routing customers), you can choose another customer build type, either of the following:

   - CiscoCustomer
   - MicrosoftCustomer
   - HybridCustomer
   - CallRedirectionOnlyCustomer (used for disaster recovery)

5. At **Customer Build Configuration Template**, select the customer build configuration template for Microsoft Operator Connect customers, `CustomerBuild_StandardMicrosoftOperatorConnectCustomersOnly_CFT`, which contains all the steps to allow the standard provisioning.

   Note: You can clone and customize this template, if required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. For the provisioning of numbers, add numbers and number ranges.

   Note: The SBC may be provisioned with the number ranges you specify in the **Number Ranges** fields of the customer build tool, or via the **Upload Number Range** page.

   When specifying number ranges for Operator Connect customers through the customer build tool, you can choose the default Microsoft Operator Connect usage template (`Default_OC_CallingUser_Assignment`), which contains the pre-configured number range usage requirements. This template can be cloned and customized for different number ranges, if required.

   Numbers are ordered and provisioned once you save and trigger the workflow for the customer build tool.

7. Choose a build action, in this case, Add, then save to trigger the workflow.

   The table describes the available customer build actions:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Customer build action	Description
AddDataOnly	
Validate	
Add	On-boards (adds) a new customer. Saving the customer build tool with this action selected triggers the customer build workflow, which: • Adds the tenant • Adds the customer • Uploads the selected number range to the Operator Connect tenant • Adds directory numbers (DNs) to the customer • Provisions the SBC with the numbers and appropriate routing elements. Once the workflow completes, you can: • View the new customer in the **Customers** summary list view. • Go to the **Numbers** page, then select the new customer from the hierarchy picker to view the numbers added for this customer and the specified ranges. • Go to the **Number Order History** page to view the numbers ordered for the new customer. • View directory numbers added to the number inventory for the customer and the specified range, via the **Number Inventory** page. Note that the number status remains *Available* until the numbers are assigned, and the internal number type is *OperatorConnect*.
Modify	Updates the customer. Allows the admin to add or release number ranges. In this case, the SBC is provisioned with the ordered or released number ranges, and the DNs are added or removed. For example, if the customer requires additional numbers, you can remove already provisioned number ranges and/or add additional number ranges, then save to trigger the workflow.
DeleteCustomer	Deletes the customer. The workflow is as follows: • SBC is configured to remove the number ranges belonging to the customer, as well as number ranges for released numbers. • The Microsoft Operator Connect tenant is removed. • Customers are removed, as well as any sites added for the customer.
DeletecustomerData	Removes the `relation/CustomerBuild_CustomerData_REL` instance.
DeleteCustomerAndcustomer-Data	Runs the Delete steps (as for DeleteCustomer) and removes the `relation/CustomerBuild_CustomerData_REL` instance.

The new customer is created and saved, and is added to the list of customers on the **Customers** page. The workflow for setting up the customer executes as described in the table for the *Add* build action.

The build tool template used for the customer can be viewed and updated (to add or remove numbers or number ranges, for example). Note that removing a number range via the customer build tool will de-provision

Copyright © 2025 VisionOSS Limited. All rights reserved.

numbers that were previously provisioned.

Related topics

- *Customers*

6.6. Data Sync Management - App Integration and Settings

6.6.1. Data Sync Management

This section describes general sync options, Cisco Webex Calling data syncs, Cisco data syncs (all Cisco UCM, CUC syncs), LDAP data syncs, Microsoft data syncs.

Data Syncs

Introduction to data sync

Tip: *Use the Action search to navigate Automate*

Overview

Data syncs can be performed from within Automate or directly on a device. For this reason, cached Automate data should be periodically synced with data on devices.

Examples:

- When an instance of a Cisco UCM is added to the system, its data is imported and cached.
- When instances are added, updated, or deleted from the Cisco UCM, the cached data in Automate becomes out of sync with data on the device.
- When deleting data from Cisco UCM before deleting it from Automate, the system displays the following error: “The specified resource could not be found”

  This means the resource is out of sync, and Automate may need to re-sync with Cisco UCM in order to delete it or update it.

Automate data syncs allow you to dynamically synchronize cached Automate data with data on devices. The data sync instance is associated with the connection parameters of a device type in Automate.

Supported devices include:

- Cisco Unified CM (Cisco UCM)
- Cisco Unity Connection (CUC)
- LDAP
- Webex
- MSTeamsOnline (Microsoft Teams)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- MSGraph

Individual add, update, and delete operations carried out by a data sync instance can be disabled on the user interface. If no operation is selected, the default behavior is maintained.

For Microsoft deployments, it is recommended that you enable *Prevent Duplicate Numbers* in the Global Settings to force the system to fail transactions involving workflow steps that create a copy of a number that already exists in Automate, for example, when creating a number range or when syncing in users. For details, see:

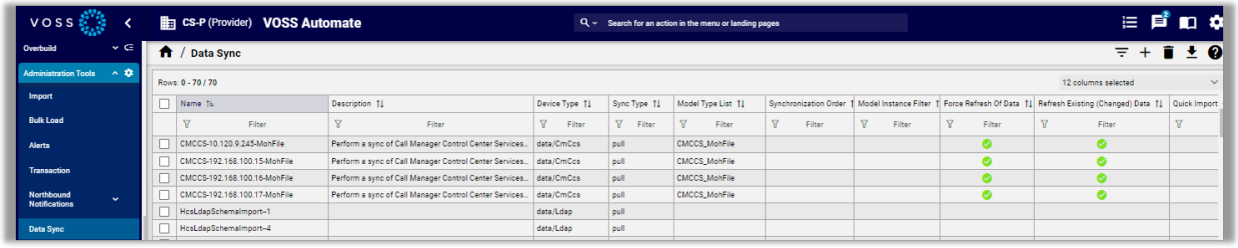
- Prevent duplicate numbers in the Core Feature Guide
- Global Settings (Number Inventory tab/panel) in the Core Feature Guide

Related topics

- Sync overview in the Best Practices Guide
- Data sync types in the Core Feature Guide
- Model instance filters in the Core Feature Guide
- Prevent duplicate numbers in the Core Feature Guide

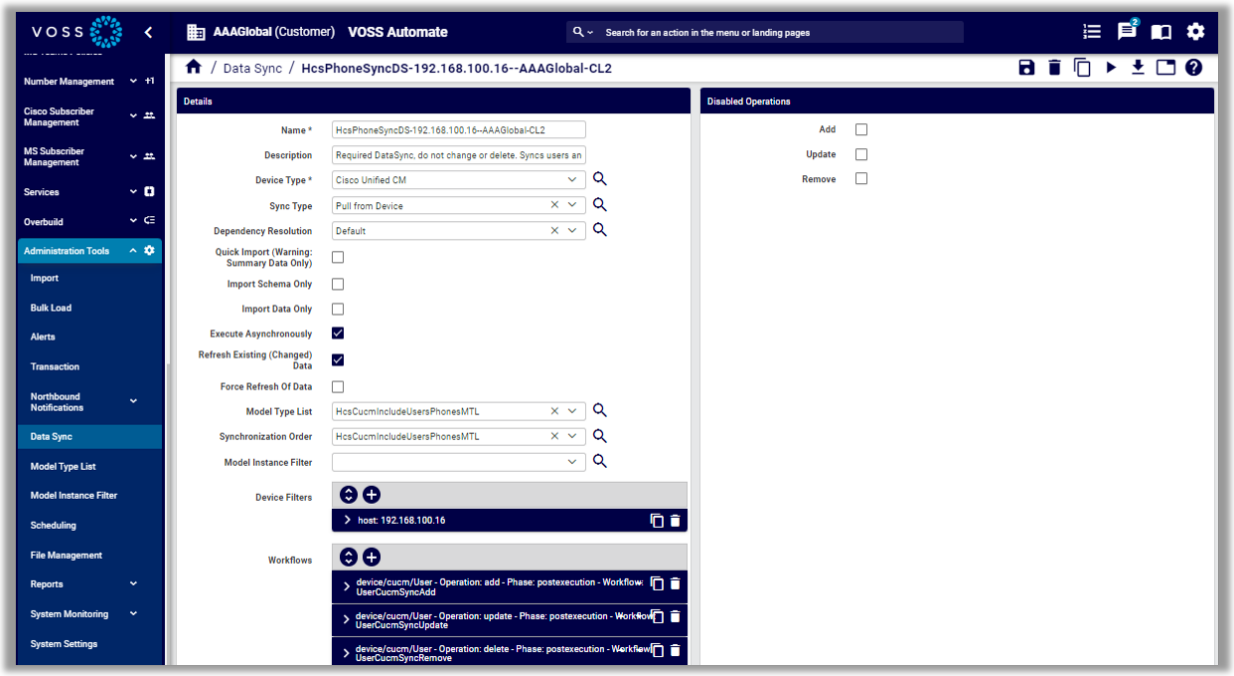
Data sync settings

To view the summary list of configured data syncs in Automate, go to the **Data Sync** page. The list view displays basic details for each available data sync, including a number of summary attributes that provide additional details about the data sync.



To view data sync settings, click on a data sync in the list to open the configuration page.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes a number of key settings that are available for data syncs:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Settings	Description
Model Type lists	Define the entities to pull in a given sync. For example: • Only pull in `device/cucm/User` records from CUCM.
Model Instance filters	Limit a sync to a subset of entities in a sync. For example: • Pull in users with a primary extension starting with *1*. A system-level administrator will need to expose this setting in the Admin Portal. • The **Purge Unmatched Records** option can be enabled to purge all Automate data that does not match the active filters during sync. This allows for a maintenance free scheduled sync that will keep the cache records in line with the filter.
Disabled Operations	Choose which operations are enabled for a sync (Add/Update/Remove). • Update requires more effort to run because this typically involves a GET API call for each record, which must then be compared to Automate data. • Add/Remove can be determined from the initial list API calls. To save time on the sync, you may wish to disable *Update* if you only require Add/Delete. From the list view of **Data Sync** entries, these fields are also available as columns (summary attributes) and can for example be used to filter the list of data syncs by the operations. **Important:** *Remove* is disabled by default if you've selected a model instance filter for the sync. You'll need to enable *Remove* if you intend for the sync to purge (remove) cache records that are excluded in the model instance filter. If you're upgrading to 21.4-PB4 from an earlier version of Automate, a migration script disables *Remove* for any syncs that have a model instance filter applied. This is to prevent the sync from unexpectedly removing a large number of records after the upgrade.
Quick Import	Uses the list API responses to update the Automate cache, and won't perform individual GET calls for each entity for the update. Recommended when the list response contains all values for the entity, or where only the key settings must be updated. Removing individual GETs speeds up the sync, since Automate is not waiting for the API responses when there are a many entities to update. This is useful if the list and GET responses are required, or if you only need the summary data from the list view. This setting is disabled by default for syncs related to *device/spark/user* syncs (*SyncSparkUsers* and *SyncSpark*). This setting is *enabled* by default for syncs related to *data/MSGraph* syncs (Syncs Microsoft License data from Microsoft Graph).

Note: *Quick Imports* can improve sync performance but must be used with extreme caution to avoid unintended changes. Typically, Quick Import is recommended only for Microsoft-related data syncs (MSOperatorConnect, MSGraph, MSTeamsOnline, MSExchangeOnline) and for Webex App/Teams-related syncs

Copyright © 2025 VisionOSS Limited. All rights reserved.

that do not include the Webex App/Teams user (device/Spark/user).

The default Full Sync instance provided for CUC also does not have **Quick Import** enabled.

Synchronous and asynchronous data sync

By default, a data sync is asynchronous; that is, other tasks can be carried out while the sync is in progress.

However, a data sync can be set to be synchronous so that a workflow step can, for example, wait for the sync process to complete.

Asynchronous imports initiated by a data sync are standalone transactions; that is, they aren't child transactions of the data sync execute transaction. Synchronous imports initiated by a data sync are children of the data sync execute transaction.

Note: By default, syncs related to *data/MSGraph* syncs (Syncs Microsoft License data from Microsoft Graph) are *synchronous*.

Data sync types

Overview

Automate provides the following data sync types:

- *Pull from Device*

  This data sync type is available to all device types:

  - Pull all data from the device
  - Pull only the schema from the device (used for LDAP)
  - Pull data from the Change Notification Feature (CNF) local data collection
- *Push to Device*: Available only to Cisco UCM devices. Push data in the cache to the device
- *Change Notification (CNF)*: Available only to Cisco UCM devices
- *Purge Local Resources*: Available only to Cisco UCM devices

Note: A quick import option is available to fetch only summary data that is contained in a list operation response and not the data for all instances/fields. See *Data Sync Overview* in the Core Guide for details.

For all sync types, Automate typically builds up the lists of entities from both Automate and the device and compares them, using the key for the device entity.

The key is typically the unique identifier (ID) for the record in the device we're syncing with. For example, for Cisco UCM, the ID is the *pkid*, which is the internal Cisco UCM database ID.

For users, a sync builds up the list of `device/cucm/Users` in Automate and then requests from the Cisco UCM the lists of users it currently has for the comparison. Differences in the lists are handled based on the sync type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Data Sync Overview in the Core Feature Guide
- Cisco UCM Change Notification Sync (CNF) in the Core Feature Guide

Pull from Device

In a *Pull from Device* sync type, the Automate resource is updated where the same key is present in both lists. In this case, the device data is the master and the Automate system model data is updated with the device data.

For example, let's say new data is added to the Cisco UCM, so that the Automate system data state for a Cisco UCM `device/cucm/User` does not show instances that are shown on the Cisco UCM.

In this case, a *pull* data sync synchronizes the system data with the Cisco UCM data. For example, a user's Department may be updated on the Cisco UCM, but the update only shows on the system after a *Pull from Device* sync. If a user resource is created in Cisco UCM but not in Automate, this adds the `device/cucm/User` instance into Automate at the level the *pull* sync was run from, for example, at the customer level.

When deleting a Automate resource from the device, so that the key is in the Automate list but not in the device list, a *pull* sync removes the resource in Automate. For example, if the resource is a user in Automate but not in Cisco UCM, the *pull* sync removes the `device/cucm/User` record in Automate.

To restrict the number of records removed in Automate, ensure you have the following named macro at the hierarchy where the sync takes place:

PULL_SYNC_DELETE_THRESHOLD_<device_type>

For details, see Pull Sync Delete Threshold topic in the Advanced Configuration Guide.

When pulling device data, for example LDAP users from an LDAP device, the results returned to Automate depend on the LDAP server configuration. For example, if the returned results exceed the LDAP server configured maximum, and if the server does not support paging, an appropriate error message is returned.

For Microsoft 365 syncs, a **Max page size** (default 1000) setting can be adjusted if the error "Template output exceeded memory limit" is shown.

For details, see *Microsoft tenant setup* in the Core Guide.

Push to Device

The *Push to Device* sync type (available only to Cisco UCM device types), synchronizes devices with the Automate system data state, which is the primary data state.

- When deleting device data from Automate so that the key is in the *device* list but not in the Automate list (for example, delete user in Automate), the user is removed from Cisco UCM. The user will not exist on the device or on Automate.
- When adding new device data to Automate so that the resource shows instances that are not shown on the device, a *push* data sync synchronizes the device data with the Automate data. For example, adding a `device/cucm/User` instance to Automate and running a *Push to Device* sync adds the user record to Cisco UCM.

Keys found in both lists are ignored. Existing records are not updated in either direction.

In the `device/cucm/User` example, if the same user exists on both Automate and on Cisco UCM, no update occurs in either direction. Detailed settings may still not match after a *Push to Device* sync.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Important: Consider data dependencies between different models when running a *Push* sync. For example, data dependencies may exist between users and phones in the Cisco UCM. In this case, if a user is associated to a phone (via the associated devices on the user), you can't add the user if the phone does not yet exist in Cisco UCM. However, for *ownerID* on the phone, pushing the phone first will fail since the user isn't in place. That may require running the *Push* sync multiple times so it loads in the required order.Alternatively, you may need to modify data (such as removing device association) to allow the *Push* sync to succeed.

Note: The keys list sync logic described in this topic implies that in case of a reversion of the Cisco UCM to restores/inactive partitions, the end-state of the relevant pkids may differ to their state the last time Automate was in sync with Cisco UCM (before a restore), particularly if testing occurred in between. This means you may, for example, have a user with the same username in both Automate and Cisco UCM, but if that user's pkid in Cisco UCM now differs to the one in Automate from previous syncs or interactions, they will be seen as different users even though they have the same usernames.

Change Notification (CNF)

The CNF sync type is available only to Cisco UCM device types.

A CNF sync type is a pull sync of changes stored in the local collection that is updated by the Change Notification Collector service.

For more details on Change Notification Sync, see the related topics in Data Sync section of the Core Feature Guide.

Purge Local Resources

A *Purge Local Resources* sync type deletes all resources or instances of device information that exists in the system are deleted. Entities in the device are not deleted.

Note: The default *purge* syncs created when adding a Cisco UCM, CUC, LDAP or CCX server type are disabled by default. To use the *purge* sync, the "Remove" check box must first be cleared on the "Disabled Operations" tab of the relevant sync.

This sync type is typically used when cleaning up the system. The system displays a warning before executing an enabled *purge* sync.

See the following sample device type syncs:

- HcsPurge-{{CUCMHostname}}–{{CUCMClusterName}}-DS
- HcsUserPurgeDS-{{CUCMHostname}}–{{CUCMClusterName}}
- HcsPhonePurgeDS-{{CUCMHostname}}–{{CUCMClusterName}}
- HcsPurge-{{CUCXHostname}}–{{CUCXClusterName}}-DS
- PurgeUccx-{{UCCXHostName}}
- HcsLdapUserPurge–{{UniqueID}}
- PurgeSpark{{CustomerName}}

Copyright © 2025 VisionOSS Limited. All rights reserved.

Full sync

A full pull sync, when it runs, empties the changes from the data collection as they don't need to be processed by the Change Notification sync. Use the disabled operations and the model type list (MTL) of the full sync to filter the changes to remove. If a model instance filter is included, no changes are removed.

It is recommended to use the `CUCXN Exclude ImportUser` MTL on Cisco Unity Connection data syncs in order to avoid unneeded data and slowing the sync time.

CUCM Models not synced by full sync (with no model type list)

- `LicensedUser`
- `LicensingResourceUsage`
- `HcsLicense`
- `CiscoCloudOnboarding`
- `RegistrationDynamic`
- `RoutePlan`
- `EnterpriseFeatureAccessConfiguration`
- `EndUserCapfProfile`

CUC Models not synced by full sync (with no model type list)

- `Handler`
- `GlobalUser`
- `LicenseStatus`
- `TenantUserLicense`
- `UserLicense`
- `SubscriberDependency`
- `ImportUser`

Manually run the default data sync

Tip: *Use the Action search to navigate Automate*

You can always manually run the default data sync when there have been updates to Cisco Unified Communications Manager (UCM) or Cisco Unity Connection (CUC) devices that need to be synced into Automate.

Note: Manually running the change notification sync is not supported.

1. Log in as provider or reseller administrator.
2. Go to **Perform Publisher Actions**.
3. From the **Action** drop-down, choose **Import**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. From the **App Type** drop-down, choose **CUCM Device** or **CUC Device**.
5. From the Clusters **Available** box, choose the device, move it to the **Selected** box, and click **Save**.

Model Type Lists (MTL)

Tip: *Use the Action search to navigate Automate*

Overview

A model type list (MTL) is a list of device models associated with the device type, for example, phone and line device models that are associated with the Cisco UCM device.

MTLs can improve sync performance as they allow you to control type of data synced in to Automate from devices from vendors such as:

- Cisco (UCM, Unity Connection)
- Microsoft
- Pexip
- Webex

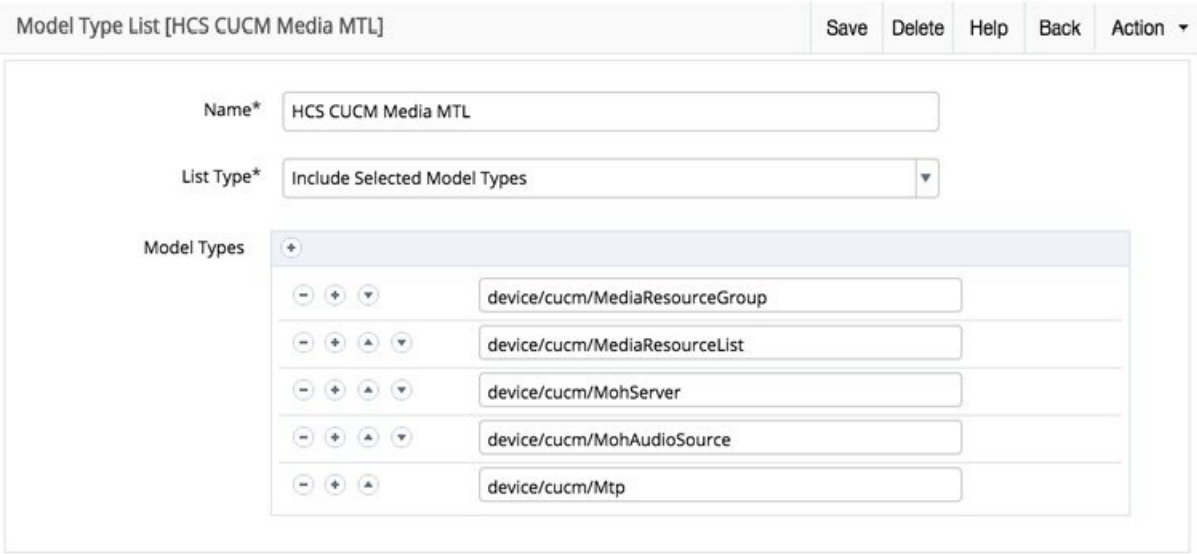
The table describes potential types of MTLs:

Model type list	Description
Include Selected Model Types	This list represents the device models to explicitly include in the data sync.
Exclude Selected Model Types	This list represents the device models to explicitly exclude from the data sync.
Ordered List	This list represents the device models to explicitly include in the data sync in the order they must be synced.

A data sync created with an empty MTL attribute results in the subsequent import(s) syncing all device models for the corresponding device.

The image shows an example of an include MTL:

Copyright © 2025 VisionOSS Limited. All rights reserved.



A data sync using this MTL will sync all Media Resource Group, Media Resource Lists, Music on Hold servers and audio sources, and Media Termination Points. No other data will be synced from Cisco UCM.

It is recommended to define MTLs for sets of data that are being modified on the device directly. An example is Cisco UCM because this is where the bulk of the configuration data for each customer resides.

By defining MTLs that target specific data sets rather than doing a full sync, the performance of Automate can be maintained with better response times and quicker transaction execution.

Note: To prevent a lengthy data sync operation due to potentially large numbers of these device models in the Cisco UCM, it is recommended that you avoid the following Cisco UCM device models, unless needed:

- Users
- Phones
- Lines

Data sync overhead can be further reduced if you want to sync only new and deleted instances of the device model and not updates to existing instances. To achieve this, clear (disable) the **Refresh Existing (Changed) Data** checkbox on the **Data Sync** configuration page. This setting defines whether existing device model instances are updated in Automate in addition to importing new instances and removing deleted instances:

- When enabled, all device model instances must be synced and examined.
- When disabled, only new and deleted instances need to be imported and the data sync will run considerably faster.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Create a targeted MTL

This procedure creates a targeted model type list (MTL).

Note: A targeted MTL and data sync is useful if you're regularly managing data on vendor devices directly - perhaps for configuration orchestrated outside of Automate (such as media resources). In this case, it is recommended that you create a MTL and data sync specifically targeting the data items you're managing. This will ensure that each data sync is highly optimized for the data being changed on the device directly, and minimizes the load on Automate.

To create a targeted model type list:

1. Log in as Provider level admin or higher.
2. Go to **Model Type Lists**, then click the Plus icon (+) to add a new record.
3. Specify the name of the model type list.

   It is recommended that you use a naming convention that makes it easy to identity the MTL in a list view, for example "Cisco UCM Media Resources".
4. From the **List Type** drop-down, choose the list type:
   - Choose **Include Selected Model Types** if the list of device models you want to sync is relatively short.
   - Choose **Exclude Selected Model Types** if the list of device models you want to sync is relatively long. Exclude device models that tend to have lots of instances (like users, phones, and lines in Unified CM).
   - Choose **Ordered List** if the list of device models you want to sync is relatively short and the order in which they are synced matters.

   Note: A data sync will fail if the **List Type** of the model type list does not match the **Device Type** of the data sync.

   ---
5. Add model types to the list of device models that are to be included or excluded according to the **List Type** selected.

   See *View list of device models* for information on how to see a list of available device models for vendor devices.
6. Click **Save**.

View list of device models

This procedure displays the device models available to use in model type lists (MTLs) for custom data syncs from vendor devices.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Option A:

1. Log in on the VOSS Customer Portal [`https://voss.portalshape.com`].
2. Select the **Documentation & Resources** menu.
3. Access the API Reference from the documentation release landing page.
4. Inspect the list of devices available from the *Model Index* link in the reference to obtain device model names.

Option B:

1. On your system, open the URL: `https://<IP>/api/choices/?format=json`
2. From the returned list, identify the device model with `device/` in the endpoint, for example `device/cucm/BillingServer`.

Next steps

When including the device model in a MTL, use the format `device/<device_type>/<device_model>`, for example, `device/cucm/BillingServer`.

Create a custom data sync

Tip: *Use the Action search to navigate Automate*

Create a custom data sync to use a targeted model type list.

1. Log in as provider admin or higher.
2. Go to the **Data Sync** page.
3. Click the Plus icon (+) to add a new record.
4. Fill out a name for the data sync in the **Name** field.

   It is recommend to use a naming convention that makes it easy to identify the data syncs in the list view, such as C1Pull-CUCM01-DS, where:

   - C1 is the customer name
   - Pull is the data sync type
   - CUCM01 is the name of the Cisco UCM
   - DS is the acronym for *Data Sync*

   You could also include the type of data included in the sync, such as *C1Pull-CUCM01-MediaResources-DS*.
5. From the **Device Type** drop-down, choose the device type you're syncing from.
6. From the **Sync Type** drop-down, choose **Pull from Device**.
7. From the **Dependency Resolution** drop-down, choose **Default**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8. Select the **Execute Asynchronously** and **Refresh Existing (Changed) Data** checkboxes.

   Execute Asynchronously means that the sync request will return a reply before it's complete when executed from the API. *Refresh Existing (Changed) Data* means that all instances of the device models specified in the model type list will be updated.

9. Select the **Force Refresh of Data** checkbox if a data update is required regardless of whether data has changed on the device. This option would for example be used if it is required that update workflows be run upon a data sync.

10. From the **Model Type List** drop-down, choose the targeted model type list you defined earlier.

11. Leave **Synchronization Order** and **Model Instance Filter** blank.

12. Click the Plus icon (+) adjacent to **Device Filters** to add an entry to the list.

    a. From the **Attribute Name** drop-down, choose **host**.

    b. From the **Condition** drop-down, choose **Equals**.

    c. From the **Value** drop-down, choose the hostname/IP address of the device.

    Note: Workflows can be added to, and executed by a custom data sync to perform specific data sync operations.

13. In the **Workflows** section, include workflows in the custom data sync if you want to perform specific data sync operations, otherwise leave the **Workflows** section empty. For example, if you want to move remote destinations from the customer hierarchy level to the site level, choose the **RD_Overbuild_PWF_wrapper** workflow from the **Workflow** drop-down.

    If the **Synchronous** checkbox is enabled, the workflows will execute in sync with data sync transaction, so that the parent pre- and post workflow steps are honoured. If disabled, the workflows will not be child transactions of the data sync execute transaction.

14. From the **Transaction Log Level** drop-down, choose the log level for the data sync. For a description of the list of log levels, see *Transaction log levels*. The default log level is *Warning*.

    You can for example reduce the log level for PULL device syncs in order to reduce the size of transaction logs. This is useful where large numbers of transactions are archived regularly.

15. Click **Save**.

Next steps

To run the custom data sync, click the data sync from the **Data Sync** list and click **Execute**.

Schedules

Sync scheduling

Sync scheduling involves scheduling actions to take place at a specified time, or to repeat.

Currently, the action is to *execute*.

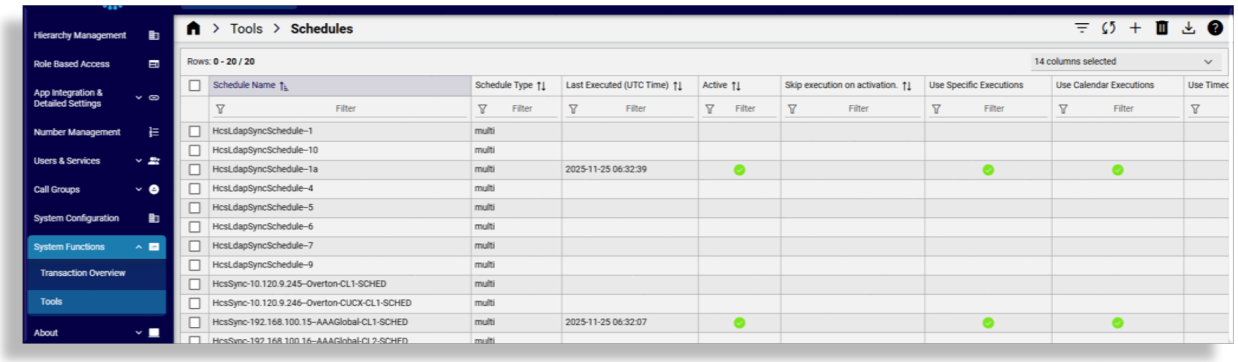
Single or multiple actions can be executed on one or more resources:

- **Data Sync**
- **Script**

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Provisioning Workflows**
- A schedule can be created during the Bulk Load process. Bulk loaded files that are not set to Execute Immediately can be scheduled by Execution Date, -Time and -Timezone. A scheduled bulk load is shown on the Schedule as a **Single Execution** schedule type and with the Resource Type as **data/BulkLoad**.

Care should be taken when transactions are scheduled. For example, data syncs should be scheduled outside of peak times. The size and scope of the transactions that run determine the length of the time that they need to run. This therefore impacts on the start time. The number of clusters on the system and their size need to be considered as part of a data sync approach.



Related topics

- Schedule dashboard export report in the Core Feature Guide

Best practice for scheduling syncs

- Avoid too many overlapping syncs at a given time. The system already blocks multiple syncs against a given device.
- The best practice is to not have more than five syncs running at a given time.
- To avoid load and issues with concurrency, schedule syncs carefully and at intervals when they are really required. For example, do not run nightly syncs unless it is necessary. Since syncs generally cover the case where information is changed on the UC apps outside Automate, the level of third party integration or direct configuration tasks should play a role in the decision to schedule. For details, refer to the topics on Cisco UCM, CUC and LDAP below.
- Since it is possible to limit the number of records processed with a given sync, more predictability can be obtained with scheduling.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Enable a scheduled data sync

Tip: *Use the Action search to navigate Automate*

This procedure enables the scheduled data sync so that it executes regularly.

Note: Setting up a Cisco UCM or CUC device in Automate:

- Creates a full pull data sync instance, which will perform the initial sync of all data from the device. It is recommended that you manually run the full pull data sync only when necessary.

  See Manually run the default data sync in the Core Feature Guide
- Creates a Change Notification Sync type (on the Data Sync page). Manually running the change notification sync is not supported.
- Creates a scheduled data sync (disabled by default) to execute a data sync every 14 days. This topic describes how to enable this regular sync.

Enable the scheduled data sync

1. Log in as provider administrator.
2. Go to the **Scheduling** page.
3. Choose the schedule instance that matches this naming convention: `HcsSync-<ip_address>-<device_name>-SCHED`

   For example: `HcsSync-192.0.2.24-CUCM01-SCHED`
4. Select the **Active** checkbox.
5. On the **Multiple Executions** tab, update the interval, as required.
6. Click **Save**.

   The full data sync executes immediately, and executes again according to the schedule.

Add or edit a schedule

Tip: *Use the Action search to navigate Automate*

This procedure displays and edits existing schedules, and adds a new schedule.

Note: Automate also provides a tool to deactivate and reactivate schedules in bulk, if required.

See Bulk Schedule Activation / Deactivation in the Core Feature Guide

1. Log in to the Admin Portal and select the relevant hierarchy.
2. Go to **Sync Scheduling** to open the list view.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. View existing schedules in the summary list view, which includes a number of attributes for each schedule.

   Note: Resource attributes are used for filtering when you want to choose a resource.

4. Choose an option:
   - To edit a schedule, click on the relevant schedule to open its configuration page. Make the changes you require, then click **Save**.
   - To add a new schedule, click the Plus (+) icon to add a new record. Go to the next step to configure the schedule.
5. Configure the schedule.

   The table describes sync schedule settings on the **Details** tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Schedule Name	The name of the schedule.
Last Executed (UTC Time)	Read-only. Displays the last time this schedule executed.
Owner	The schedule owner. The user who created this schedule. Read-only for existing schedules.
Schedule Type	Mandatory. Select the schedule type. Either Single Execution or Multi Execution. See below for the configurable settings for either single execution or multi execution.
Active	This checkbox defines whether the scheduled sync is enabled (active) or disabled. Clear the checkbox to disable the sync schedule. If you're enabling the sync schedule and there is a "next execution" in the past, the sync executes immediately when you save. To prevent the execution of this past sync schedule, select **Skip execution on activation**.
Skip execution on activation	Prevents the execution of a "next execution" in the past if you're choosing to enable the schedule now. Selecting this option prevents a situation where, for example, you wish to pause the execution of scheduled syncs for a period, perhaps to perform an upgrade. Post-upgrade, when activating the schedule, a number of pending syncs may execute immediately. This setting clears pending scheduled syncs so that the schedule executes again only at the next scheduled execution time, after the schedule is set to "active".
Scheduled resources	Mandatory. Displays only when **Active** is selected. Adds one or more scheduled resources. Configure the following: • Click the Plus icon (+) to add a scheduled resource. • Select the action, typically, Execute. You can schedule one or more actions or one or more resource types, and choose resource attributes for each. • Choose the resource type (resources that can be executed, for example, `data/DataSync`). • Choose the resource attribute to filter on when choosing the resource type, which is typically `name`. • At **Resource**, select the value of the resource attribute. For example, if the attribute is `name`, then the name of the resource. • At **Perform Action**, define whether to enable or disable the resource scheduled action.

The table describes sync schedule settings on the **Multiple Executions** or **Single Execution** tab/panel. The tab/panel that displays depends on the option selected for **Schedule Type**:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Schedule Type	Settings
Single Execution	• At **Execution Date and Time**, choose a date and time from the calendar date/time picker. • Choose the execution timezone.
Multiple Executions	Choose one or more of the following options: • Use Specific Executions • Use Calendar Executions • Use Timed Executions Configure settings for the options you selected. When choosing two or more options, the first scheduled time takes priority. If a schedule is in a state where the last executed and next execution time are equal, the next execution time is recalculated to ensure its execution.

6. Click **Save** to create (or update) the schedule.

   The schedule you added (or updated) displays in the **Scheduling** list view.

Model instance filters

Tip: *Use the Action search to navigate Automate*

Overview

Model instance filters (MIF) allow the administrator to provide criteria to define a subset of model instances to sync in. This causes the sync to only sync in those instances matching the criteria instead of all the instances.

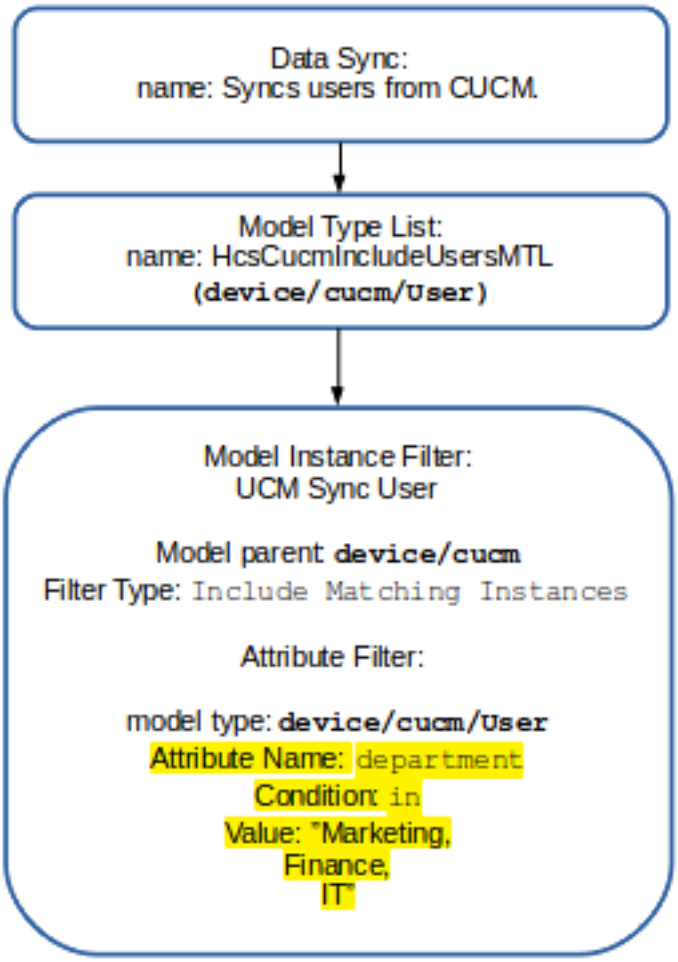
A data sync can be set up with reference to:

- The device that is the sync target
- A set of data in the form of a model type list, which also defines the sync sequence of the models in this list
- Model instance filters of the models in the list - to provide more specific filtering of specific instances of the models to sync

Note: When using a model instance filter with a data sync, the ability of the sync to remove (purge) records is disabled by default to prevent the unintentional removal of records that are excluded by the model instance filter. You'll need to enable *Remove* if you intend for the sync to purge cache records that are excluded by the model instance filter. See *Introduction to data sync*

If you're upgrading to 21.4-PB4 from an earlier version of Automate, a migration script disables *Remove* for any syncs that have a model instance filter applied. This is to prevent the sync from unexpectedly removing a large number of records after the upgrade.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Add a model instance filter

1. Log in as a Provider level administrator, then go to **Model Instance Filter** to open the list view of existing model instance filters at the corresponding administrator hierarchy.
2. Click the Plus icon (+) to add a new model instance filter.
3. Fill out a name for the new model instance filter.
4. From the **Model Parent** drop-down, choose the device or model type. The filter will be applied to it.

   Note: A data sync will fail if the **Model Parent** of the Model Instance filter does not match the **Device Type** of the Data Sync.

5. Choose the type of filter - the inclusion or exclusion of attributes: **Include Matching Instances** or **Exclude Matching Instances**.
6. Add one or more filters in the **Model Filters** group:
   a. Choose the **Model Type** that belongs to the **Model Parent**.
   b. Add one or more attribute filters in the **Attribute Filters** group:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **Attribute Name** should be selected after inspecting list request responses in the Transaction log - refer to the note below.
- Choose its **Condition**.

  For **In** and **Not In**, if the field specified turns out to be an array, then "in" means there is an overlap between the field value and the value it is being checked against. For example, "lines in <an array of lines>" is comparing an array to an array.

  The **Like** condition is a regular expression match, so in any regex should work here, but a very basic usage of regex is a "contains" type functionality, for example, "username like fred".

  Note: Automate issues a warning when it detects an `in` condition for `UserPrincipalName` used alongside other `CsOnlineUser` filters during sync and filtering. In Microsoft tenants with auto-filter enabled, the expected records may not be returned if your MsolUser cache is not up to date.

- Provide a **Value** to filter on.

  It is often better (frequently faster) to try and use a built-in **Condition** rather than resorting to macros in the **Value** that needs to be matched on.

Filter criteria can be set up according to your purposes:

- Multiple **Model Type** entries are treated as an OR condition; creating a list of criteria. Any records matching any of the entries will result in a match. This is useful when defining criteria for different model types, for example, criteria for user records and different criteria for phone records. It is also useful for defining multiple criteria on the *same* model type and attribute, for example, multiple entries for `device/cucm/User` model type where the attribute of `userid` for example matches different macro-based conditions.
- Multiple **Attribute Filters** - attribute criteria for a model type are treated as a logical AND condition and entries need to match *all* the criteria in order to meet the condition. This is useful when creating criteria that match multiple different attributes of the model type, for example, match a user that has a matching `userid` as well as a matching `department`.

7. Click **Save**. The filter can be selected from the **Model Instance Filter** drop-down when creating or modifying a Data Sync.

Note:

- If the filter is added at a hierarchy level *below* that of the the Data Sync, executing the Data Sync will fail, displaying a message "Model type list <ModelTypeList> not found at or above the current hierarchy.".
- In order to identify the **Attribute Name** of the model that can be used for a filter, inspect the transaction log for a list request of the model from the device.

  For example, in order to find the available Model Instance Filter attributes of `device/cucm/UserProfileProvision`, inspect the response from a list request from the device.

  From the RESPONSE snippet below, it can be determined that the attributes available for filtering are:

  - name
  - description
  - allowProvision
  - limitProvision

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
</ns0:listUserProfileProvision>
</soapenv:Body>
</soapenv:Envelope>

RESPONSE:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <ns:listUserProfileProvisionResponse xmlns:ns="http://www.cisco.com/AXL/API/11.5">
      <return>
        <userProfileProvision uuid="{96FA39CD-8A29-4B26-A3F5-0FF683326134}">
          <name>Standard (Factory Default) User Profile</name>
          <description>Standard (Factory Default) User Profile</description>
          <allowProvision>false</allowProvision>
          <limitProvision>10</limitProvision>
        </userProfileProvision>
```

Common use of model instance filters

While model instance filters can be used on any sync type, their common uses are:

- Add syncs - to retrieve a subset of records from the underlying device into Automate. For example, to limit the users pulled from LDAP, from UCM, and so on.
- Remove/purge sync - to target specific records for removal in a purge or delete sync. For example, to purge a subset of users from Automate that were inadvertently pulled in.

  Note: When using a model instance filter with a data sync, the ability of the sync to remove (purge) records is disabled by default to prevent the unintentional removal of records that are excluded by the model instance filter. You'll need to enable *Remove* if you intend for the sync to purge cache records that are excluded by the model instance filter. See *Introduction to data sync*

Note: Model instance filters do not work with CUCM Change Notification sync types. If a model instance filter is needed for a CUCM element, this model type should be excluded from the change notification sync and a separate sync should be se up for this.

Macro functions in model instance filters

Macro functions can be used in the **Value** field to define matching criteria. This is particularly useful for "contains" matching, for example, using `fn.contains` or `fn.containsIgnoreCase`.

The value read in from the device API call can be referenced using the input context and the field name from the API call (for example, `input.telephoneNumber`).

For example, the **Value** field can have:

- for `fn.contains`:

```
((fn.contains Dublin, input.description == True)) <{{input.description}}>
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

This `fn.contains` function will search as *case sensitive*, and in the example will only match where the description field contains the word "Dublin".

- for `fn.containsIgnoreCase`:

```
((fn.containsIgnoreCase +27,input.telephoneNumber == True)) <{{input.telephoneNumber}
↪}>
```

You can also use a named macro (e.g. `macro.ZA-number`), that has the macro above in the **Value** field instead, so that:

- **Model Type**: `device/cucm/User`
- **Attribute Name**: `telephoneNumber`
- **Value**: `macro.ZA-number`

This condition will sync every user with a telephone number that includes `+27`.

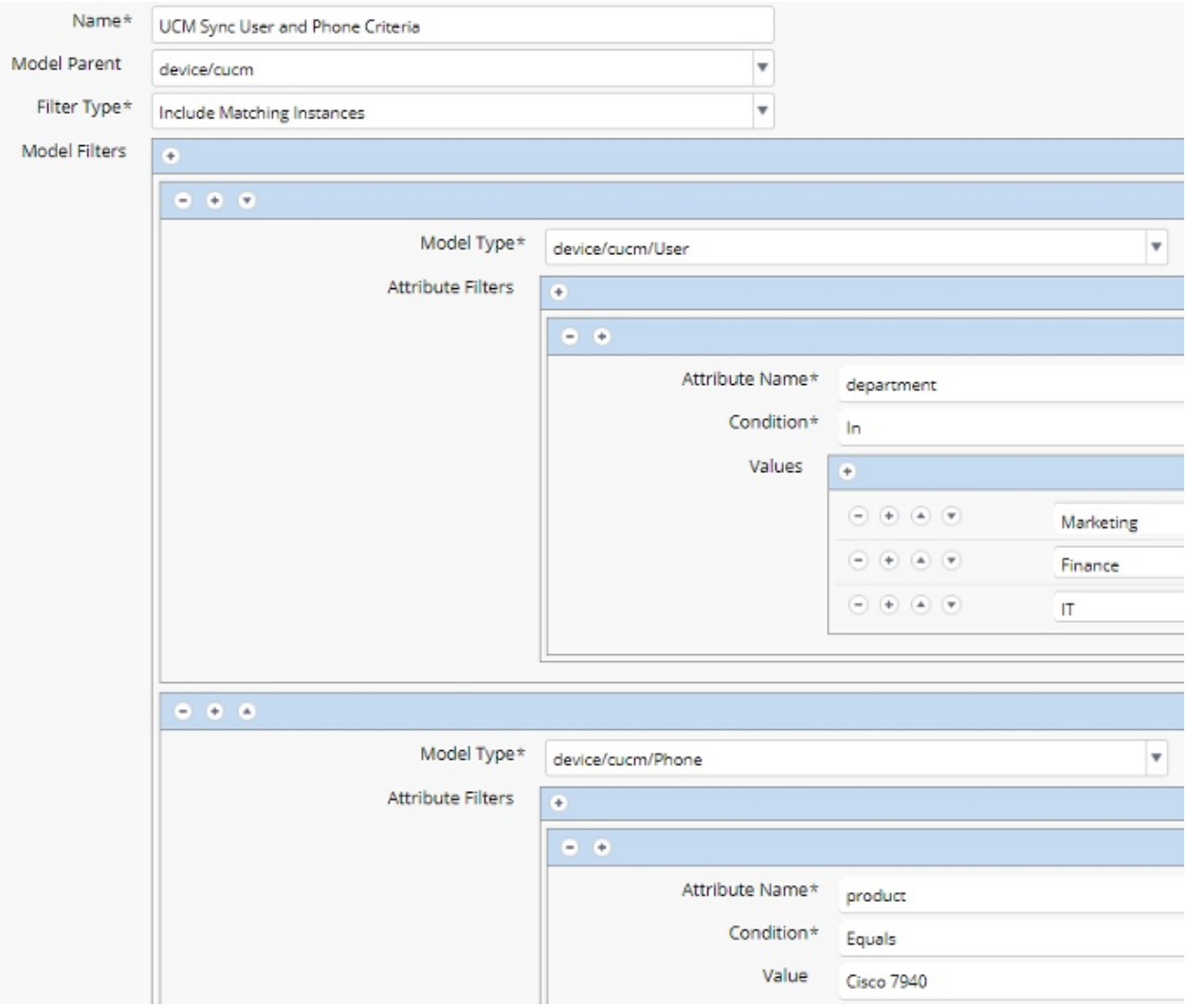
Macros cannot be used in the **Value** field in conjunction with the "in" **Condition**.

Model instance filter examples

This section describes a few examples for using model instance filters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

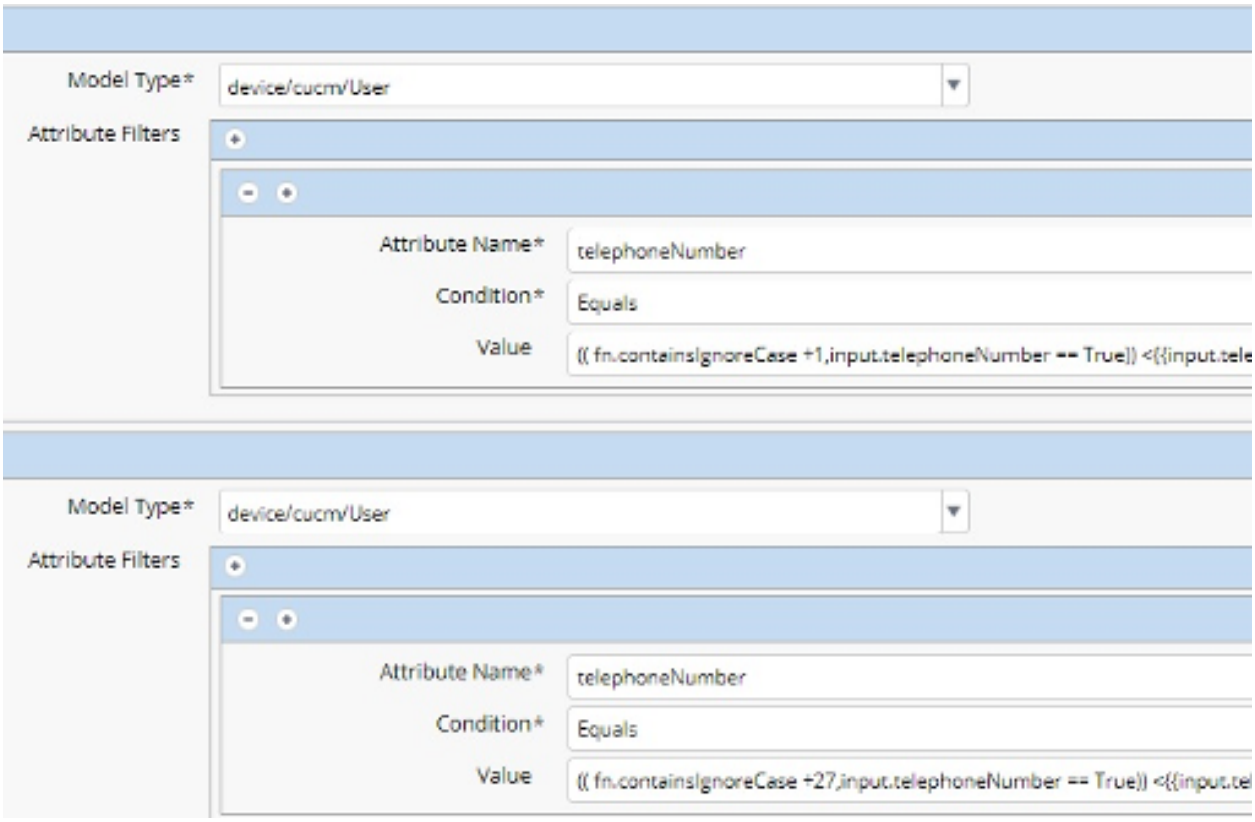
Model instance filter with multiple model filter entries to match criteria on different model types:



This model instance filter will result in: looking at `device/cucm/User` records it will match users that have a department of Marketing, Finance, or IT (due to the IN condition). When looking at `device/cucm/Phones` it will match phones of the type “Cisco 7940”.

Copyright © 2025 VisionOSS Limited. All rights reserved.

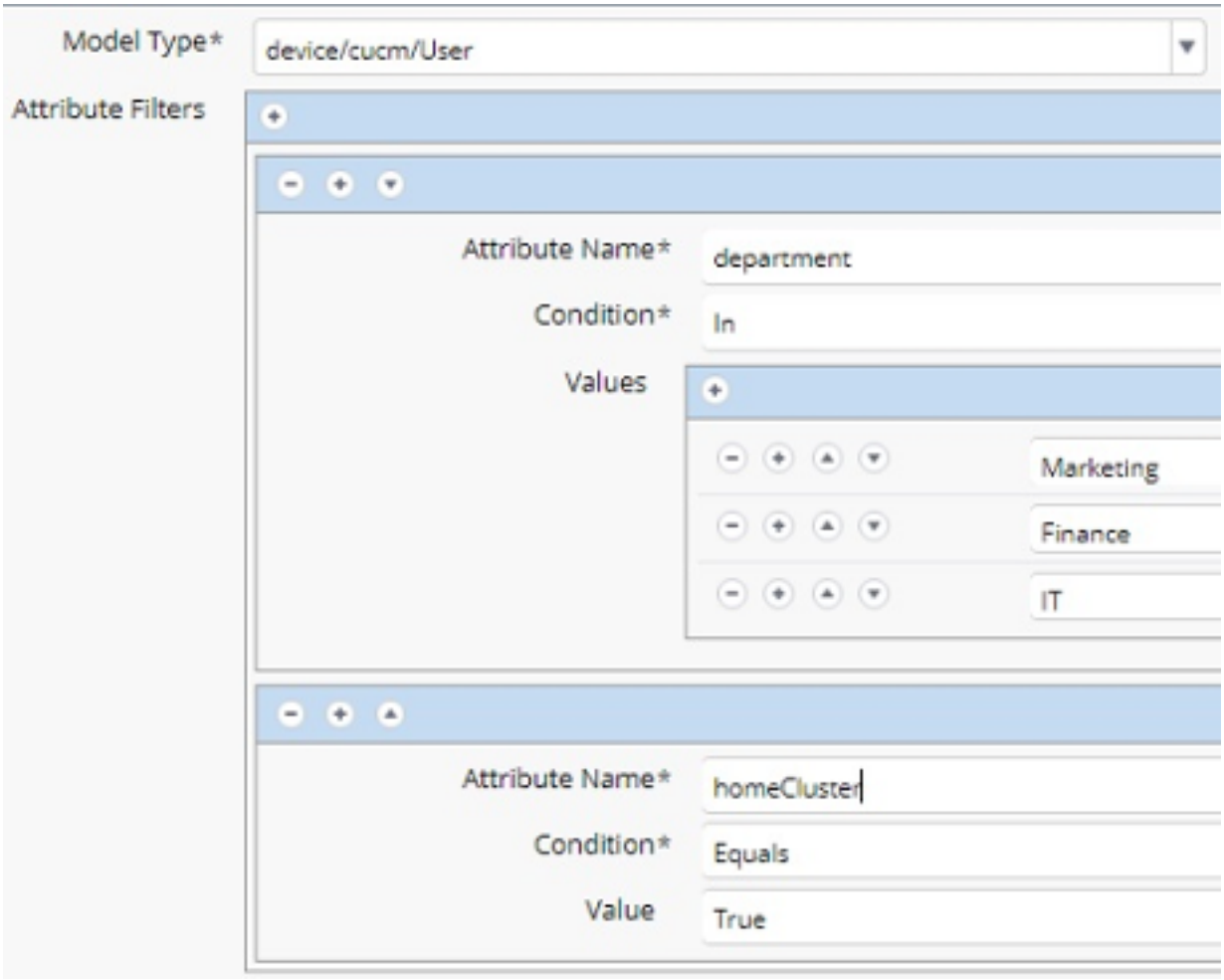
Model instance filter with multiple model filter criteria entries with the same model type and macros to create a list of records to match



For this example, when looking at the `device/cucm/User` records it will match users that have a telephone number containing `+1` OR `+27`. The macro in the value field is cut short but it's using the macro in the notes above for reference. Due to the macros in use in the value, this had to be done as multiple model filter entries instead of a attribute filter using the IN condition.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Model instance filter with multiple attribute filters applied to the same model type



When looking at the `device/cucm/User` records it will match users that have a department matching Marketing, Finance, or IT, AND has the home cluster flag set to true.

Default Cache Control Policy

A default Cache Control Policy is applied to manage the caching behavior of the system, in other words, it controls how data is read.

The defaults are set as follows:

- Cache Policy for Reads: read from cache then device
- Read Before Write: On Update
- Read After Write: On Add
- Read After Write: On Update
- Model specific overrrides:
  - Model Type: `device/notification_service/*`
    - Cache Policy for Reads: Cache

Copyright © 2025 VisionOSS Limited. All rights reserved.

The following concepts apply:

- Cache only: Unless overridden within the request, instance reads via the API always return the cached version of data. There is no need for the client to query the uncached instance data.
- Cache then device: The API will return the cached data, the Admin Portal will indicate that the data shown is cached and will automatically make an API call requesting non-cached data. It is up to external clients to query the data requesting non-cached data. If this option is selected, data is loaded into the system in two steps:

  1. Load cached data
  2. Load device data

  The 'cached' visual indicator is displayed until the second step is complete.

  The device data overrides the previously displayed data unless the user has made an input:

  a. The fields changed by the user will reflect the user's input and not the device data.
  b. Arrays are blocked for the duration of the device data loading (while the 'cached' flag is displayed) and the user can not add or remove elements until the device data loading completes.

  Data is validated constantly as displayed values change, and validation status always reflects the very latest state.
- Manual: Unless overridden within the request, instance reads via the API always return the cached version of data. An external client using the API needs to provide a button to allow the user to manually retrieve non-cached data.
- No cache: Unless overridden within the request, instance reads via the API always return the uncached version of data that is queried from the device. In this mode the Admin Portal will not show any data until it is retrieved from the device.

For Relation model types, the relation's cache control policy will filter down to the joined device models. For example:

- If the cache control policy of a Relation is Cache then Device, any GET operations that do not specify the cached parameter will return a cached result. It then becomes the client's responsibility to make another request with `cached=false`.
- If the cache control policy of a Relation is Cache only or Manual, then any GET requests that do not specify the cached parameter, return cached data for all joined models.
- If the cache control policy on read is No cache, the Relation will always fetch the latest device data.

Allowlists and denylists

sys-admin

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate supports allowlists and denylists to specify parameters that cause the workflows attached to your data sync to run. These are defined via the system **Global Settings**; typically available to sysadmin users in the system.

Allowlists and denylists specify the fields on the device model that trigger workflows attached to a sync, when they change. The allowlist defines the fields that will trigger the workflow when they change, while all other fields are ignored. The denylist indicates the fields that will be ignored if they change, and won't trigger the workflow.

Note: Allowlists and denylists affect "Update" workflows only, and are used to prevent unnecessary "Update" workflows from triggering on data syncs.

Workflows for "Add" or "Delete" are triggered regardless of any allowlist or denylist entries.

The allowlist takes priority over the denylist if both are defined for the model; thus, choose one approach or the other. The recommendation is to use allowlists, as these are more explicit regarding the fields that will trigger the change. Regardless if a workflow is running or not, the model is updated in Automate, so the changed field is pulled in - it just will not initiate a workflow to do anything further (e.g update `data/User`).

The system ships with a number of predefined allowlists and denylists, which provide a starting point for optimized syncs. See the Best Practices Guide for more guidance on using the lists for given technologies and the default behavior.

Allowlists and denylists are typically used to keep syncs efficient, particularly for high volume elements (such as users). There are a number of fields pulled in from the devices that are useful to view, but do not require any specific processing (for instance fields like last login time, etc). So the default lists are based on a typical setup and help provide out-of-the-box optimization. For the most part, these will not need to be adjusted, but can be if required to meet a specific need in a deployment.

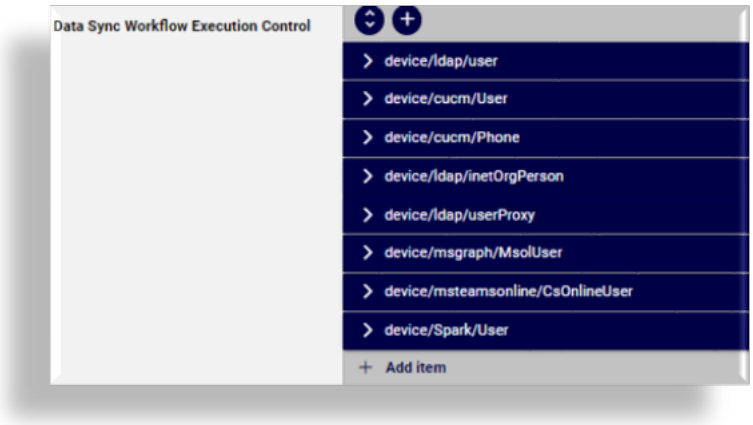
Related topics

- Settings (Data Sync Workflow Execution Control) in the Advanced Configuration Guide.
- Microsoft syncs in the Best Practices Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Global allowlist and denylist attributes

A `sysadmin` user can review the default system-level allowlist and denylist attributes currently set up for their environment via the `data/Settings` model (**Settings** page).



Note: Allowlist and denylist attributes for any of these model types may be added or removed in future releases. For example:

- At release 20.1.1, or after applying patch EKB-4362-19.2.1_patch, the previously denylisted LDAP attributes were no longer imported during LDAP synchronization:

  Model type: `device/ldap/user`

  Denylist attributes:

  - `logonCount`
  - `adminCount`
  - `lastLogonTimestamp`
  - `whenCreated`
  - `uSNCreated`
  - `badPasswordTime`
  - `pwdLastSet`
  - `lastLogon`
  - `whenChanged`
  - `badPwdCount`
  - `accountExpires`
  - `uSNChanged`
  - `lastLogofflastLogoff`

- At 21.4-PB2, the following allowlist model attributes were added:

  Model type: `device/msteamsonline/CsOnlineUser`

  Allowlist attributes:

  - `UserPrincipalName`

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - DisplayName
  - Department
  - City
  - FeatureType
  - EnterpriseVoiceEnabled
  - LineURI

Default allowlist and denylist attributes

Note: The attributes listed in this section of the guide are correct at the time of writing (for Automate 25.2).

- device/ldap/user
  - Denylist:
    - logonCount
    - adminCount
    - lastLogonTimestamp
    - whenCreated
    - uSNCreated
    - badPasswordTime
    - pwdLastSet
    - lastLogon
    - whenChanged
    - badPwdCount
    - accountExpires
    - uSNChanged
    - lastLogoff
    - userPassword
- device/cucm/User
  - Denylist:
    - primaryDevice
    - attendeesAccessCode
    - displayName
    - enableUserToHostConferenceNow
    - pinCredentials
    - passwordCredentials
    - associatedRemoteDestinationProfiles

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `device/cucm/Phone`
  - Allowlist:
    - `lines`
    - `ownerUserName`
- `device/ldap/inetOrgPerson`
  - Denylist:
    - `userPassword`
- `device/ldap/userProxy`
  - Denylist:
    - `accountExpires`
    - `adminCount`
    - `badPasswordTime`
    - `badPwdCount`
    - `bind_dn`
    - `dSCorePropagationData`
    - `distinguishedName`
    - `employeeID`
    - `homeMDB`
    - `instanceType`
    - `lastLogon`
    - `lastLogoff`
    - `lastLogonTimestamp`
    - `legacyExchangeDN`
    - `logonCount`
    - `mDBUseDefaults`
    - `mailNickname`
    - `manager`
    - `msExchArchiveQuota`
    - `msExchArchiveWarnQuota`
    - `msExchBlockedSendersHash`
    - `msExchCalendarLoggingQuota`
    - `msExchDumpsterQuota`
    - `msExchDumpsterWarningQuota`
    - `msExchELCMailboxFlags`
    - `msExchHomeServerName`
    - `msExchMailboxGuid`

Copyright © 2025 VisionOSS Limited. All rights reserved.

        * msExchMailboxSecurityDescriptor
        * msExchMobileAllowedDeviceIDs
        * msExchMobileBlockedDeviceIDs
        * msExchMobileMailboxFlags
        * msExchPoliciesIncluded
        * msExchRBACPolicyLink
        * msExchRecipientDisplayType
        * msExchRecipientTypeDetails
        * msExchSafeSendersHash
        * msExchTextMessagingState
        * msExchUMDtmfMap
        * msExchUserAccountControl
        * msExchVersion
        * msExchWhenMailboxCreated
        * objectCategory
        * objectClass
        * objectGUID
        * objectSid
        * physicalDeliveryOfficeName
        * primaryGroupID
        * protocolSettings
        * proxyAddresses
        * pwdLastSet
        * sAMAccountType
        * showInAddressBook
        * textEncodedORAddress
        * uSNChanged
        * uSNCreated
        * userAccountControl
        * whenChanged
        * whenCreated
        * userPassword
- device/msgraph/MsolUser
    - Allowlist:
        * UserPrincipalName
        * Title

Copyright © 2025 VisionOSS Limited. All rights reserved.

        * `PhoneNumber`
        * `StreetAddress`
        * `State`
        * `PostalCode`
        * `Office`
        * `MobilePhone`
        * `LastName`
        * `FirstName`
        * `DisplayName`
        * `Department`
        * `Country`
        * `City`
        * `PrimarySmtpAddress`
- `device/msteamsonline/CsOnlineUser`
    - Allowlist:
        * `UserPrincipalName`
        * `LineURI`
- `device/spark/User`
    - Allowlist:
        * `department`
        * `email`
        * `firstName`
        * `lastName`
        * `locationId`
        * `manager`
        * `phoneNumbers`
        * `title`

Cisco UCM Change Notification (CNF) Sync

Overview

Partners can use Cisco UCM's *Change Notification* (CNF) functionality to process *update sync* operations faster. This feature is disabled by default. You can enable it if required.

This topic provides guidelines for setting up a sync schedule, and lists associated performance implications.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Further details for using *CNF* is provided elsewhere in the Automate documentation. The changes described here are not transactions so details don't display in the transaction log, but in special logs created for CNF.

These guidelines are derived from concepts related to total processing capacity. The total number of updates processed in a time period is the sum of all updates across the customers selected for update in that time period. In this case, the time period is one hour. In this example, it is assumed that each customer has 1000 UCM-related changes in that hour.

Recommendations provided in the following table indicates that 5 customers can run in parallel (concurrently), and therefore a total of 5,000 changes processed in total.

Partners exceeding the recommendation of 5 concurrent customers may notice a performance degradation, and the full set of required changes may not complete within that hour. Alternatively, if the number of changes for any customer is significantly higher than 1,000, or if the total number of changes is significantly greater than 5,000, the supported concurrency number may be less than 5.

If some of the planned changes do not complete within the hour noted in the table, those changes are completed the next time that particular customer is scheduled for a sync.

If the number of changes for any customer is so large that the changes continually exceed those that can be processed in one hour, it will eventually result in a full sync. For such customers, it is recommended to schedule within an hour where less than 5 customers execute concurrently.

Configuration	Recommendation
Maximum number of concurrent CNF sync	5
Maximum number of changes processed per CNF sync	1,000
CNF sync schedule frequency	Once per hour per customer - This is subject to the staggering of CNF sync across customers.
Staggering of CNF syncs across customers	Factor of maximum changes processed and maximum number of concurrent CNF syncs.
CNF collector frequency	Initial recommendation is 15 minutes.
When is full sync required?	Weekends only or when there are CNF alerts prompting for full sync.

Note: It is recommended that you disable CNF if you experience significant performance degradation. Contact your support representative if you have any performance concerns.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Staggering CNF syncs across customers

This section provides an example and considerations for change notification (CNF) syncs across customers.

If a partner has twenty customers who want to use CNF sync, only schedule a maximum of five CNF syncs to run concurrently. This means that syncs would run as follows:

- 1st hour, for example 12:00

  Customer 1 to Customer 5
- 2nd hour, for example 13:00

  Customer 6 to Customer 10
- 3rd hour, for example 14:00

  Customer 11 to Customer 15
- 4th hour, for example 15:00

  Customer 16 to Customer 20
- 5th hour, for example 16:00 (Begin repeating customers)

  Customer 1 - Customer 5
- and so on.

The preceding example means that the CNF sync schedule per customer must run at 4 hour intervals. Therefore, there are 6 CNF syncs per customer within a 24 hour window. With each CNF sync processing up to 1k changes, there are:

- A total of 6k changes processed per customer in a 24 hour window
- A total of 120k changes processed across all 20 customers in a 24 hour window

CNF components

Automate's interaction with the Cisco Unified Communication Manager (Cisco UCM) Change Notification Feature (CNF) sync has two primary components:

Component	Description
Data Collector	Collects changes from Cisco UCM and updates the VOSS cache on the predefined frequency (defaults to every 300 seconds). This collector must be enabled to collect the changes, otherwise the sync won't process any changes.
Change Notification Sync	A change notification (CNF) sync type that processes the changes changes the data collector places in the VOSS cache. A scheduled sync must be set up and enabled so that the changes are processed within a reasonable period. The CNF sync can also be run adhoc, if required, around the the schedule.

The Automate data collector retrieves change records from Cisco UCM based according to the predefined interval. By default, this is every 300 seconds (3 minutes).

Copyright © 2025 VisionOSS Limited. All rights reserved.

When running a CNF sync, Automate processes the change records that are collected as follows:

Operation	Description
Add	Performs a GET API call to retrieve the full record, and adds it to Automate.
Update	Performs a GET API call to retrieve the full record, and updates updates the record in Automate.
Del	Removes the record from Automate.

Update syncs perform GET API calls only for changed records, which reduces the time it takes to run the sync. This is particularly beneficial for large UC installations.

With a data collector polling period of 300 seconds and a CNF sync scheduled for every 24 hours, the process is as follows:

- Every 300 seconds (5 minutes) the polling collector retrieves all current changes from Cisco UCM.
- The polling repeats every 5 minutes, and updates the Automate cache.
- After 24 hours, the CNF sync runs, and processes all the changes that Automate stored over that 24hr period.

  The sync duration depends on the number of changes to process, since each changed object requires an AXL GET API request. A GET AXL request is only required for objects changed in the time between syncs.

For example, on a system with 10 000 users, if 100 of these users are changed, then only 100 GET AXL request are required in a CNF sync. By contrast, a non-CNF sync would require 10 000 GET AXL requests to update these 100 users.

The Automate data collection can store up to 200,000 changes from a single Cisco UCM cluster.

- A system warning is triggered when the data collection storage reaches 75% of capacity
- A sync error is triggered when the 200 000 changes capacity is reached - see *Troubleshooting Change Notification (CNF)*

  To prevent the sync error, it is recommended that you have a regular, scheduled CNF sync running.

Cisco UCM and CNF

The Cisco UCM CNF capability supports all the objects that are available via AXL. Typically, this means that everything Automate can manage in Cisco UCM is available via change notification.

Data that Automate pulls from Cisco UCM that is *not* via AXL, includes:

- `device/cucm/PhoneType` - this is a combination of thinAXL so would not auto-update. This includes when you add or update phone types in Cisco Unified CM with COP files or via Cisco Unified CM upgrades. So a non-CNF sync is still required for this model.
- Phone Status and IP Address - this is pulled into the system when the phones are viewed in Automate (list view or individual phone). This is not via AXL so would not be updated via change notification or even a normal sync at this point.

In Cisco UCM, the change queue cache is stored in memory and is limited to 100,000 changes. The cache can fill quickly depending on the types of changes performed. For example, if an XSI (IP Phone) Service has been configured for 10,000 phones and the service is deleted, the cache will include one entry representing

Copyright © 2025 VisionOSS Limited. All rights reserved.

the deletion of the service plus 10,000 phone updates indicating the service was removed from each device. The polling period from the Cisco Unified CM is configurable and the timing should be considered based on how frequent configuration changes are being made in Cisco Unified CM. The default in Automate when polling is enabled is 300 seconds but it can be modified to be longer (up to 7200 seconds) as desired.

Cisco UCM setup to use CNF

There are two settings in the Cisco Unified Communications Manager (Cisco UCM) to check and update to ensure change notification (CNF) is enabled and set up for the right queue size (accessed via service parameters: - **System > Service Parameters > Cisco Database Layer Monitor** then click the **Advanced** button):

Service Parameter Name	Setting
AXL Change Notification	This should be set to “On”
AXL Change Notification Queue Size	This has a default of 20000. For a typical system, it is suggested this is changed to the maximum of 100000 to reduce the chance of changes being missed under heavy provisioning tasks.

Enable / disable CNF syncs for a Cisco UCM cluster

This section describes the high level steps for enabling change notification (CNF) syncs for a Cisco Unified Communications Manager (Cisco UCM) cluster in Automate:

Note: Perform these steps in reverse order to disable change notification for the cluster.

1. Enable and configure the service in Cisco UCM - see *Cisco UCM setup to use CNF*
2. Enable change notification on the Cisco UCM cluster in Automate - see *Automate change notification*
3. Review the change notification settings for the cluster - see *Automate change notification*
4. Review or create the required data sync instances for change notification, for the cluster.

   See Introduction to data sync in the Core Feature Guide

   Note: The actual number of syncs and their setup will depend on the needs for your system and the design.

   See the Best Practices Guide for guidance on sync logic and recommended setups. If further recommendations or guidance is needed, contact your VOSS account team or VOSS support.

5. Review or create required schedules for the data sync(s) created in the previous step, and activate the schedule(s) - see *Enable a scheduled data sync*

   Note: Follow the guidance for scheduling around syncs to ensure the load on the system is optimized.

   At least one sync schedule should be activated for the CNF sync setup to be complete.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate change notification

This section provides more details on the functionality of the Change Notification Feature (CNF) components in Automate.

Change notification collector

The `data/DeviceChanges` model has an instance per UCM cluster and will provide the data collector status and pending changes in the cache for that cluster. An instance of the model will appear for all UCM clusters whether change notification is enabled or not. It gives you access to:

- **Base** tab
  - **Last Collection Time** - time the changes were last collected from the device
  - **Pending Change Notifications** - a view of pending changes collected for different types of models and by type of change (Add/Update/Delete). By default, this is `device/cucm/User`, `device/cucm/Line` and `device/cucm/Phone`. However, these models are adjustable on the **Settings** tab. If additional model types to the defaults above are added to the list, these are also shown. The remaining model types are all grouped in a single row called `Other`.
- **Settings** tab
  - **Polling Interval (seconds)** (300-7200 seconds with default 300) - the duration for collection of changes from the device
  - **Enable Change Collection** - enable or disable the change collector for that device.
  - **Ignored Operations** - you can select certain operations (Add/Mod/Del) to not be collected. Typically you want to collect all changes; however this option can be used to ignore some changes for specific scenarios if needed (for example, you will only handle updates via the CNF sync).
  - **Displayed Model Types** - here you can configure which models you want to see summary stats for on the **Base** tab. You can add, remove or change models to meet specific needs (for example, `deviceProfile` for extension mobility profiles, `remoteDestination` for SNR remote destinations, and so on).

The `data/DeviceChanges` model should be included in menu layouts for roles that need access to this level of detail for the CNF syncs.

Change notification sync type

When a Change Notification sync type is used in a data sync, there are a number of differences in the sync behavior in comparison with a normal pull sync:

- A GUI portal rule on the Data Sync interface will change some of the settings visible on the Data Sync GUI interface when the **Sync Type** is set to Change Notification Sync. This selection hides settings that are not relevant and exposes new settings for this type only.
- **Number of Changes to Process** - This input field becomes available from the Data Sync interface. Leaving the input box blank or typing in 0 will mean the sync will process all the pending changes collected - subject to the selected model type list and Disabled Operations set up on the sync. If you enter a number, the sync will process that number of changes only and leave any additional changes in the change collection for the next sync.

  Typically this value should be 0 or blank, unless there is a specific reason to limit the number of changes to process, for example when managing how long the sync may run.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- A **Model Type List** (MTL) can be set up and selected to be associated with UCM change notification collection. This list allows a user to whitelist/blacklist certain model types from the Call Manager change notification collector service so that change notifications which are not in the MTLs do not accumulate and possibly trigger the maximum changes counter which prevents any new changes from being collected.

All other visible settings are the same as with a normal pull sync, for example, device filters, workflows, and so on.

When a sync runs (either a normal pull sync or a change notification sync), it will clear out the change notification collection of any model types and changes processed for that cluster.

The model type lists and disabled operations define which models and types of actions are processed in either a pull or a change notification sync:

- The model type list (if one is assigned) assigned to the sync will determine which model type changes will be processed from the collected changes (for example, `device/cucm/User` for user entities only).
- The **Disabled Operations** tab defines if any of the types of changes are ignored. For example, selecting **Remove** will ignore delete changes.

Pull Sync and Change Notification Sync details:

- A pull sync does not utilize the change notification collection as a source of data. However, it will clear the collection for the models types it processes.
  - A *full* pull sync (a pull sync without a model type list) will clear the change collection as part of the sync process since it is pulling *all* the latest information from the UCM.
  - A pull sync with a model type list defined (for example one that contains `device/cucm/User`) will clear the change collection of any `device/cucm/User` changes, since it is syncing all the user information anyway. All other model types and changes will be left in the collection.
  - If a pull sync is run with **Disabled Operations** selected (for example, **Add** is selected) this will process the pending changes for Update and Delete actions for any matching models. However, *all* actions for the matching model will be cleared from the cache, *including Add actions*.
- A Change Notification Sync utilizes the change collection as its source of information and will clear that changes from the change collection for any model types it is processing.
  - A *full* Change notification sync (CNF sync without a model type list) will process *all* the pending changes and clear the change collection (unless limited by a value in the **Number of Changes to Process** setting on the sync. Then only that number of changes will be processed and cleared).
  - A change notification sync with a model type list defined (for example contains `device/cucm/User`) will process all the pending changes for the `device/cucm/User` model type and clear those from the change collection.
  - If a change notification sync is run with **Disabled Operations** (for example, **Add** is selected), it will process the Update and Delete changes for the matching models. However, *all* actions for the matching model(s) will be cleared from the cache, *including Add actions*.

This sync behavior means that you may wish to set up multiple syncs for a cluster to handle different types of sync and sync schedules to meet your needs. Ensure that you generally have all the model types covered in your scheduled syncs if CNF is enabled, otherwise some changes may never be cleared from the change collection, thereby taking up space.

For additional considerations and information around sync setup best practices, see the Best Practices Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate setup to enable change notification

Enabling the Cisco UCM Change Notification Feature (CNF) capability is completed on a per Cisco UCM cluster basis. This can be done on the Cisco UCM Server configuration page for a publisher via the **Publisher** tab and selecting the **Enable Change Notification Sync** check box. When selected and saved, the system will:

- Enable the data collector for that cluster
- Create a CNF sync type for the cluster
- Create a schedule for the CNF sync (disabled by default).
- These settings should all be reviewed, adjusted, or additional instances created to meet your needs. See further information in:
  - The Best Practices Guide
  - The System Monitoring Configuration section in the Advanced Configuration Guide on sync best practices for different scenarios and other considerations.
- A full sync with the Cisco UCM cluster should be executed just before or after enabling CNF for the cluster. This can be part of changing the setting for an existing cluster or adding a new publisher. Currently, both actions will invoke a full sync of the cluster. However, if the sync is not completed during the add/modify of the publisher, then one should be initiated.

When CNF is disabled on the Publisher configuration page (or if the cluster is removed from the system), the following will occur:

- The auto-generated schedule that was added during enabling will be removed. Any additional custom scheduled added will not be removed automatically and should be removed before disabling the change notification for the cluster to avoid unnecessary syncs running.
- The auto-generated CNF sync type that was added during enabling will be removed. Any additional custom CNF sync types for the cluster added will not be removed automatically and should be removed before disabling the change notification for the cluster to avoid unnecessary syncs being set up.
- The data collector for the cluster will be disabled.

Note: If the collector is only disabled via the `data/DeviceChanges` model, then the schedules and sync will remain. This is the best approach if you need to temporarily disable the CNF sync (for example, for a maintenance window).

Troubleshooting Change Notification (CNF)

A number of scenarios may result in error conditions in the change notification (CNF) process. In this case, Automate is able to display alerts automatically, which means it won't be necessary to configure change notification (CNF) alerts manually.

Administrators can view the alerts at the hierarchy level they log in at and all the levels below that hierarchy. For example, if an alert is raised at the customer level (sys.hcs.provider.reseller.c1), then the provider, reseller, and customer administrators can see that alert, but not the site administrators. All the administrators have read and delete permissions to the alerts.

When a CNF alert is raised, the Notifications indicator on the Admin Portal GUI displays the alert. Clicking the notifications launches a dialog and a message that alerts have been raised. Click on the message to be able to go to the list of alert messages, which are also accessible via the **Alerts** page.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Properties of CNF alerts

CNF alerts have these properties:

- ID: A generated identifier of the target device of the collector For Unified CM, the ID shows the host name, port, and hierarchy.
- Code: An error or warning code associated with the alert.
- Alert category: The category of the alert - Device Change Notification Collector
- Severity: Automate displays severity codes and messages as follows ("{}" indicate device or number placeholders in the messages). Each alert has some properties, for example, severity (Error, Warning or Info), the number of times that the same alert has been raised, and the time stamp of the last alert instance.
- Message: Displays error message description and the statement to fix the error.
- Count: Displays the number of times the alert has occurred for a specific device.
- Latest Alert: Displays the last time this alert occurred.

Note: Administrators can also filter alerts by any of the alert fields.

Error scenarios for CNF alerts

Automate displays change notification alerts for the following error scenarios:

Important: Errors codes not discussed in this section may be relevant for alerts that are more internal, and you may need to raise a support ticket for further investigation.

- Warning:
  - 45000: Unprocessed changes at 75% of limit for device {}. Please configure and run the necessary data syncs.
- Error:
  - 40000: Device change notifications are not supported for device {}.
  - 40001: Device change notification data for device {} has been lost. Tracking data has been repaired and collector process will continue. Some changes may have been lost, please run a full sync on the device.
  - 40002: Device change notification tracking data for device {} has become corrupted. Tracking data has been repaired and collector process will continue. Some changes may have been lost, please run a full sync on the device.
  - 40003: Device change notification tracking DB write for device {} failed. The collector process will continue to attempt DB writes. Please investigate the database write failure.
  - 40004: Device change notification data DB write for device {} failed. The collector process will continue to attempt DB writes. Please investigate the database write failure.
  - 40005: Unable to repair device change notification tracking data for device {}.
  - 40006: Too many unprocessed changes recorded for device {}. No new changes will be recorded until at least {} changes are processed. Please configure and run the necessary data syncs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - 40008: Could not update pending changes data for device {}. {}.

The administrator reads, inspects, acts on (for example, run a full sync on the device), and then manages alerts of the Change Notification collection service. The administrator can delete the alert from the list only when the issue that raised the alert has been resolved.

Note: If the Administrators forget to remove the change notification feature alert after resolving it, the alert will still be shown when they log in to Automate. We strongly recommend removing the alert after resolving it.

Change Cache Full on Cisco UCM

If the Cisco UCM maximum number of stored change records is exceeded, the Cisco UCM drops the oldest changes that have not been collected. This can happen if the polling time in Automate is set up to be too long or the Cisco UCM is experiencing a very high level of changes. In this case, the system automatically attempts to recover once it receives the polling error. This activity is logged as an alert in the system and provides the outcome, either of the following:

- recovery was successful (alert code 40001 or 40002)
- recovery was not successful (alert code 40005)

If recovery is successful, you may want to review and consider a full sync as some changes would have been lost (the oldest changes in the Cisco UCM cache).

If recovery was not successful, a full sync is required to update and to get CNF functioning again. The full sync is needed as changes would have been missed from the Cisco UCM, and a clean sync is required in order to start processing changes again. In this situation, application info log messages are logged as well - “Repaired change notification tracking data for device {}” or “Unable to repair change notification tracking data for device {}”

Change Collection Full for a CUCM Cluster

If the Automate change collection for a given Cisco UCM cluster exceeds the maximum changes - 200,000 - then an alert with code 40006 is raised. This alert means that no further changes are collected from the Cisco UCM until some of the pending changes are processed. This can be carried out by an administrator executing a sync for that Cisco UCM cluster to clear some of the changes. If the next scheduled sync is not too far ahead in time, then waiting for the next scheduled sync to run may be acceptable.

Bulk Schedule Activation / Deactivation

sys-admin

VOSS Automate provides a bulk schedule tool for creating a catalog of active and inactive schedules, and for activating and de-activating these schedules. For systems with many schedules, this facilitates simpler activation and de-activation of scheduled tasks when downtime is needed, for example, when upgrading.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Exposing the utility

The bulk schedule tool is comprised of a set of data models, views, configuration templates, and workflows.

High level administrators with access to the following data models can expose the utility on an administrator menu:

Data model	Description
`data/BulkScheduleToo`	A data model that stores the list of created schedule catalogs. Each entry is identified by the entered catalog name and contains a list of schedules that were active on creation.
`view/BulkScheduleToo`	A form allowing the admin to create catalogs of schedules to deactivate and re-activate a selected catalog of schedules.

Note: The administrator's access profile should also allow create permissions on these models.

Using the Bulk Schedule Tool

Administrators with access to the bulk schedule tool from their menu can perform the bulk schedule deactivation and reactivation task, which is typically done before and after a system upgrade. This will allow better management of scheduled tasks during upgrades.

On the view interface:

1. To create a new catalog of schedules and deactivate these:

   From **Choose Action**, select **Catalog and Deactivate Schedules**, enter a catalog name in **New Catalog Name** and click **Save**.

   A workflow will collect the name of all active schedules and add this list along with the catalog name to be stored in the data model. The list of schedules are also deactivated. This can be verified from the **Administration Tools > Scheduling** menu.

2. To reactivate a catalog of schedules:

   From **Choose Action**, select **Activate Deactivated Catalog**, select the **Restore catalog Name** and click **Save**.

   A workflow will reactivate all deactivated schedules in the catalog.

   Note: If any schedules in the selected catalog are not available or have already been activated, these are ignored.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Datasync Builder

Tip: *Use the Action search to navigate Automate*

Introduction to the Datasync Builder

The Datasync Builder enables an admin to create data syncs against any device type, using data sync templates.

The Datasync builder is modular and vendor-agnostic, providing an admin with full control over the data syncs they're building, which is particularly useful when needing to build data syncs for multiple customers with different sync requirements. For example, for Webex customers you can build a relevant template for the customer, and the Datasync builder builds all required components for the data sync for the customers you execute it against.

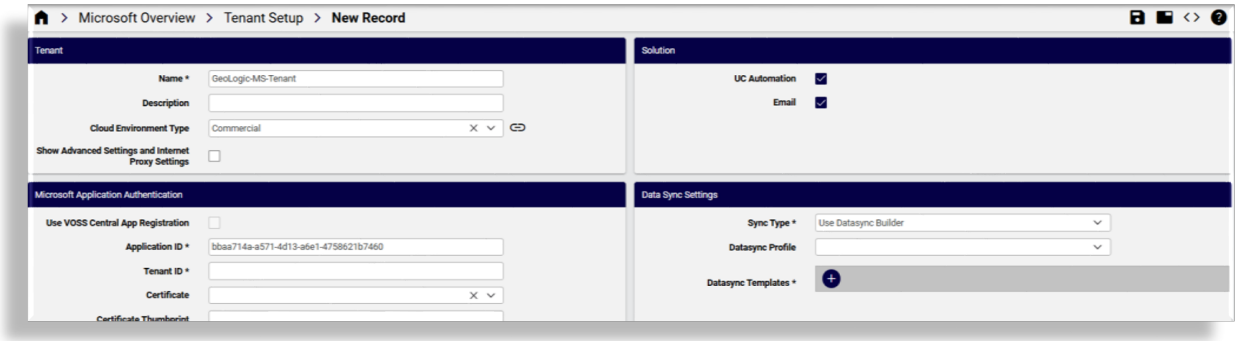
Automate 25.3 ships with predefined example data sync templates, including templates based on Microsoft use cases that are integrated with the Microsoft tenant.

Datasync Builder integration with the MS tenant

The Datasync Builder tool is integrated with the Microsoft tenant by default so that you can choose it as the sync type for the tenant.

On the MS tenant, the Datasync Builder uses a custom data sync template to create the required data syncs for the tenant, based on a single enabled solution. You can use the Datasync Builder on the tenant with a data sync profile or select one or more data sync templates based on your requirements.

Datasync templates available on the tenant are filtered by the solutions enabled on the tenant, for example, UC Automation or Email.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Using Datasync Builder on the tenant

There are two options for using the Datasync Builder sync type on the Microsoft tenant:

- **Option 1: Use Datasync Builder and choose templates**
  - Select as the sync type, **Use Datasync Builder**.
  - At **Datasync Templates**, add the templates you want to use.
  - If the template you selected is for recurring syncs you'll be able to select a first execution date and time.

  The templates available for this option are filtered by the solution enabled on the tenant. The advantage with this option is that for recurring syncs, you can set the first execution date and time on the tenant screen for the sync. The scheduling configured on this form applies to the tenant you're configuring and is not added to a template or profile. Start dates earlier than the current date are considered invalid.
- **Option 2: Use Datasync Builder with a data sync profile**
  - Select as the sync type, **Use Datasync Builder**.
  - At **Datasync Profile**, select one of the predefined data sync profiles. Each data sync profile groups a number of data syncs.
  - The workflow will execute the data sync builder as many times as there are data syncs in the profile, including MTLs, MIFs and other configuration components you may have in the profile.

  The disadvantage with this option is that there is no way to add the start time for each of the recurring syncs in the tenant form. This means that when using the data sync profile, the schedules can be built but you'll need to configure the first execution date and time and recurrence options into each of the scheduled syncs in the profile.

Related topics

- *Microsoft tenant setup*
- *Datasync builder templates*
- *Datasync profiles*

Create data syncs using the Datasync Builder

This procedure uses the Datasync Builder to build out a set of data syncs and associated configuration.

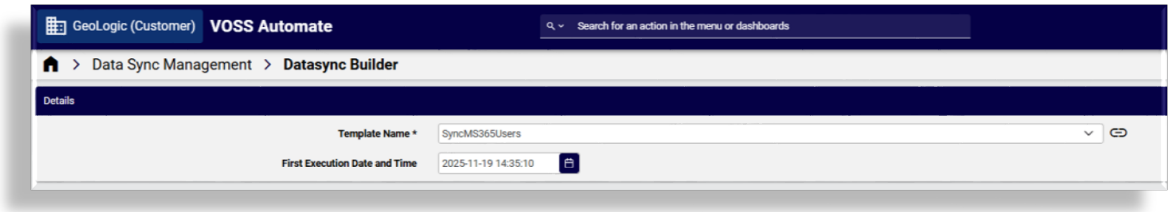
1. In the Admin Portal, set the hierarchy to the relevant customer.
2. Go to **Datasync Builder**.
3. Select a template.

   Select a shipped template, or create your own at this hierarchy so that it will be available in the drop-down.
4. If this is a non-purge sync, select the first execution date and time.

   Note: Schedules aren't relevant for *Purge* syncs since they're executed "on demand". Creating data syncs from a template allows you to define the first execution date and time for syncs that should

Copyright © 2025 VisionOSS Limited. All rights reserved.

execute regularly, and to define the execution frequency (for example, daily or weekly) when configuring the template.



5. Click **Save**.

   The workflow executes and creates the following:

   - One data sync. You'll need to run the Datasync Builder tool for each additional data sync you need.
   - Model type lists (MTLs) to define the sync order.
   - Model instance filters (MIFs)
   - A schedule

Note: Model instance filter (MIF) templates can be used in the Microsoft tenant, where you can select a predefined MIF template. MIF templates aren't mandatory but if you're creating many data sync templates, it's useful to pre-configure one or more MIFs. You can also explicitly create MIF templates for specific purposes.

Next steps

- Configure the data sync builder template. See *Datasync builder templates*

6.7. Dialplan Tools - App Integration and Detailed Settings

6.7.1. Cisco Custom Dial Plans

Tip: *Use the Action search to navigate Automate*

Overview

Automate provides support for Cisco HCS dial plans, and Cisco Custom dial plans. This section describes the Cisco Custom dial plans.

Important: Contact your dedicated VOSS support representative for details on how to set up and configure Cisco Custom Dial Plans.

Copyright © 2025 VisionOSS Limited. All rights reserved.

By default, the Dial Plan Management Tool and associated menus is visible in an Enterprise environment, and hidden on Provider deployments. To expose this feature on Provider deployments, set the Global Setting "Enforce HCS Dial Plan" to *No*. For details, see:

- *Configure access profile for Cisco custom dial plans*
- *Configure the Cisco custom dial plan management menus*

Related topics

- *Microsoft dial plan models*

Features of Cisco custom dial plans

Cisco custom dial plans:

- Allow you to manage dial plans independent of the hierarchy schema approach of Cisco HCS dial plans. However, you can also use Cisco Custom dial plans with schema-based dial plans.
- Can be used in place of or together with the schema or schema group approach, for example to add elements in an additional dial plan in an ad-hoc manner.
- Allows senior administrators to define complete complex dial plans and to provide access to these dial plans to lower level administrators, who won't need to understand the complete dial plan.
- Cisco Custom dial plan models use all functionality of schemas, as well as call routing via route filters.
- Provide additional configuration options, and a repeatable process for managing CUCM elements.
- Can be provisioned in a modular manner.
- Provide a structure for storing dial plan models.

Deployment elements included with Cisco Custom dial plans:

The elements included in a Cisco Custom dial plan are collectively referred to as a Dial Plan Model.

Each dial plan element is broken into its own container or model for storage in Automate. This allows for simple management of the dial plan model as a whole.

Cisco Custom dial plan models may be bulk loaded into Automate and managed via the Admin Portal.

The following elements are included in Cisco Custom dial plan:

- Device Pools - Regions - Locations -SRST
- Transcoders
- Conference Bridge
- Media Resource Groups
- Media Resource Group Lists
- Route Groups
- SIP Trunks
- CTI Route Points *with Lines* (Lines are not supported in schemas)
- Time Periods

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Time Schedules
- Partitions
- CSSs
- Route Patterns
- Transition Patterns
- Called Party Transformation Patterns
- Calling Party Transformation Patterns
- SIP Route Patterns

Configure the Cisco custom dial plan management menus

1. Login as an administrator with sufficient rights to change menu layouts.
2. Go to **Menu Layouts**.
3. Click on the relevant menu to edit it.
4. Configure the **Dial Plan Management** menu as described in the table, then save your changes:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Type	Display As
Dial Plan Management Tool		List
Dial Plan Maintenance	/api/view/DP_MaintenanceVIEW add	Form
Multi-Cluster Dialplan Maintenance		Form
Dial Plan Viewer	relation/DP_REL	List
Delete Dial Plan	/api/view/DP_DeleteDialPlanModel/add	Form
Dial Plan Input Data		List
• Global Data	data/DP_GlobalDialPlanData	List
• Site Level Data	data/DP_SiteDialPlanData	List
Cisco Dial Plan Models		
• Device Pool-Region -Location-SRST	data/DP_DP-Reg-Loc	List
• Conference Bridge	data/DP_ConfBridge	List
• Media Resource Group List	data/DP_MediaResourceGroupList	List
• SIP Trunks	data/DP_SIPTrunk	List
• CTI Route Points	data/DP_CTIRoutePoint	List
• Route Groups	data/DP_RouteGroup	List
• Route Lists	data/DP_RouteList	List
• Route Patterns	data/DP_RoutePattern	List
• Translation Patterns	data/DP_TransPattern	List
• Called Party Transformations	data/DP_Called_Party_Transformation	List

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Type	Display As
Cisco Dial Plan Models (Continued)		
• Calling Party Transformations	data/DP_Calling_Party_Transformation	List
• SIP Route Patterns	data/DP_SIPRoutePattern	List
• Calling Search Space	data/DP_Css	List
• Transcoders	data/DP_Transcoder	List
• Time Periods	data/DP_TimePeriod	List
• Time Schedules	data/DP_TimeSchedule	List
• Media Resource Group	data/DP_MediaResourceGroup	List
• Partitions	data/DP_Partition	List
Dial Plan Log	data/DP_DialPlanLog	List

Note: If you have a Microsoft-only environment, or a multi-vendor or hybrid environment that includes Microsoft, the Dial Plan Management Tool menu also includes the **Microsoft Dial Plan Models** menus. See *Microsoft dial plan models* for details.

Configure access profile for Cisco custom dial plans

1. Log in as HCS administrator or higher (you'll need sufficient rights to change access profiles).
2. Go to **Access Profiles**.
3. Select the required administrator name, for example ProviderAdminAP.
4. Configure the provider access profiles as shown in step 5.
5. Under **Type Specific Permissions** add the following new **Permitted Type** entries and **Permitted Operations**:
   - Permitted Type: view/DP_MaintenanceVIEW
   - Permitted Operations: Create, Field Display Policy, Read

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Permitted Type: relation/DP_REL
- Permitted Operations: Create, Read
- Permitted Type: view/DP_DeleteDialPlanModel
- Permitted Operations: Create, Read
- Permitted Type: data/DP_GlobalDialPlanData
- Permitted Operations: Create, Delete, Export, Export Bulk Load, Read, Tag, Update
- Permitted Type: data/DP_SiteDialPlanData
- Permitted Operations: Create, Delete, Export, Export Bulk Load Template, Read, Tag, Update
- Permitted Types:
  - data/DP_CalledParty_Transformation
  - data/DP_CallingParty_Transformation
  - data/DP_ConfBridge
  - data/DP_Css
  - data/DP_CTIRoutePoint
  - data/DP_DialPlan
  - data/DP_DialPlanLog
  - data/DP_DP-Reg-Loc
  - data/DP_MediaResourceGroup
  - data/DP_MediaResourceGroupList
  - data/DP_Partition
  - data/DP_RouteGroup
  - data/DP_RouteList
  - data/DP_RoutePattern
  - data/DP_SIPRoutePattern
  - data/DP_SIPTrunk
  - data/DP_TimePeriod
  - data/DP_TimeSchedule
  - data/DP_Transcoder
  - data/DP_TransPattern
- Permitted Operations: Create, Delete, Export, Export Bulk Load Template, Read, Tag, Update

6. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Cisco custom dial plan checklist

The high level task workflow for setting up Cisco Custom dial plans is as follows:

- Load Dial Plan Models for Global Values via bulk loader or JSON
- Load Dial Plan Models for Site Values via bulk loader or JSON
- Set Dial Plan Input Data for Global or Site level values. Only the fields that are referenced via Macro in the dial plan model must be populated.
- Push Global dial plan data to Cisco Unified Communications Manager (CUCM), using the Dial Plan Maintenance Tool. Be sure to check that the tool is run at the appropriate hierarchy level.
- Push Site level dial plan data at CUCM, using the Dial Plan Maintenance Tool. Be sure to check that the tool is run at the appropriate hierarchy level.
- Should any changes need to be made to the pushed dial plans, the tool does allow for removal in reverse order then a re-push once the dial plan models are updated.
- Set Site Defaults via the site default profile tool.

6.7.2. Multi-Cluster Dial Plan Maintenance

In contrast with the *Dial Plan Maintenance* view, the **Multi-Cluster Dial Plan Maintenance** allows for a selected Dial Plan to be added to or removed from multiple Cisco Unified Communications Manager (CUCM) clusters in a single step.

Both modes of the tool work in the same manner:

1. Choose the **Dial Plan Name** to manage on the CUCM clusters.

   The dial plan tag allows only dial plans meant for a specific hierarchy use to be shown. The **Chosen Dial Plan Type** shows this.
2. An operation is chosen from the **Operation** drop-down.
3. Select the CUCM clusters from the **Available** transfer box so these are shown in the **Selected** box.
4. Click **Save** to carry out the task.

Note:

- All dial plan elements are added to or removed from the selected clusters in accordance with the selected operation.
- The operation's transaction log sub-transactions **Detail** column show dial plan, hierarchy and target cluster.
- If for example a site level dial plan is selected, this tool will check the CUCM of the Network Device List (NDL) belonging to the site to verify if a dial plan is applied to this CUCM.
- Sites cannot be excluded if a site level dial plan is applied in the cluster.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6.7.3. Dial Plan Model Bulk Loader

Individual dial plans are meant to be established in the system with a bulk loader. Reference Bulk Loaders will be provided by VOSS staff for use in customer deployments. The key to dial plan for use with the tooling is the Dial Plan Name. This is the top entry in the dial plan model loader. Once a name is established it will carry down through the rest of the fields pertaining to the dial plan name.

Example of the dial plan model bulk loader:

	A	B	C	D	E	F	G	H	I	
1	##	Dial Plan Name								
2		entity: data/DP_DialPlan; parallel: False; parallel_transaction_limit: ; template:								
3		hierarchy	action	search_fields	device	template	ndi	pkid	dpName	
4		# Base							# DP_DialPlan	
5	# Comment	# Hierarchy Node	# Action	# Search Fields	# Device	# CFT Template	# Network Device List	# Unique Identifier	# Dial Plan Name	
6		sys.hcs	Add						Tiered_Cust_Level_DP	Global Dial Plan E
7	##									
8	##									
9	##	Device Pool - Region - Location - SRST Refernce								
10		entity: data/DP_DP-Reg-Loc; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template:								
11		hierarchy	action	search_fields	device	template	ndi	pkid	dpName	
12		# Base							# Device Pool	
13	# Comment	# Hierarchy Node	# Action	# Search Fields	# Device	# CFT Template	# Network Device List	# Unique Identifier	# Dial Plan Name	
14	0	sys.hcs	Add						Tiered_Cust_Level_DP	{{ macro.DP_Cust
15	##									
16	##									
17	##	Time Periods								
18		entity: data/DP_TimePeriod; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template:								
19		hierarchy	action	search_fields	device	template	ndi	pkid	dpName	
20		# Base							# Time Period	
21	# Comment	# Hierarchy Node	# Action	# Search Fields	# Device	# CFT Template	# Network Device List	# Unique Identifier	# Dial Plan Name	#
22	0	sys.hcs	Add						Tiered_Cust_Level_DP	01:00
23	0	sys.hcs	Add						Tiered_Cust_Level_DP	07:00
24	0	sys.hcs	Add						Tiered_Cust_Level_DP	No Office Hours

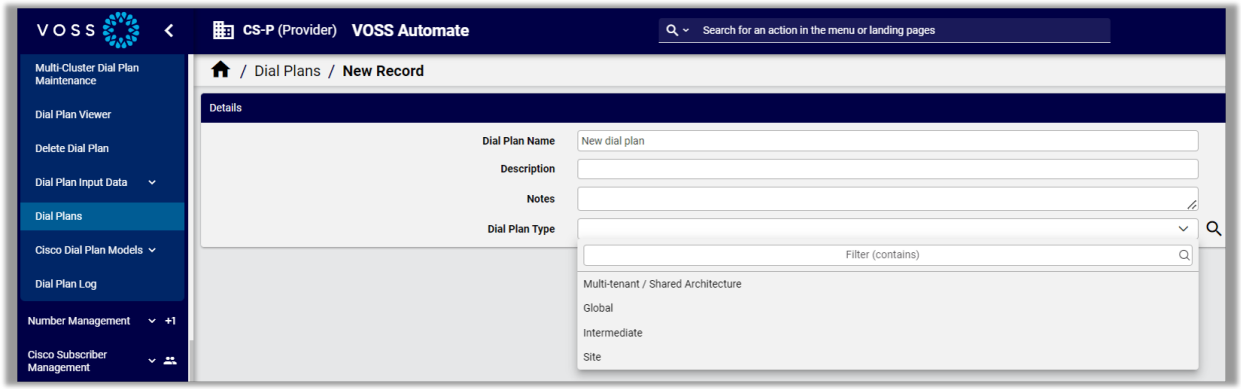
6.7.4. Custom Dialplan Tool - Actions

Dial Plans

This menu allows you to view, delete, and export existing dial plans, and add new dial plans.

Important: The Dial Plan Management Tool and associated menus is visible in an Enterprise environment, and hidden on Provider deployments. To expose this feature on Provider deployments, set the Global Setting "Enforce HCS Dial Plan" to *No*. For details, see:

- *Configure access profile for Cisco custom dial plans*
- *Configure the Cisco custom dial plan management menus*



Copyright © 2025 VisionOSS Limited. All rights reserved.

When adding a new dial plan via the **Dial Plans** menu, you can choose the dial plan type - either of the following:

- Multi-tenant / Shared Architecture
- Global
- Intermediate (allows you to push a dial plan at Intermediate node)
- Site

All dial plans you add can be viewed on the Dial Plans list view.

The Dial Plan Management Tool allows you to add dial plans at the site hierarchy, customer hierarchy, or at intermediate nodes, which is useful for multicluster/multicountry customers.

Intermediate node dial plans allows you to create country dial plans at the intermediate node, which use macros to pull input data from the global data at the intermediate node. This reduces the amount of hardcoded elements in the dial plan template; instead it is mostly driven by the global input data.

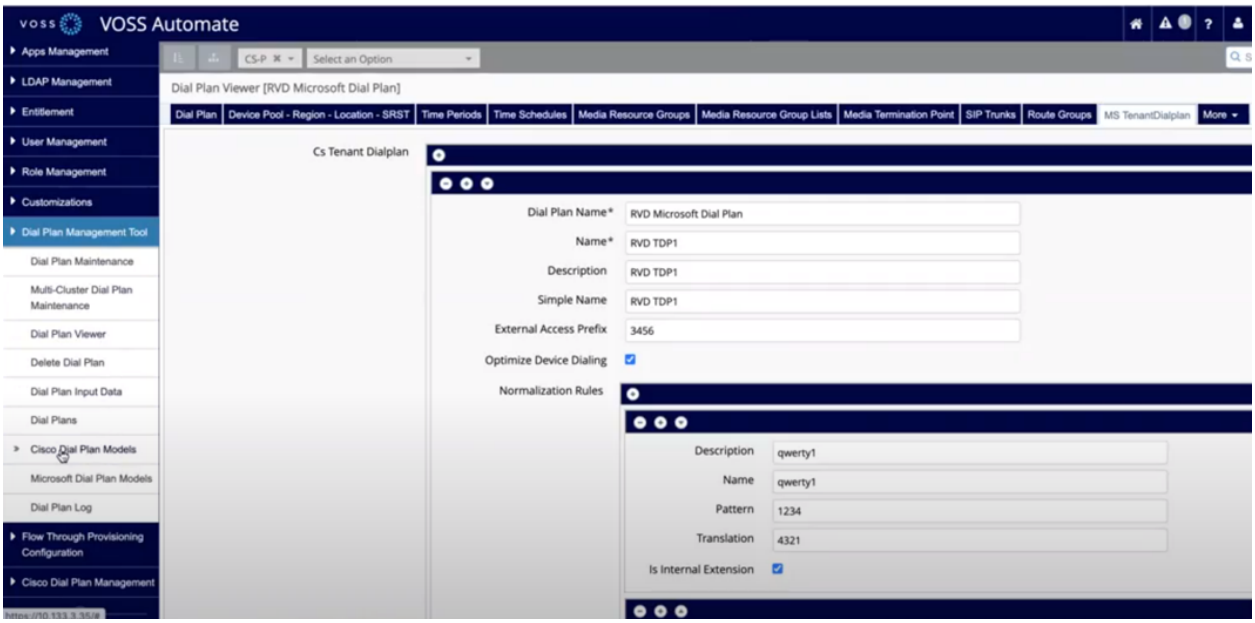
Dial Plan Viewer

The Dial Plan Viewer provides read-only details of all the dial plan elements of a selected dial plan.

The contents of this view corresponds with the view of a dial plan schema, but in a format that is easier to inspect.

Note that the viewer does not allow for any changes to be made to the dial plan.

See also “Dial Plan Models” for details of each specific dial plan element.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial Plan Input Data

Cisco

Overview

The Cisco Custom dial plan **Dial Plan Input Data** menus (**Global Data** and **Site level Data**) simplify the update of Cisco Custom dial plans by exposing a set of values that can be provided to and then easily applied by lower level administrators.

The table describes the type of input data that can be defined, each corresponding to a dial plan type:

Global Data	Applies to Global dial plan type (customer)
Site level Data	Applies to Site dial plan type

All values are optional, and field display policies (FDPs) can be configured to hide unused fields, if required. For example, **Secondary SIP Trunk Destination IP** and **Secondary SIP Trunk Destination Port**.

You can also add custom values, and use macros to allow these values to be referenced in dial plan elements. In this case, you can use a FDP to rename the input field label, if needed.)

Input data may be used in combinations to build patterns dynamically, since the pattern itself is a macro. For example, site-level translation patterns for 7 or 10 digit dialing can use the Customer-level macro for PSTN access (or External Breakout Number), then followed by a "." , then the macro for Area Code or Exchange:

```
{{ macro.DP_Global_PSTNAccess }}.{{ macro.DP_AreaCode }}XXXXXXX
```

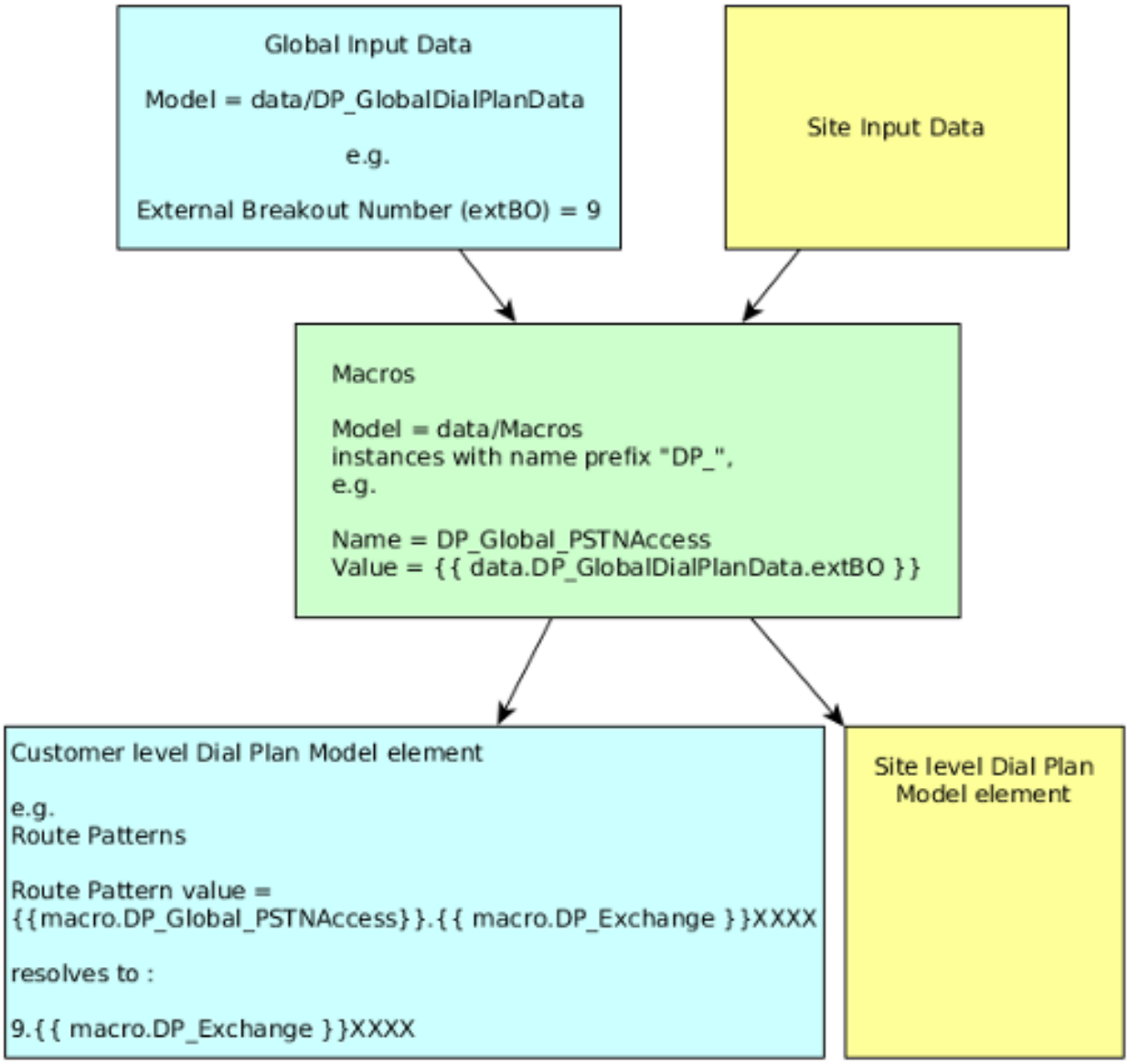
when applied, could be inserted to Cisco Unified Communications Manager (CUCM) as `9.214XXXXXXX` for 10 digit dialing.

```
{{ macro.DP_Global_PSTNAccess }}.{{ macro.DP_Exchange }}XXXX
```

when applied, could be inserted to CUCM as `9.256XXX` for 7 digit dialing.

The diagram below provides an example of the use of a macro in a Global (customer) level dial plan element: **Route Patterns**.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Global Data

The Global Data page contains three tabs:

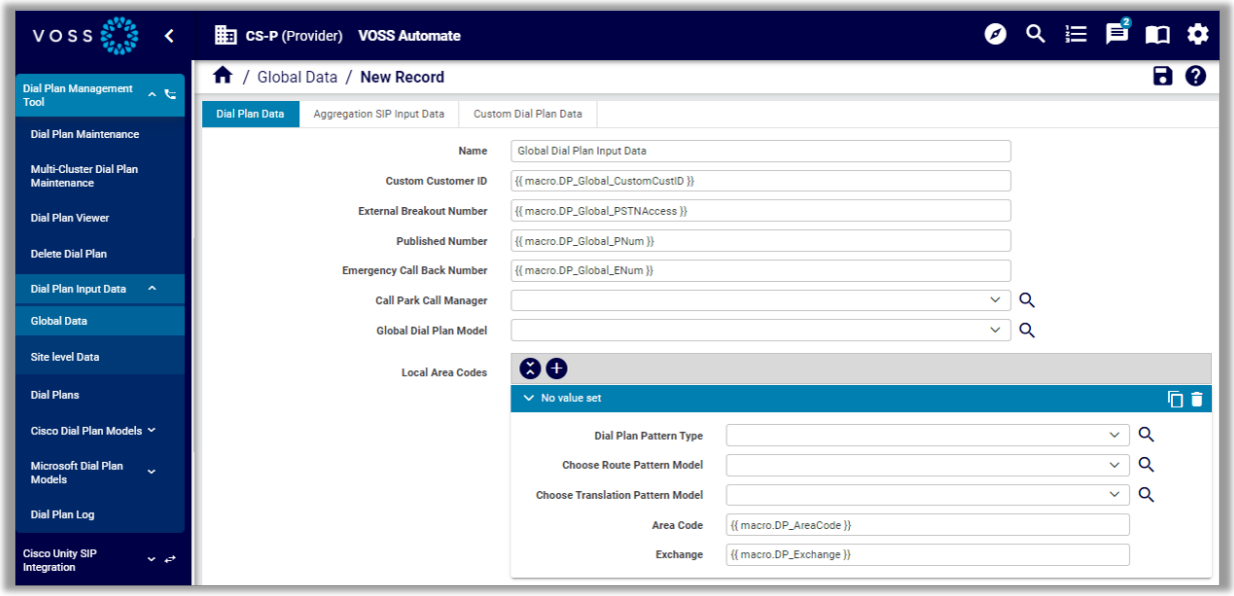
- Dial Plan Data
- Aggregation SIP Input Data
- Custom Dial Plan Data

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial Plan Data Tab (Global - Single Instance)

On this tab you can use the following macros:

- Custom Customer ID: `{{ macro.DP_Global_CustomCustID }}`
- External Breakout Number: `{{ macro.DP_Global_PSTNAccess }}`
- Published Number: `{{ macro.DP_Global_PNum }}`
- Emergency Call Back Number: `{{ macro.DP_Global_ENum }}`
- Area Code: `{{ macro.DP_AreaCode }}`
- Exchange: `{{ macro.DP_Exchange }}`

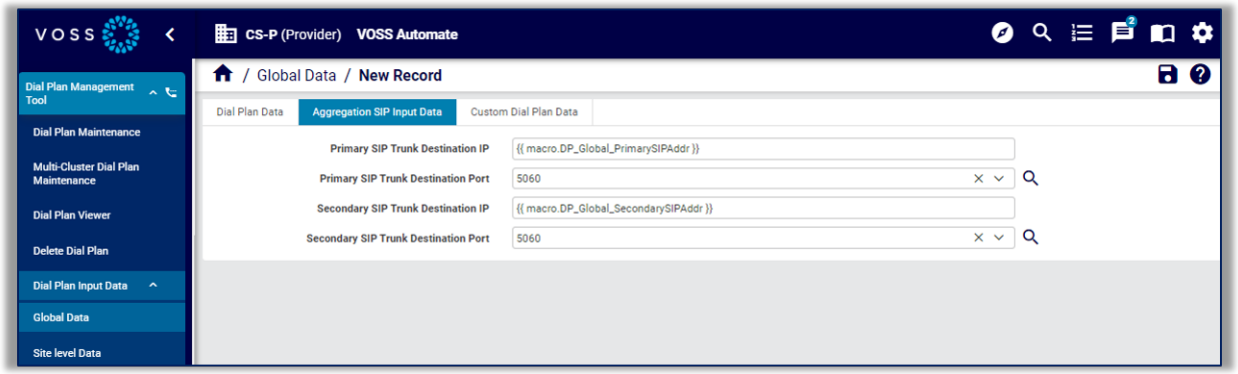


Aggregation SIP Input Data Tab (Global)

On this tab you can use the following macros:

- Primary SIP Trunk Destination IP: `{{ macro.DP_Global_PrimarySIPAddr }}`
- Primary SIP Trunk Destination Port: `{{ macro.DP_Global_PrimarySIPPort }}`
- Secondary SIP Trunk Destination IP: `{{ macro.DP_Global_SecondarySIPAddr }}`
- Secondary SIP Trunk Destination Port: `{{ macro.DP_Global_SecondarySIPPort }}`

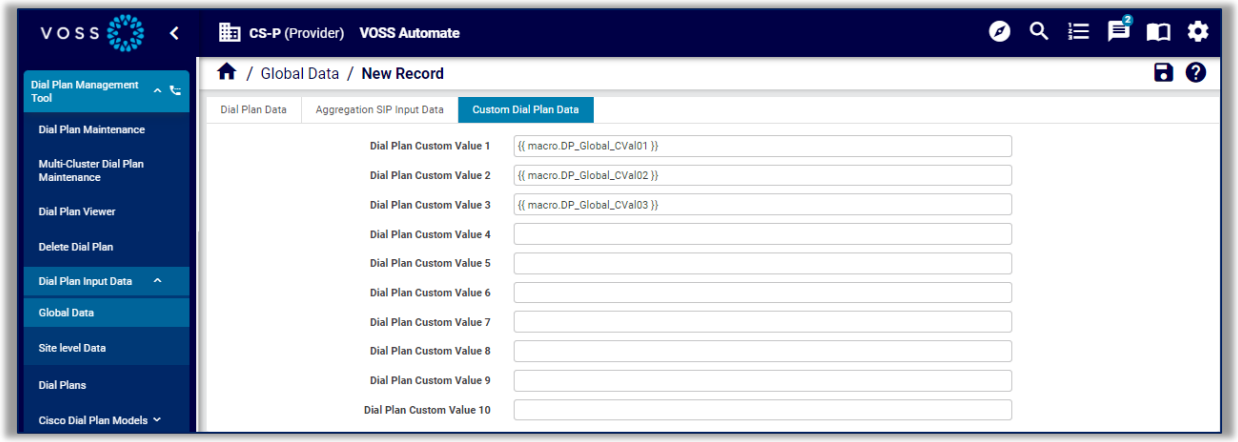
Copyright © 2025 VisionOSS Limited. All rights reserved.



Custom Dial Plan Data Tab (Global)

On this tab you can use the following macros:

- Dial Plan Custom Value 1: `{{ macro.DP_Global_CVal01 }}`
- Dial Plan Custom Value 2: `{{ macro.DP_Global_CVal02 }}`
- Dial Plan Custom Value 3: `{{ macro.DP_Global_CVal03 }}`
- Dial Plan Custom Value 4: `{{ macro.DP_Global_CVal04 }}`
- Dial Plan Custom Value 5: `{{ macro.DP_Global_CVal05 }}`
- Dial Plan Custom Value 6: `{{ macro.DP_Global_CVal06 }}`
- Dial Plan Custom Value 7: `{{ macro.DP_Global_CVal07 }}`
- Dial Plan Custom Value 8: `{{ macro.DP_Global_CVal08 }}`
- Dial Plan Custom Value 9: `{{ macro.DP_Global_CVal09 }}`
- Dial Plan Custom Value 10: `{{ macro.DP_Global_CVal10 }}`



Copyright © 2025 VisionOSS Limited. All rights reserved.

Site Level Data

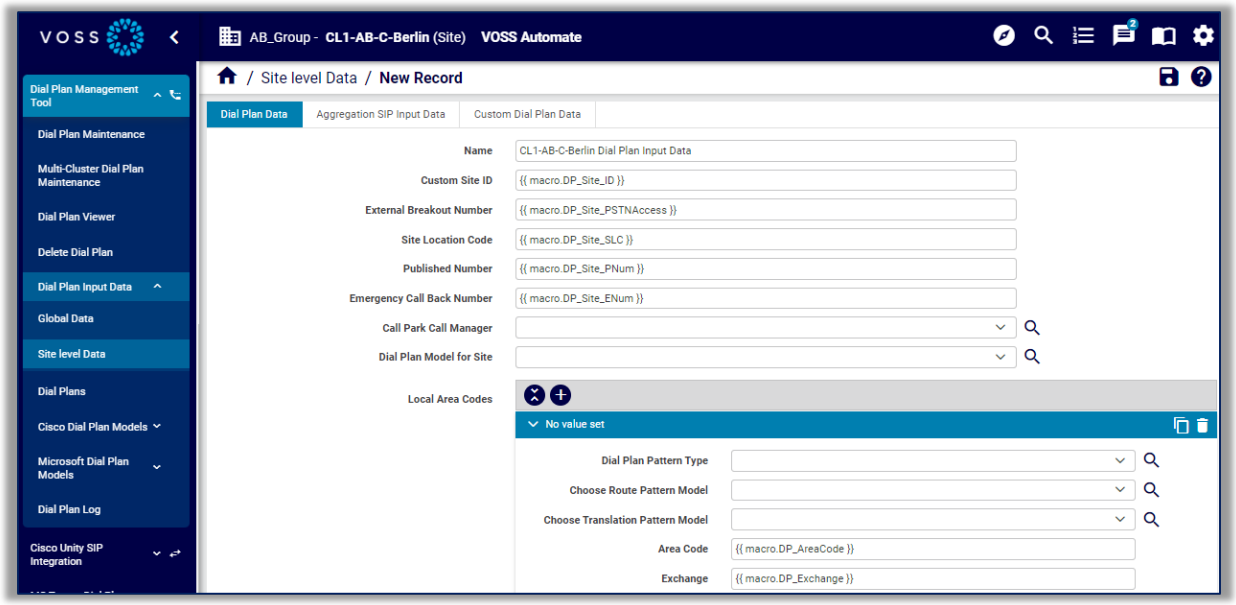
The Site level Data page contains three tabs:

- Dial Plan Data
- Aggregation SIP Input Data
- Custom Dial Plan Data

Dial Plan Data Tab (Site - Single Instance)

Data from the provided fields may be referenced with the provided macros:

- Custom Site ID: `{{ macro.DP_Site_ID }}`
- External Breakout Number: `{{ macro.DP_Site_PSTNAccess }}`
- Site Location Code: `{{ macro.DP_Site_SLC }}`
- Published Number: `{{ macro.DP_Site_PNum }}`
- Emergency Call Back Number: `{{ macro.DP_Site_ENum }}`
- Area Code: `{{ macro.DP_AreaCode }}`
- Exchange: `{{ macro.DP_Exchange }}`

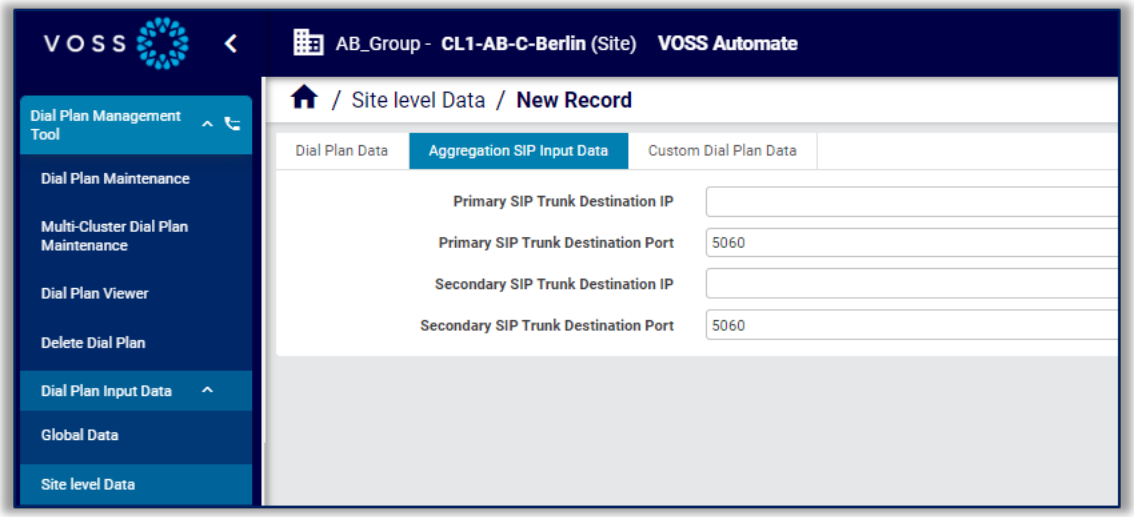


Copyright © 2025 VisionOSS Limited. All rights reserved.

Site Aggregation SIP Input Data Tab (Site)

Data from the provided fields may be referenced with the provided macros:

- Primary SIP Trunk Destination IP: `{{ macro.DP_Site_PrimarySIPAddr }}`
- Primary SIP Trunk Destination Port: `{{ macro.DP_Site_PrimarySIPPort }}`
- Secondary SIP Trunk Destination IP: `{{ macro.DP_Site_SecondarySIPAddr }}`
- Secondary SIP Trunk Destination Port: `{{ macro.DP_Site_SecondarySIPPort }}`

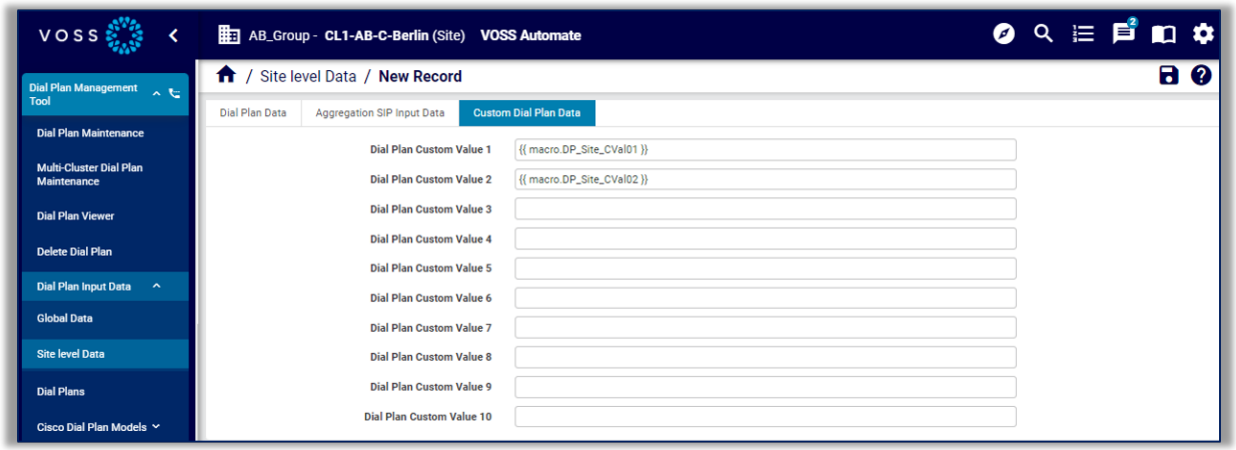


Site Custom Dial Plan Data Tab (Site)

Data from the provided fields may be referenced with the provided macros:

- Dial Plan Custom Value 1: `{{ macro.DP_Site_CVal01 }}`
- Dial Plan Custom Value 2: `{{ macro.DP_Site_CVal02 }}`
- Dial Plan Custom Value 3: `{{ macro.DP_Site_CVal03 }}`
- Dial Plan Custom Value 4: `{{ macro.DP_Site_CVal04 }}`
- Dial Plan Custom Value 5: `{{ macro.DP_Site_CVal05 }}`
- Dial Plan Custom Value 6: `{{ macro.DP_Site_CVal06 }}`
- Dial Plan Custom Value 7: `{{ macro.DP_Site_CVal07 }}`
- Dial Plan Custom Value 8: `{{ macro.DP_Site_CVal08 }}`
- Dial Plan Custom Value 9: `{{ macro.DP_Site_CVal09 }}`
- Dial Plan Custom Value 10: `{{ macro.DP_Site_CVal10 }}`

Copyright © 2025 VisionOSS Limited. All rights reserved.



Dial Plan Log

Logs that will record any dial plan push/remove actions within the system. The information is read only and informational.

Dial Plan Log

Timestamp in UTC	Dial Plan	Dial Plan Action	Dial Plan Elements	Launched By	Action Hierarchy	Hierarchy
2017-06-29 20:05:57.931482	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:39:03.092865	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:44:48.719970	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:47:13.973042	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:48:13.449928	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:53:32.707848	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:55:33.029889	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver

Dial Plan Log [2017-06-29 20:55:33.029889]

Timestamp in UTC	2017-06-29 20:55:33.029889
Dial Plan	Site_Level_DP
Dial Plan Elements	all
Dial Plan Action	push
Target Call Manager	["10.5.25.21", "8443", "hcs.VLS"]
Launched By	VLSAdmin
Action Hierarchy	sys.hcs.VLS.Tenant1.Vancouver

Log fields:

- Timestamp in UTS: The timestamp of the time the dial plan action was launched
- Dial Plan: The dial plan model applied
- Dial Plan Elements: Point to all or subset of dial plan elements.
- Dial Plan Action: Push or Remove

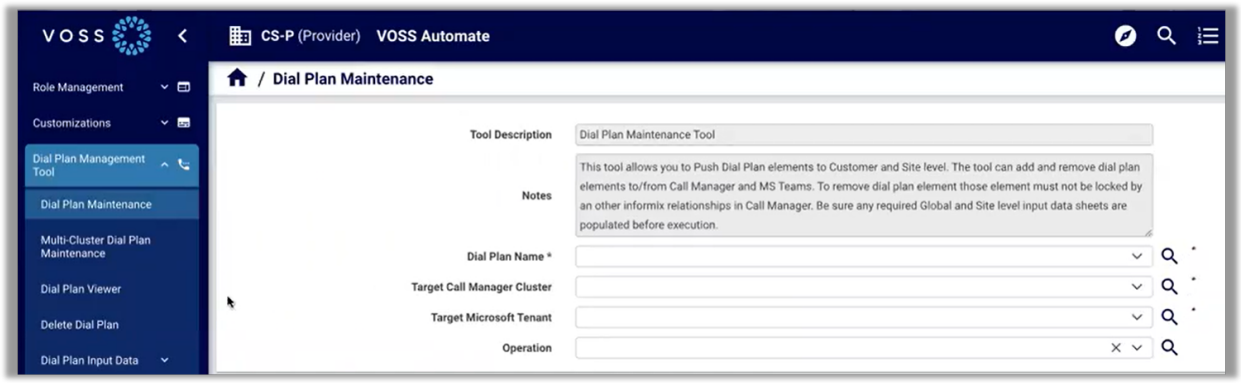
Copyright © 2025 VisionOSS Limited. All rights reserved.

- Target Call Manager: The URI to the destination Call Manager
- Launched By: The administrator who submitted the request
- Action Hierarchy: The hierarchy level at which the action was launched.

Dial Plan Maintenance

Overview

The **Dial Plan Maintenance** menu of the Dial Plan Management Tool allows you to push or remove dial plans to a selected target Cisco Unified Communication Manager (CUCM) cluster or to a Microsoft tenant.



You can use this tool at any hierarchy. The dial plan name should indicate at what level the dial plans may be used (customer or site).

Important: The Dial Plan Management Tool and associated menus is visible in an Enterprise environment, and hidden on Provider deployments. To expose this feature on Provider deployments, set the Global Setting "Enforce HCS Dial Plan" to *No*. For details, see:

- *Configure access profile for Cisco custom dial plans*
- *Configure the Cisco custom dial plan management menus*

You can tag dial plans in the dial plan model with their type (Multi-tenant/Shared Architecture, Global, Intermediate, or Site) to introduce error checking into the tool.

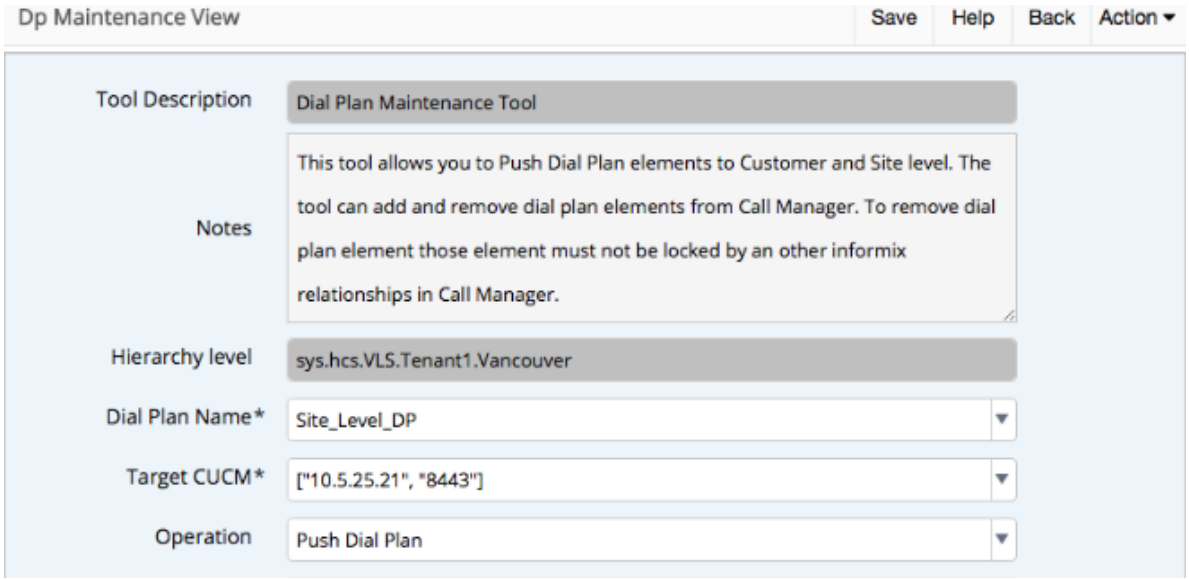
The dial plan name allows only dial plans meant for a specific hierarchy use to be shown in the Dial Plan Maintenance tool. For example, If an administrator is at customer level in VOSS Automate and uses the dial plan drop-down, the list of available dial plans are only those tagged "Global". We do this to ensure the dial plan models with hierarchy specific macros are executed at the correct hierarchy levels.

Copyright © 2025 VisionOSS Limited. All rights reserved.

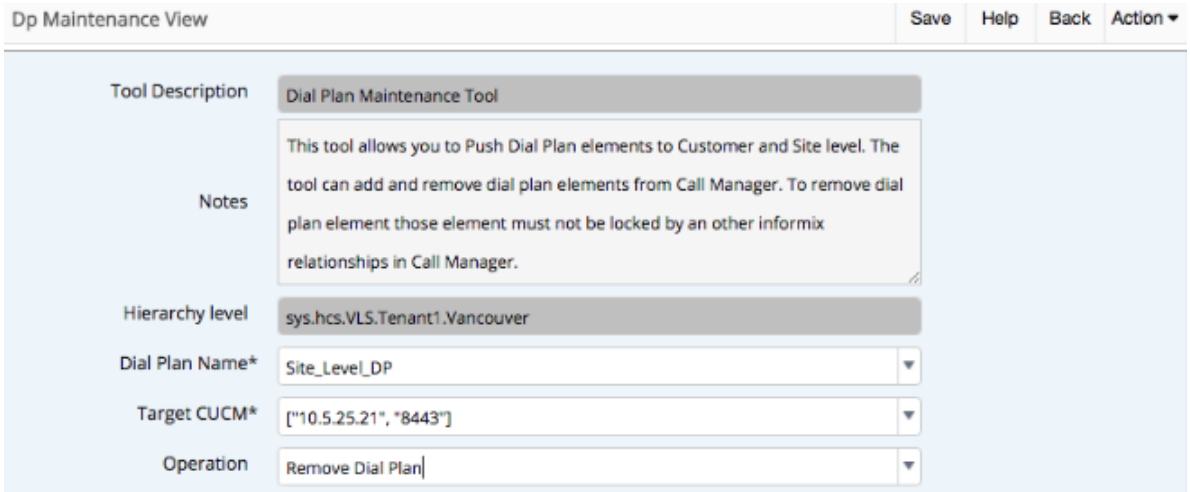
Push or Remove Dial Plan

The Dial Plan Maintenance tool provides two operations:

- Push dial plan



- Remove dial plan



Both push and remove operations work in the same manner:

1. A dial plan model is chosen from the **Dial Plan Name** drop-down.
2. A target CUCM or Microsoft tenant is chosen from the **Target Call Manager Cluster** drop-down.
3. Choose operation, **Push Dial Plan** or **Remove Dial Plan**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial Plan Management Tool

The **Dial Plan Management Tool** menus provide access to enhanced dial plan management functionality:

Important: By default, the Dial Plan Management Tool and associated menus is visible in an Enterprise environment, and hidden on Provider deployments. To expose this feature on Provider deployments, set the Global Setting "Enforce HCS Dial Plan" to *No*. For details, see:

- *Configure access profile for Cisco custom dial plans*
- *Configure the Cisco custom dial plan management menus*

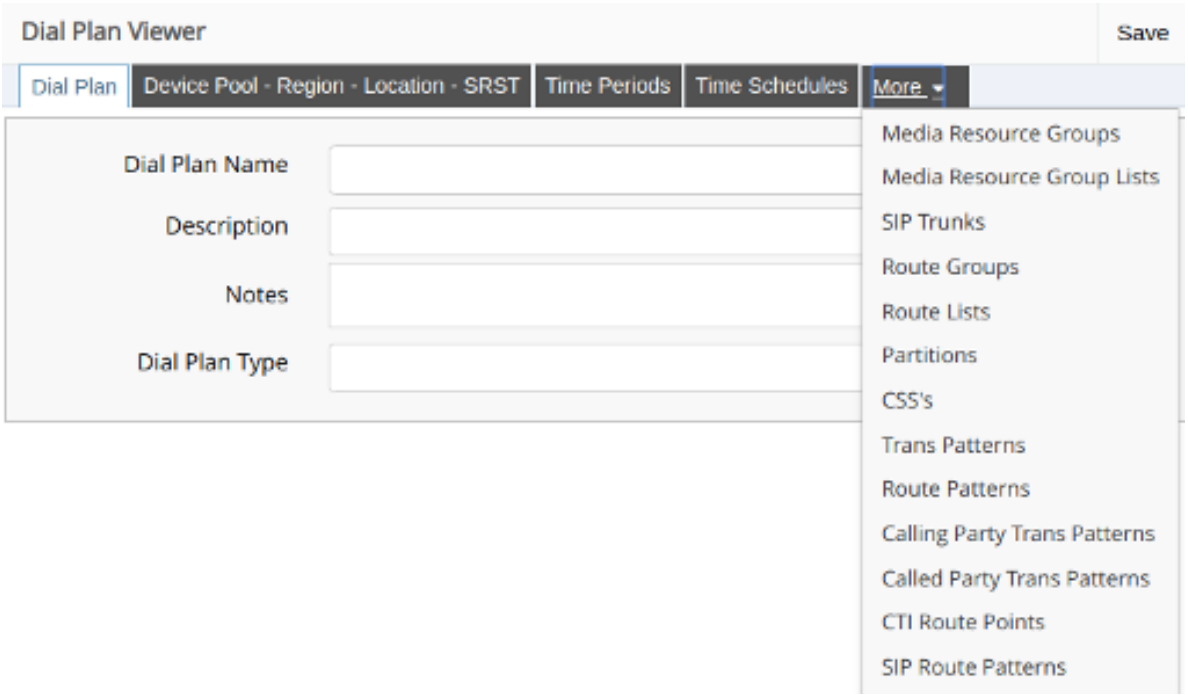
- **Dial Plan Maintenance** - this menu provides an interface for the dial plan you configured to be pushed to or removed from the selected, target CUCM cluster or Microsoft tenant.

  The hierarchy on which you push or pull the dial plan filters the list of dial plans, based on the dial plan type created on the dial plan models (Cisco or Microsoft).

  This utility can also be used to push a dial plan to the cluster for inspection and then to remove it again, provided no elements were added to the CUCM cluster or Microsoft tenant that rely on the dial plan elements. For example, adding phones on CUCM that would lock CSSs and partitions.

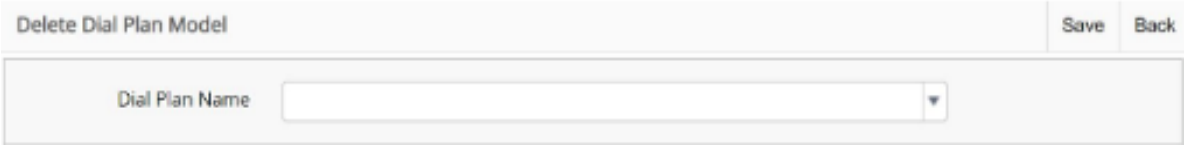
- **Dial Plan Viewer** - this menu provides a read-only view of all the dial plan elements of a selected dial plan you configured with the Dial Plan Management Tool. The contents of this view corresponds with the view of a dial plan schema, but in a format that is easier to inspect.

  Note: Details in the Dial Plan Viewer are read-only.



- **Delete Dial Plan Model** - this menu allows you to delete an entire dial plan you configured. All dial plan model elements associated with the selected dial plan model are removed, as well as the dial plan model itself.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- **Dial Plan Input Data** (Cisco-only) - an interface allowing lower level administrators to easily set up data to be added to either global or site level dial plan types. Custom dial plan data can also be included.

  In the individual dial plan elements, the values entered here are then referenced with macros, so that shared dial plan data can be managed efficiently.
- **Cisco Dial Plan Models** / **Microsoft Dial Plan Models** - a list of menus to manage elements of dial plans created with the feature. Individual elements - such as route patterns, SIP trunks, and translation patterns - are accessible for management via their menus.
- **Dial Plan Log** - a read-only record of Push and Remove operations carried out from the **Dial Plan Maintenance** menu. Recorded details include time and hierarchy of operation, target CUCM or Microsoft tenant, and dial plan name.

6.7.5. Custom Dialplan Tool - Cisco Routing Models

Setup and manage the Cisco routing models for the custom dialplan tool.

6.7.6. Custom Dialplan Tool - Cisco Basic Setup Models

6.7.7. Custom Dialplan Tool - Microsoft Dialplan Models

Set up and manage the Microsoft elements for the custom dialplan tool.

6.7.8. Cisco UCPrep Management

Introduction to UC Prep

Overview

Automate's UCPrep Profile tool streamlines the preparation process of deployment of Cisco applications with VOSS Automate Provider and Enterprise so that administrators won't have to repeat the same configuration tasks each time they stage or build a UC application.

The UCPrep Profile tool provides an easy, flexible, and repeatable way to define, store, and load static configurations and other infrastructure setup needed in the UC applications. One or more sets of static configuration data can be set up and stored.

The created static configuration can then be pushed to UC Apps as a "one-off", and does not always have to be tied into a overall workflow.

Note: Use of the UCPrep Profile tool can vary from provider to provider and even by customer within a provider.

Copyright © 2025 VisionOSS Limited. All rights reserved.

UCPrep feature scope

The UCPrep tool covers the following areas of the Cisco application deployment:

- CUCM Date Time Groups
- CUCM Groups
- CUCM Host Adjustment
- CUCM SIP Trunk Security Profiles
- CUCM SIP Profiles
- CUCM Audio Codec Preferences
- CUCM Application Users
- CUCM Feature Control Policies
- CUCM Route Filters
- CUC Authentication Policies
- CUC User Templates

It is not necessary to adjust all of these UC Application elements within a given UCPrep Profile. For example, if a Unity server is not part of a deployment, the CUC elements may remain un-configured. Similarly, if there is no need to adjust the hostname of a CUCM node, the input form tab for that configuration can remain empty.

Note: Pushing data must be run at the level of the apps.

UCPrep functionality in Automate

Tip: *Use the Action search to navigate Automate*

When the UCPrep feature is exposed on an Admin profile, links to related functionality is available on menus and dashboards in Automate to perform the UCPrep tasks.

A typical workflow involves setting up one or more UCPrep profiles for use, and then pushing these to the UC applications.

- Initial timezones can be selected before the UCPrep Profile configuration in order to simplify the management of the drop-down list of timezones in the tool.
- The UCPrep Application User List can also be set up where these are repeatedly used and pushed to UC Applications.
- The related Configuration Templates that drive the workflows of the configuration of the elements are grouped together for detailed customization and management.

Copyright © 2025 VisionOSS Limited. All rights reserved.

GUI	Description
UCPrep Profile Push	Used to push profile data into the target Cisco UC Applications.
UCPrep Profiles	The VOSS data structure that contains the configurations that can be repeatedly applied to UC applications.
UCPrep Friendly Timezones	List of timezones that is a mirror of the Call Manager available time zone database. This table is used to populate the Date/Time Group portion of the UCPrep Profile.
UCPrep Application User List	Administrator configurable list of Application Users that may be pushed into a Cisco Call Manager.
UCPrep Configuration Templates	Collection of configuration templates used to provision the individual UC application elements. Note that the menu item filters the configuration templates based on the prefix "ucprep". Should any configuration template be cloned for customization please use the prefix.

UCPrep profiles

Tip: *Use the Action search to navigate Automate*

Overview

The **UCPrep Profiles** list view displays all created profiles at the administrator's hierarchy and below.

UCPrep profiles are intended to be templates at a higher level in the hierarchy and are then cloned to a lower level for specific settings to a cluster. When cloning a UCPrep profile, the UCPrep profile name must be unique. UCPrep profile notes should also be descriptive so that this information is available when the UCPrep Profile Push tool is used.

For example, a provider level profile may contain global element configuration that are not site or cluster specific. At a customer or site level, this profile can then be cloned and updated with configuration elements that apply to the customer or site.

UCPrep profiles settings

You can select the following tabs on this page:

- UCPrep Profile
- CUCM Date Time Groups
- CUCM Groups
- CUCM Host Adjustment
- CUCM SIP Trunk Security Profiles
- CUCM SIP Profiles
- CUCM Audio Codec Preferences
- CUCM Application Users

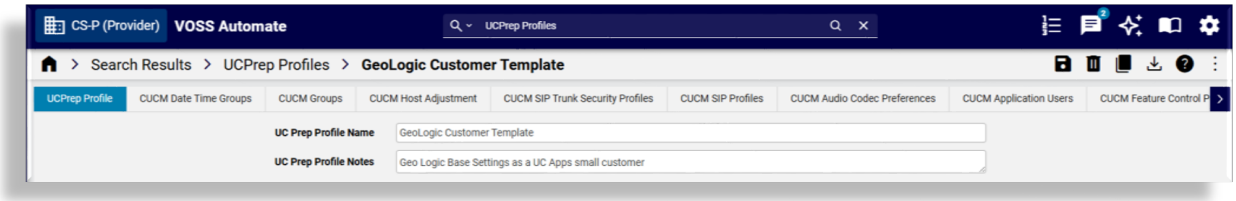
Copyright © 2025 VisionOSS Limited. All rights reserved.

- CUCM Feature Control Policies
- CUCM Route Filters
- CUCM Phone Services
- CUCM SIP Normalization Scipts
- Unity Authentication Policies
- Unity User Templates

UCPrep Profile tab

The table describes settings on the UCPrep Profile tab:

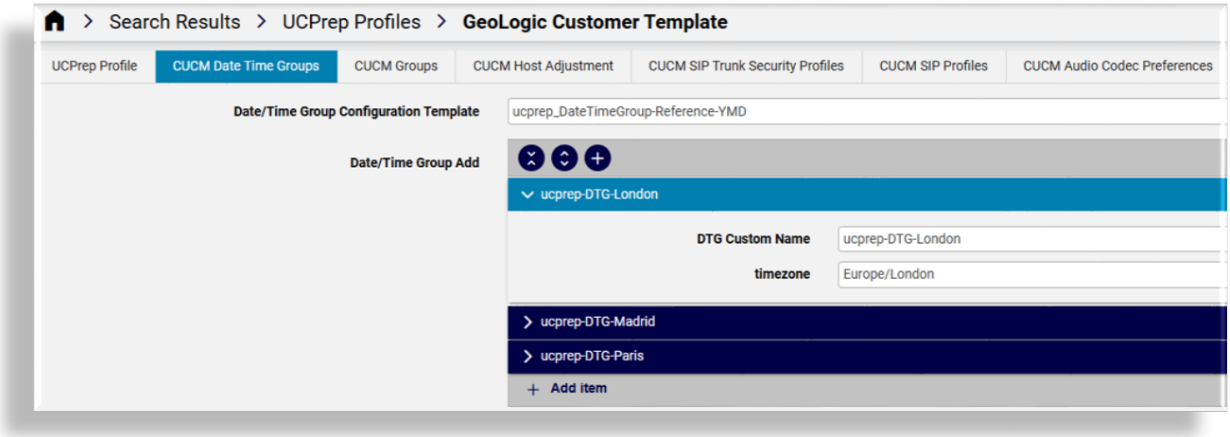
Field	Description
UC Prep Profile Name	Friendly name for the UCPrep profile. This is the name populated into the push tooling above.
UC Prep Profile Notes	Fill out helpful information describing the UCPrep Profile. This is the field populated to the push tooling above.



CUCM Date Time Groups tab

Configuration templates can be customized and added so that these become available in the **Date/Time Group Configuration Template** drop-down list, for example to templates to customize the date format and listed on the **UCPrep Configuration Templates** page.

The **UCPrep Friendly Timezones** page can be used to manage the list available in the **timezones** drop-downs, for example to shorten the list to only include the timezones that are used in the Data/Time groups.



Copyright © 2025 VisionOSS Limited. All rights reserved.

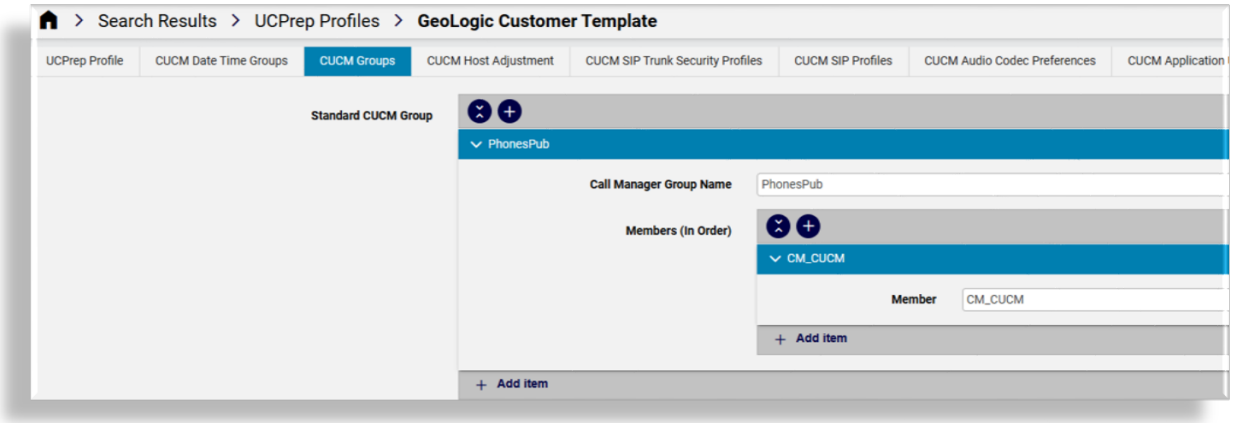
The table describes settings on the CUCM Date Time Groups tab:

Field	Description
Date/Time Group Configuration Template	Configuration template used to configure the specific settings to a Data-Time Group in Call Manager. Options available in the Configuration template are date format, separator, Time format, and so on. Note: the name of the date time group is automatically configured based on the chosen timezone entry. A timezone drop-down entry of `America/New_York` will create a date time group named `America-New_York`.
Date/Time Group Add	Timezones are chosen and added via drop-down. Any number of timezones may be chosen.

CUCM Groups tab

The **Members** drop-down works once a UCPrep profile has been cloned to the level of the UC applications.

The order in which the members are added indicate primary and secondary members of the group.



The table describes settings on the CUCM Groups tab:

Name	Description
Standard CUCM Group	Entry mechanism to allow for configuration of an unlimited number of Call Manager Groups.
Call Manager Group Name	Free text entry box for Call Manager Group Name.
Members (In Order)	Add Call Manager nodes via drop-down by adding member entry boxes. The Call Manager nodes are added to the Call Manager Groups in the order presented in the input box.

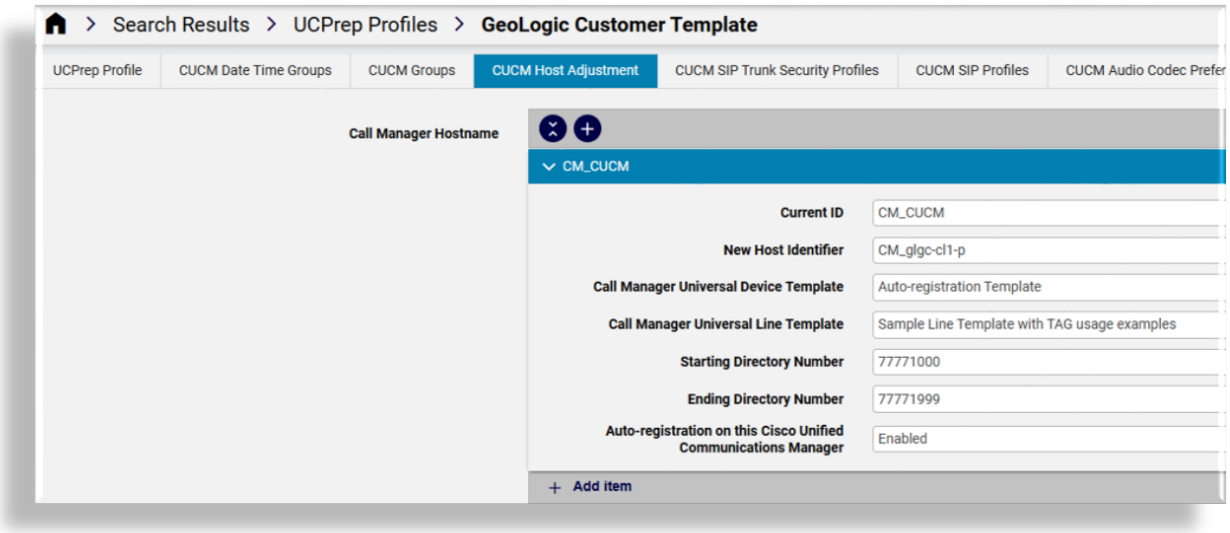
Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Host Adjustment tab

Multiple nodes of the cluster at the hierarchy can be modified.

Considerations for Host Adjustment are:

- Since the CUCM Host Adjustment modifies existing data in Call Manager, the data must be re-set or removed if a UCPrep Profile must be applied more than once.
- The CUCM Host adjustment occurs after the Call Manager Group configuration because the Call Manager will internally adjust the node names within a Call Manager Group when the node is renamed.
- If a node name is adjusted and a UCPrep profile is run a second or more times, the data on the **CUCM Groups** tab must be updated from the drop-downs to be the current CUCM node name.



The table describes CUCM Host Adjustment tab settings:

Copyright © 2025 VisionOSS Limited. All rights reserved.

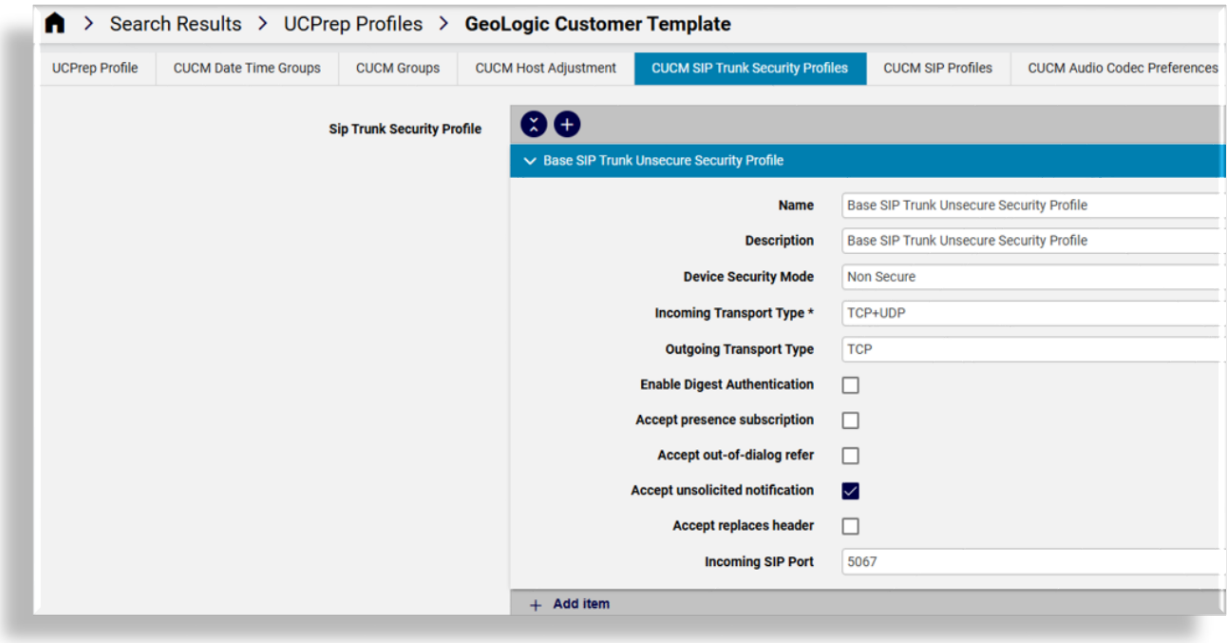
Name	Description
Call Manager Hostname	Entry area for multiple Call Manager Hostname adjustments.
Current ID	Drop-down providing the current Call Manager node names in the cluster.
New Host Identifier	Free text area to enter the new name as per business standards.
Call Manager Universal Device Template	Drop-down providing the CUCM configured Universal Device Templates. These templates are only required when configuring auto-registration on the Call Manager Node.
Call Manager Universal Line Template	Drop-down providing the CUCM configured Universal Line Templates. These templates are only required when configuring auto-registration on the Call Manager Node.
Starting Directory Number	Free text field for entry of starting directory number for auto-registration.
Ending Directory Number	Free text field for entry of ending directory number for auto-registration.
Auto-registration Enabled on this Cisco Unified Communications Manager	Check box to enable auto-registration on the Call Manager node.

CUCM SIP Trunk Security Profiles tab

The table describes settings on the CUCM SIP Trunk Security Profiles tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

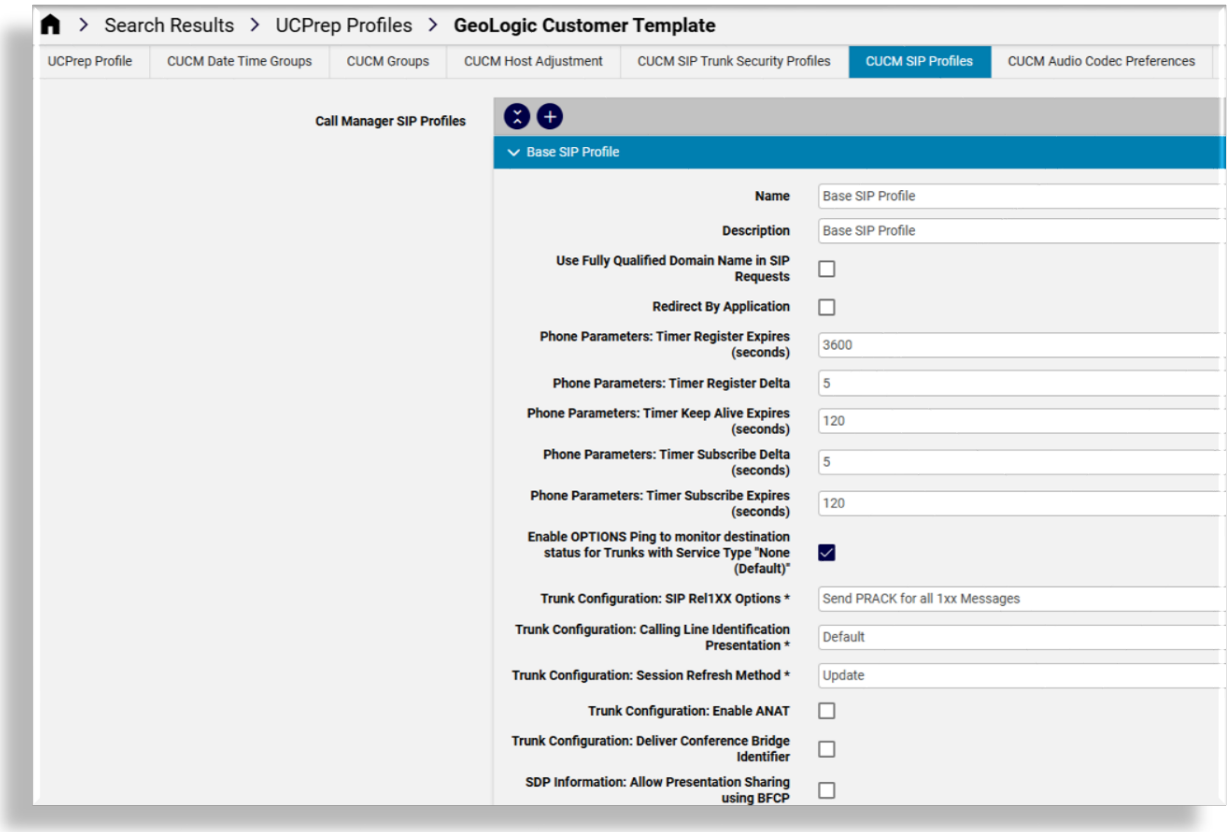
Field	Description
Name	Free text field to enter Sip Trunk Security Profile name.
Description	Free text field to enter Sip Trunk Security Profile description.
Device Security Mode	Drop-down providing options: • Non Secure • Authenticated • Encrypted
Incoming Transport Type	Drop-down providing options: • TLS • TCP and UDP
Outgoing Transport Type	Drop-down providing options: • TCP • UDP • TLS
Enable Digest Authentication	Check box to enable Digest Authentication.
Accept presence subscription	Check box to enable Accept of presence subscription.
Accept out-of-dialog refer	Check box to enable Accept out-of-dialog refer.
Accept unsolicited notification	Check box to enable Accept unsolicited notification.
Accept replaces header	Check box to enable Accept replaces header.
Incoming SIP Port	Free text box to set Incoming SIP Port.



Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM SIP Profiles tab

Where values or time settings display on the page when adding a profile, these are the static values corresponding with the Call Manager defaults.



The table describes settings on the CUCM SIP Profiles tab:

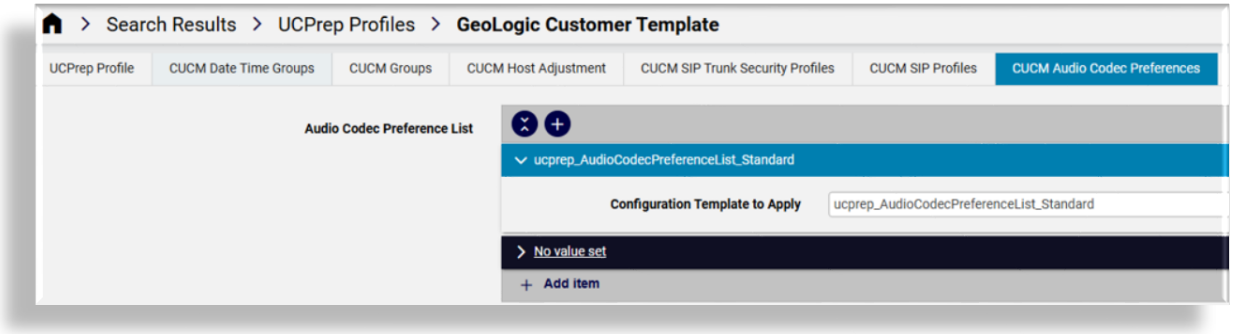
Copyright © 2025 VisionOSS Limited. All rights reserved.

Field Name	Description
Call Manager SIP Profiles	Entry box to add any number of SIP Profile definitions.
Name	Free text field to enter name of SIP Profile.
Description	Free text field to enter description of SIP Profile.
Use Fully Qualified Domain Name in SIP Requests	Check box to enable Use Fully Qualified Domain Name in SIP Requests.
Phone Parameters: Timer Register Expires (seconds)	Free text box to adjust the Timer Register Expired timeout. Default 3600
Phone Parameters: Timer Register Delta	Free text box to adjust the Timer Register Delta. Default 5
Phone Parameters: Timer Keep Alive Expires (seconds)	Free text box to adjust the Timer Keep Alive Expires. Default 120
Phone Parameters: Timer Subscribe Delta (seconds)	Free text box to adjust the Timer Subscribe Delta. Default 120
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type “None (Default)”	Check box to Enable OPTIONS Ping.
Trunk Configuration: SIP Rel1XX Options	Drop-down providing options • Disabled • Send PRACK if 1xx Contains SDP • Send PRACK for all 1xx Messages
Trunk Configuration: Calling Line Identification Presentation	Drop-down providing options • Default • Strict From URI presentation Only • Strict Identity Headers presentation Only
Trunk Configuration: Session Refresh Method	Drop-down providing options • Invite • Update
Trunk Configuration: Enable ANAT	Check box to enable ANAT
Trunk Configuration: Deliver Conference Bridge Identifier	Check box to enable Deliver Conference Bridge Identifier.
SDP Information: Allow Presentation Sharing using BFCP	Check box to enable Allow Presentation Sharing using BFCP

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Audio Codec Preferences tab

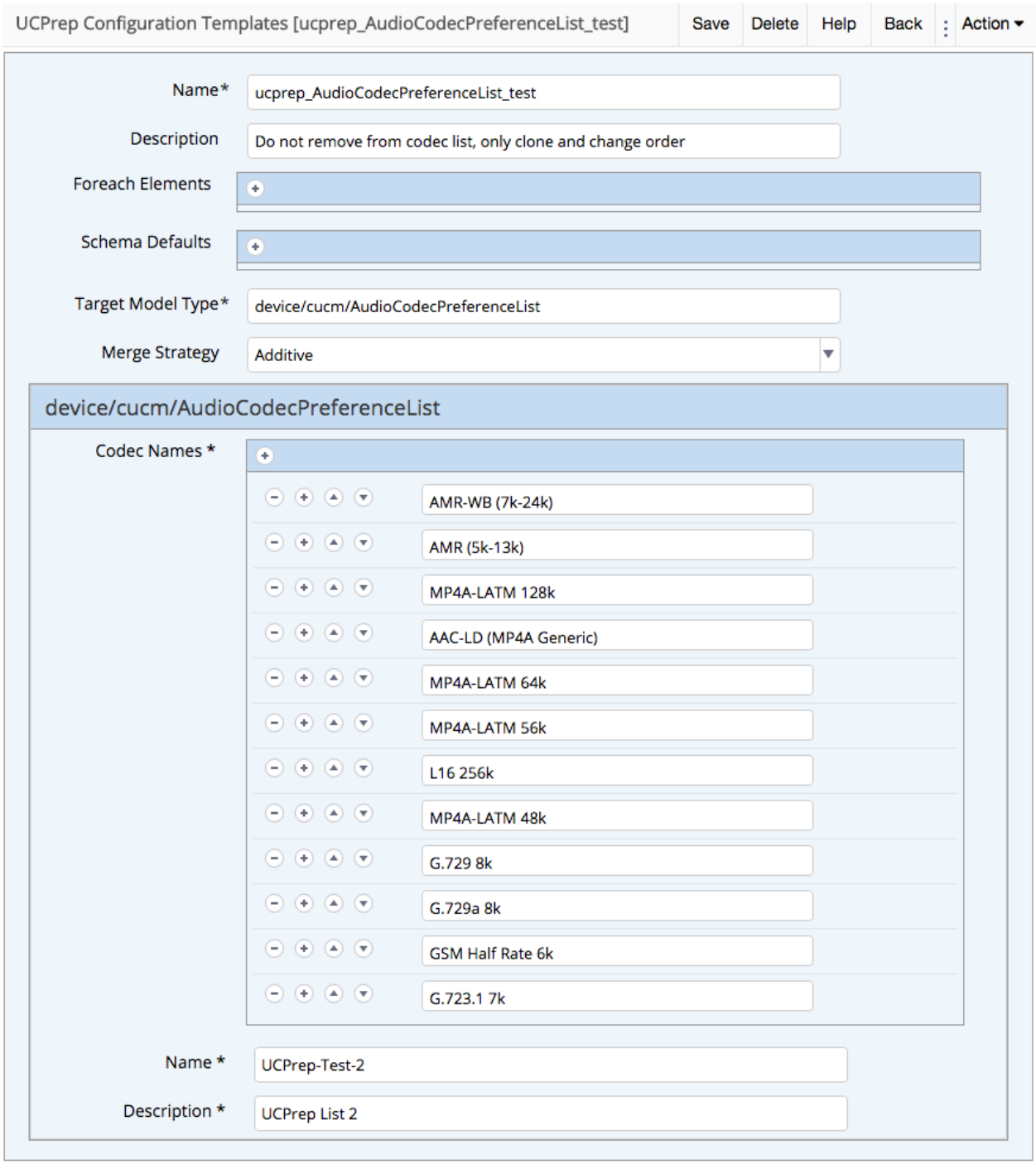
The Audio Codec Preferences List lends itself to be driven by a configuration template rather than a GUI input of a list of codecs.



The lists are written to Call Manager by selecting any number of configuration templates that have been set up to list out groups of codecs. Typically, a configuration template from the menu **UCPrep Configuration Templates** list view is cloned and modified to show the required codecs and settings.

Audio Codec Preference List Configuration Template Example:

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes the settings on the CUCM Audio Codec Preferences tab:

Field	Description
Audio Codec Preference List	Entry mechanism for any number of Codec lists.
Configuration Template to Apply	Drop-down providing a list of available configuration templates.

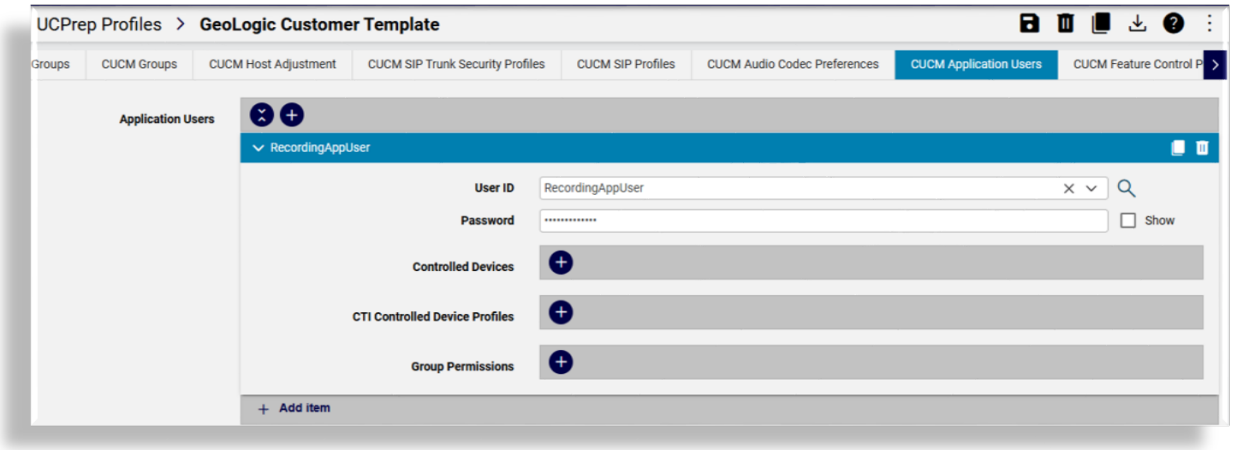
Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Application Users tab

Application users can initially be set up from the **UCPrep Application User** page, to be available from the **Application Users** drop-down on the input form of this tab.

New application users can also be added on the form by entering the user name directly into the **Application Users** input.

Application user roles are automatically added from the selected **Group Permissions**.



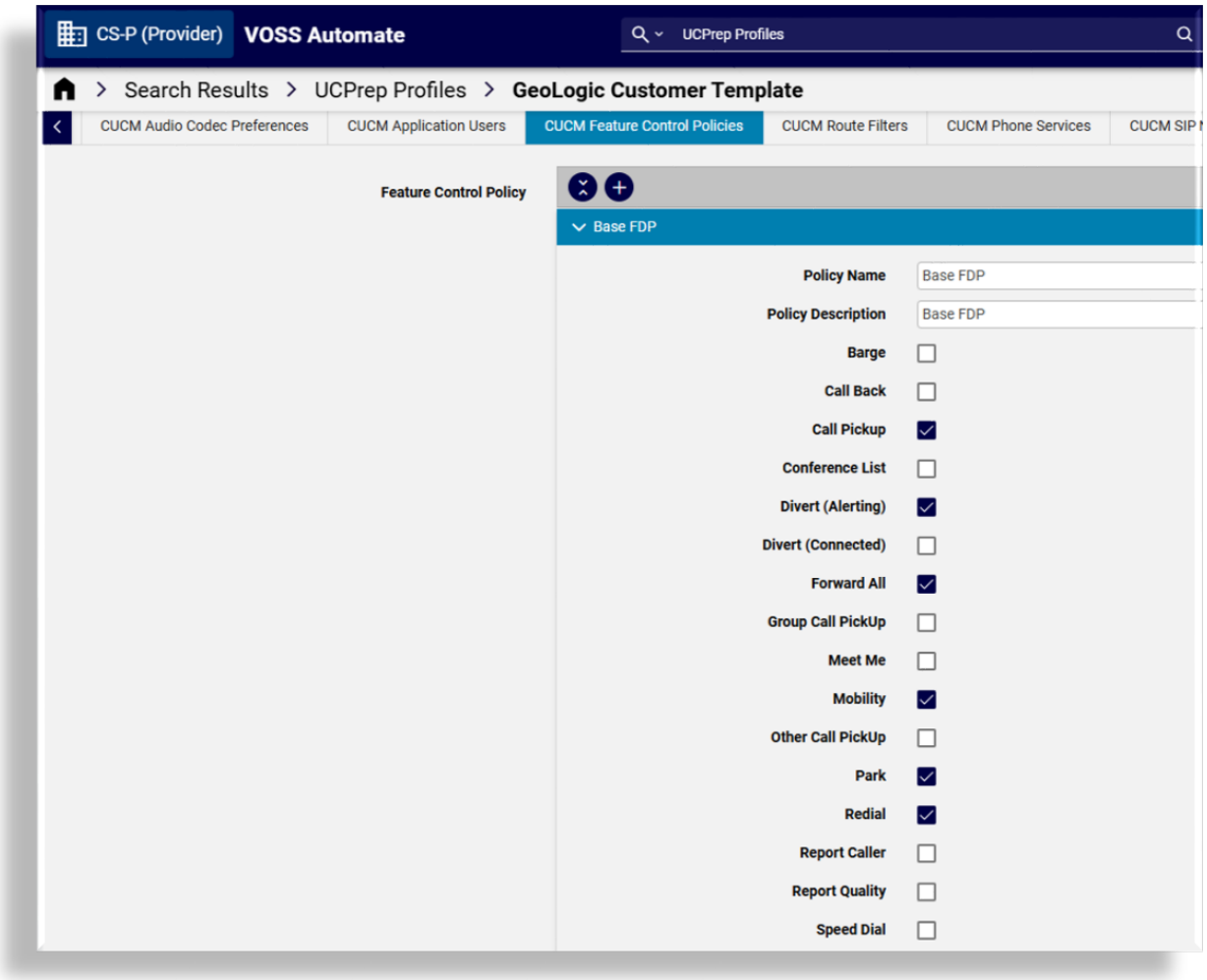
The table describes the settings on the CUCM Application Users tab:

Field Name	Description
Application Users	Mechanism for adding an unlimited number if application users to a Call Manager.
User ID	The Application User ID. This drop-down is driven from the UCPrep Application User List in the menu. The idea behind this is to cut down on AppUser misspelling.
Password	Password for the application user
Repeat Password	Confirmation of entered password.
Controlled Devices	Drop-down that provides a list of configured devices on Call Manager should an association be necessary.
CTI Controlled Device Profiles	Drop-down that provides a list of configured device profiles on Call Manager should an association be necessary.
Group Permissions	Drop-down that provides the ability to build group permissions for the application user. The drop-downs will provide all configured groups from the Call Manager.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM Feature Control Policies tab

Feature control policies are defined by entering policy names and selecting features from the list of check-boxes.



The table describes the settings on the CUCM Feature Control Policies tab:

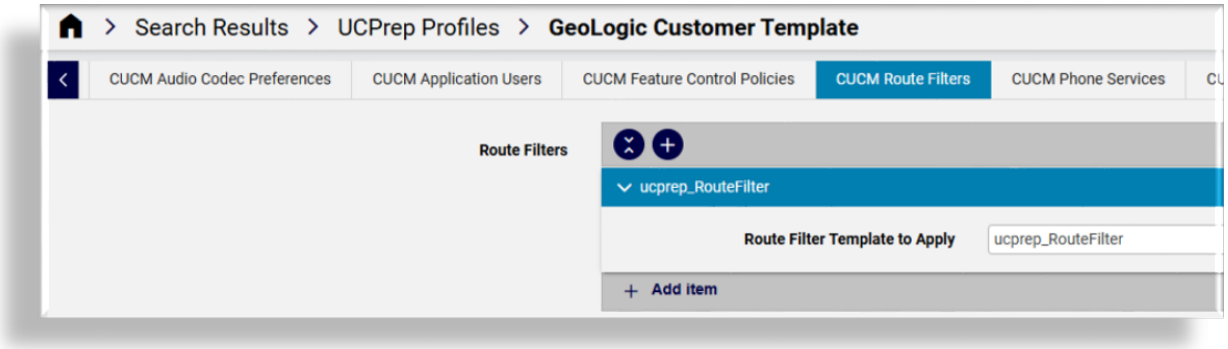
Copyright © 2025 VisionOSS Limited. All rights reserved.

Field Name	Description
Feature Control Policy	Mechanism to enter an unlimited number of Feature Control Policies
Policy Name	Free text field for entry of Feature Control Policy Name.
Policy Description	Free text field for entry of Feature Control Policy Description.
Check boxes to add the individual services into the Feature Control Policy	• Barge • Call Back • Call Pickup • Conference List • Divert (Alerting) • Divert (Connected) • Forward All • Group Call PickUp • Meet Me • Mobility • Other Call PickUp • Park • Redial • Report Caller • Report Quality • Speed Dial

CUCM Route Filters tab

The Route Filter lends itself to be driven by a configuration template rather than a GUI input of clauses.

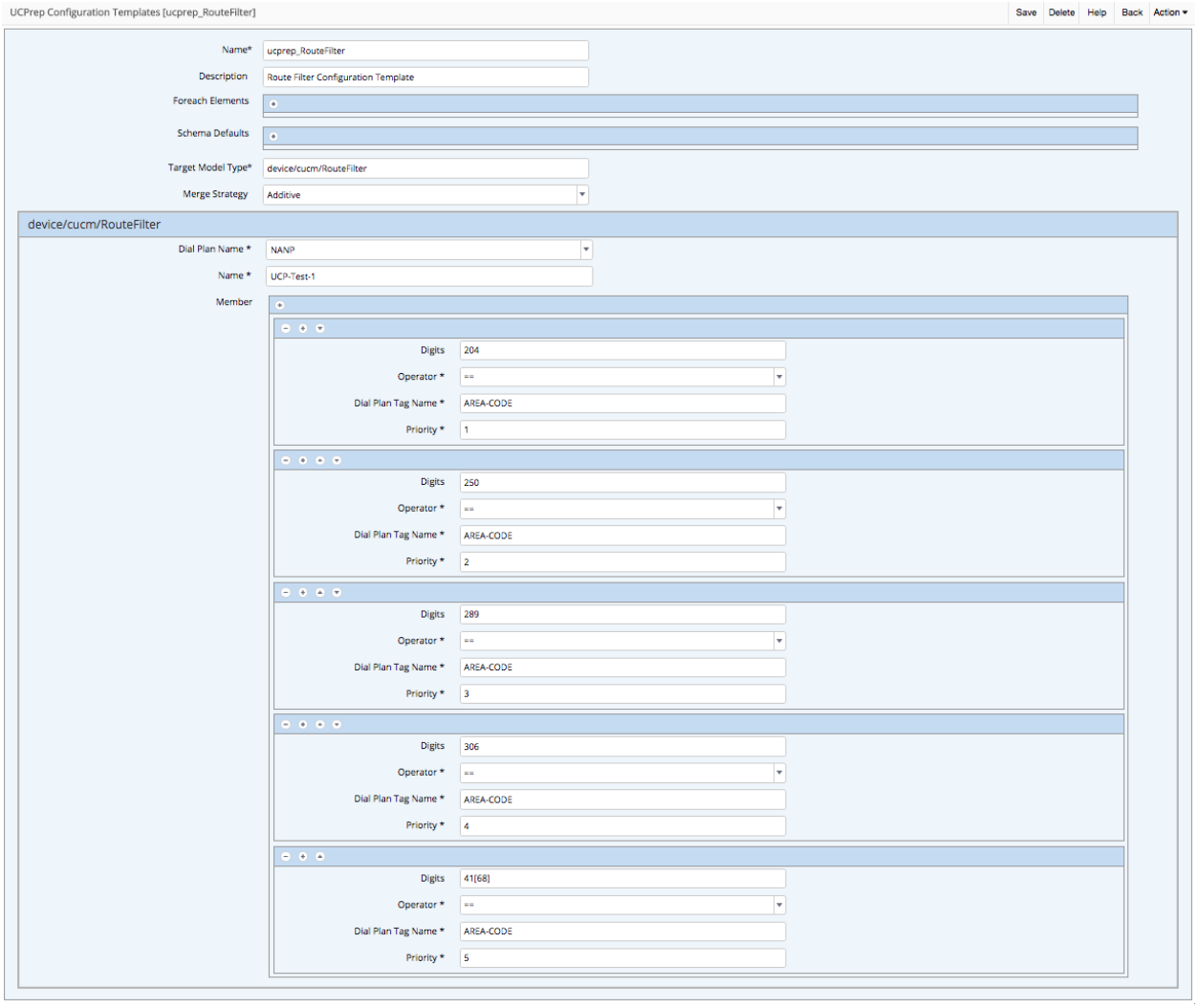
The filters are written to Call Manager by selecting any number of configuration templates from the **Route Filter Template to Apply** drop-down on the input form.



Typically, a configuration template from the menu **UCPrep Configuration Templates** list view is cloned and modified to show the required Route Filter settings.

Example of Route Filter Configuration Template:

Copyright © 2025 VisionOSS Limited. All rights reserved.



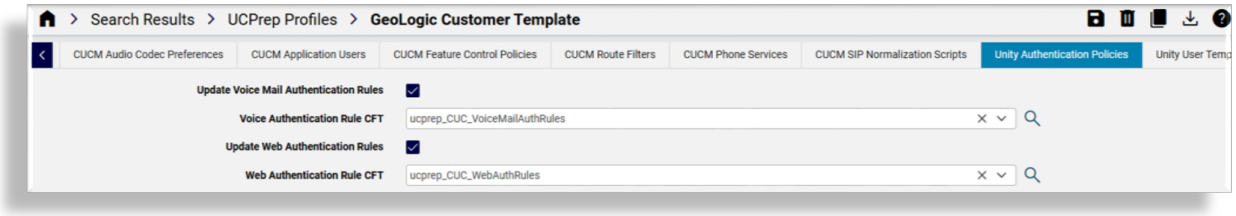
The table describes the settings on the CUCM Route Filters tab:

Field	Description
Route Filters Route Filter Template to Apply	Mechanism to add an unlimited number of route filters via configuration template. Drop-down to provide a list of available configuration templates.

Copyright © 2025 VisionOSS Limited. All rights reserved.

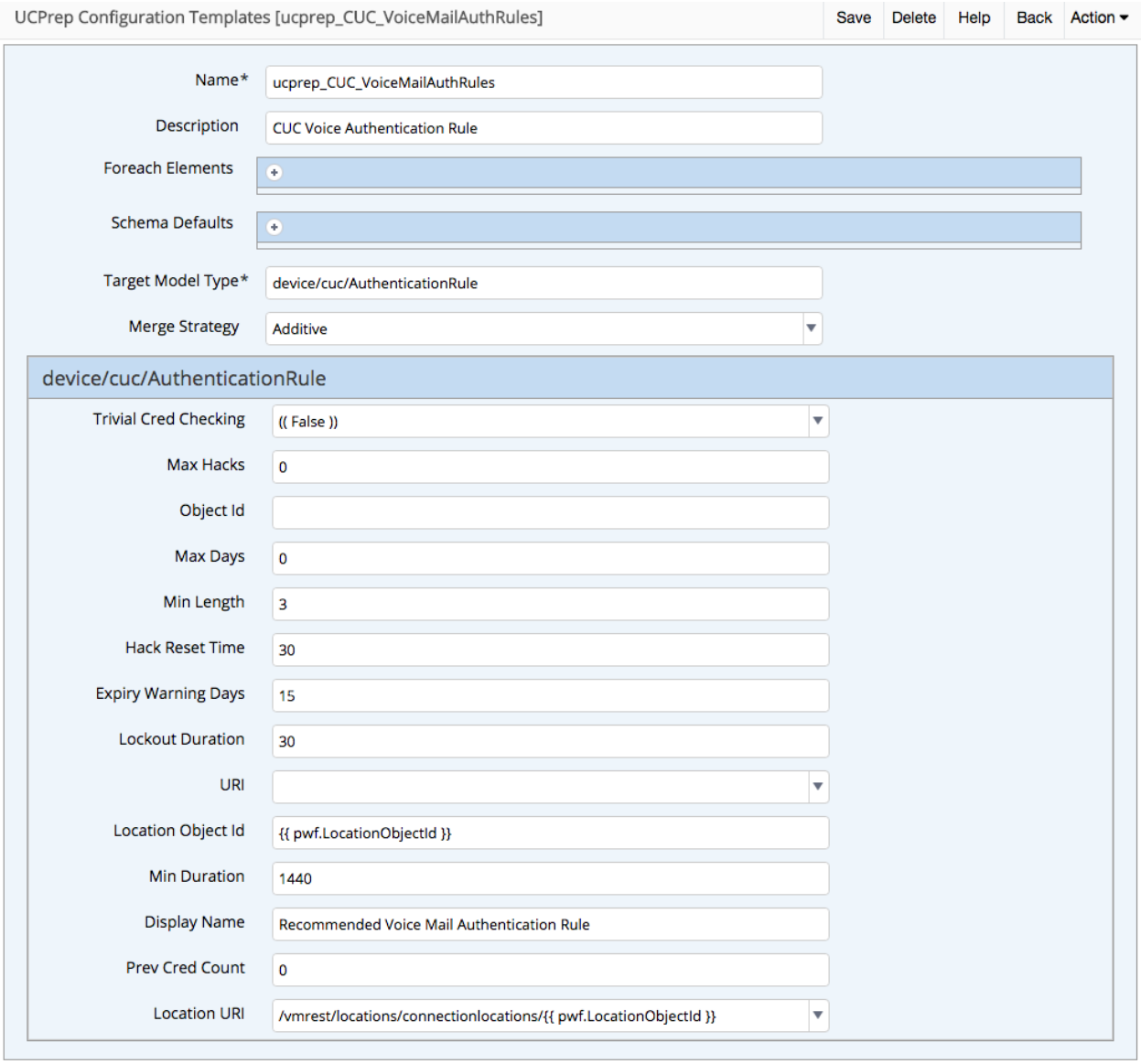
Unity Authentication Policies tab

The Unity authentication rule lends itself to be driven by a configuration template rather than a GUI input, since settings commonly do not change and the same group of settings are repeated.



Typically, configuration templates from the menu **UCPrep Configuration Templates** list view are cloned and modified to show the required Voice and Web Authentication Rules.

Example of Authentication Rule Configuration Template:



Copyright © 2025 VisionOSS Limited. All rights reserved.

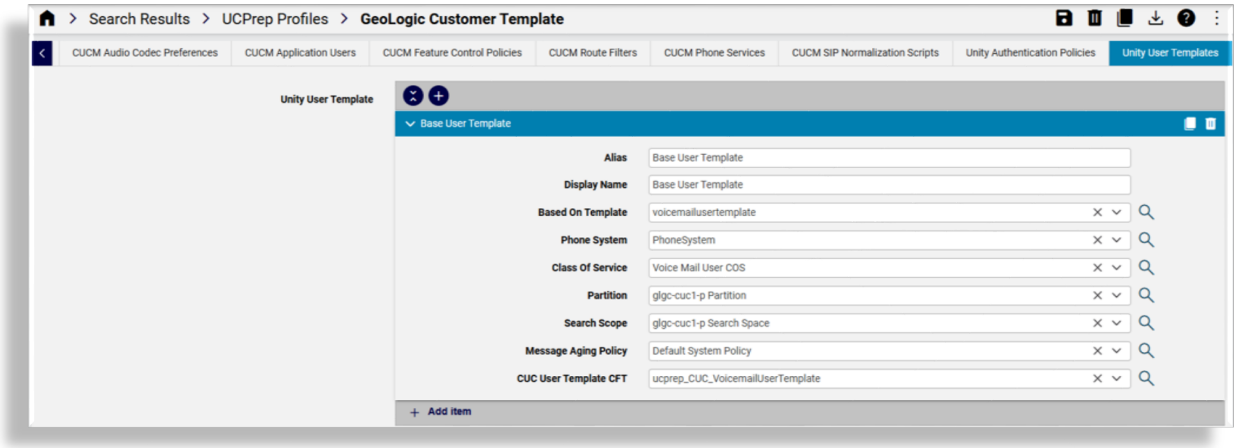
The table describes the settings on the Unity Authentication Policies tab:

Field	Description
Update Voice Mail Authentication Rules	Check box to enable the update of the Voice Mail Authentication Rule from the UCPrep Profile.
Voice Authentication Rule CFT	Drop-down providing a list of available configuration templates.
Update Web Authentication Rules	Check box to enable the update of the Web Authentication Rule from the UCPrep Profile.
Web Authentication Rule CFT	Drop-down providing a list of available configuration templates.

Unity User Templates tab

The list of user templates shown on the input form are those that are most often changed. Own templates can be added as new entries and options selected from the available drop-downs.

Additional required fields can be added by selecting a created Configuration Template containing these from the **CUC User Template CFT** drop-down.



The table describes the settings on the Unity User Templates tab:

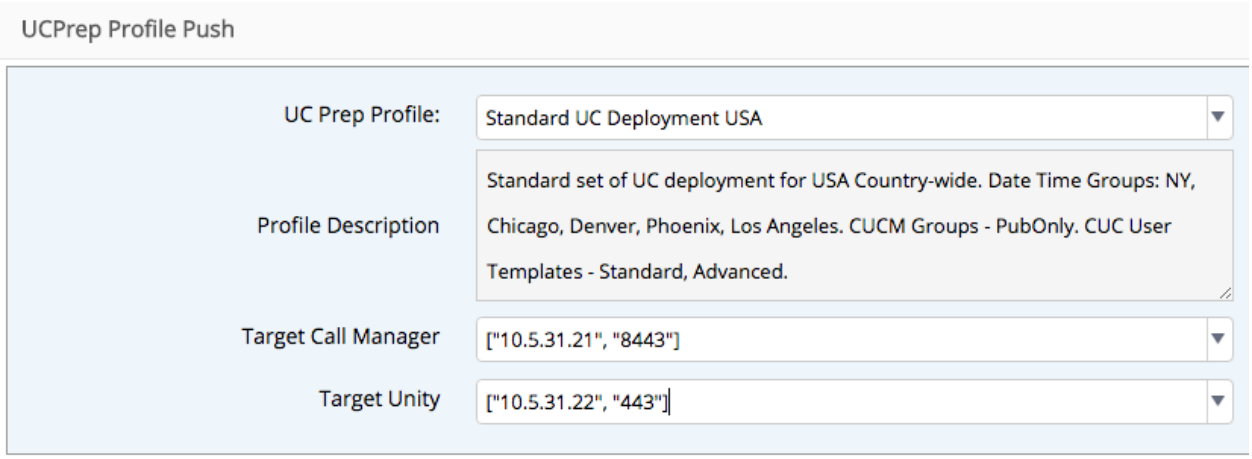
Copyright © 2025 VisionOSS Limited. All rights reserved.

Field Name	Description
Unity User Template	Mechanism to enter an unlimited number of user templates.
Alias	Free text field to enter the User Template Alias.
Display Name	Free text field to enter the User Template Display Name.
Based On Template	Drop-down providing a list of Unity configured templates to use as the required reference.
Phone System	Drop-down providing the Unity configured phone system.
Class Of Service	Drop-down providing the Unity configured and available Class of Service.
Partition	Drop-down providing the Unity configured and available Partitions.
Search Scope	Drop-down providing the Unity configured and available Calling Search Spaces.
Message Aging Policy	Drop-down providing the Unity configured and available Message Aging Policies.
CUC User Template CFT	The VOSS configuration template, which will be used to populate the unexposed fields of a User Template.

UCPrep Profile Push

Tip: *Use the Action search to navigate Automate*

UCPrep Profile Push configuration settings



Copyright © 2025 VisionOSS Limited. All rights reserved.

Name	Field Description
UCPrep Profile	Drop-down providing the available UCPrep Profiles configured on the system.
Profile Description	Description populated automatically when a UCPrep Profile is chosen from the UC Prep Profile drop-down.
Target Call Manager	Cisco Call Manager to which the UCPrep Profile Data will be pushed.
Target Unity	Cisco Unity server to which the UCPrep Profile Data will be pushed.

6.7.9. HCS Dial Plan Tools - For use with managed HCS Dialplans

Introduction to Cisco HCS dial plan

provider

Tip: *Use the Action search to navigate Automate*

Overview

Automate Provider solution supports Cisco HCS dial plan tools.

Custom (non-HCS) Cisco dial plans are also supported for Enterprise deployments. For details, see *Appendix: Optional Features* in this guide. The Cisco custom dial plan is independent of the hierarchy schema approach of the Cisco HCS dialplan. However, it can also be used in conjunction with schema-based dial plan management.

Note: For Microsoft dial plan, see *Microsoft Teams Dial Plan Management* in this guide.

Related topics

- Dial Plan Schemas in the Provider HCS Dial Plan Management Guide
- Dial Plan Schema Groups in the Provider HCS Dial Plan Management Guide
- Associate Custom Dial Plan Schema Group in the Provider HCS Dial Plan Management Guide
- Emergency and CLI Settings in the Provider HCS Dial Plan Management Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Example workflow for Cisco HCS dial plan

This section provides a high level example workflow for a Cisco HCS dial plan.

Note: See also the Provider HCS Dial Plan Management Support Guide for additional details around using Cisco HCS dial plans in Automate.

1. Mandatory. Deploy country dials plans (for countries other than United States or United Kingdom).

   Note: This task is mandatory when using country dial plans other than US or UK. For details, see the "Provider HCS Dial Plan Management Support Guide".

2. Apply customer dial plan at customer.
3. Apply site dial plan at site.
4. Optional. Configure Class of Service (CoS) at site.
5. Add Directory Number Inventory at customer or site.
6. Optional. Configure E.164 Inventory at customer or site.
7. Optional. Configure E.164 Number to Directory Number associations at customer or site.
8. If not using Site Location Codes (that is, you have deployed a Type 4 Dial Plan), configure Directory Number Routing at site to enable intra- and inter-site calls.
9. Optional. Configure Short Codes at site.
10. Edit Site Defaults as follows:
    a. On the **Device Defaults** tab, set the default Automate device CSS to an appropriate device Class of Service.
    b. On the **Line Defaults** tab, set the Default UCM Line CSS to an appropriate line Class of Service.
11. For offnet PSTN call configuration, see the "Provider HCS Dial Plan Management Support Guide".
12. For Local Breakout (LBO) configuration, see "IOS Device Management".
13. For user, phone, and line configuration, see "User Management".

Cisco shell schema groups

To deploy your own existing dial plan rather than one of Cisco's out-of-the-box dial plans, use the shell schema group to enable core functionality without deploying a pre-configured Automate schema group.

The shell schema group provides a starting point for you to build your own dial plan. The shell schema group has no preset site default values other than Default Device Pool and Default UCM Group. The shell schema group does not contain any default core schemas, features schemas, or country schemas. You can clone the shell schema group instance and tailor all other settings to your own specifications.

On the **Custom Workflows** tab, the shell schema group provides default workflows for the following registry events used to create customer inventories and associations:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Registry event	Description
addDnInventory	Allows you to create DN inventory without enforcing any rules or constraints on the DN numbers
addE164Inventory	Allows you to create E164 inventory without enforcing any rules or constraints on the E164 number other than enforcing the country code prefix for a given site
associateE164ToDn	Allows E164 to DN number association (N to N) on Automate without configuring anything on Cisco Unified CM
unassociateE164ToDn	Removes E164 to DN number association (N to N) from Automate without removing anything on Cisco Unified CM
associateE164ToSingleDn	Allows E164 to DN number association (N to 1) on Automate without configuring anything on Cisco Unified CM
unassociateE164ToSingleDn	Removes E164 to DN number association (N to 1) on Automate without removing anything on Cisco Unified CM

Note: For more information on configuring schema groups and associating them with customers, see the *Provider HCS Dial Plan Management Support Guide*.

Dial plan roles and privileges

provider

Administrators can perform all tasks associated with their roles, as well as all dial plan tasks that are lower on the navigation hierarchy.

Hierarchy is shown from left (highest) to right (lowest) in the table below.

The table lists out dial plan privileges for administrators, depending on the role assigned:

Tasks	HCS Admin	Provider / Reseller Admin	Customer Admin	Site Admin
Create a Customer Dial Plan	X (Customer level)	X (Customer level)	X (Customer level)	
Create a Site Dial Plan	X (Site level)	X (Site level)	X (Site level)	
Configure Class of Service	X (Site level)	X (Site level)	X (Site level)	
Configure Short Code	X (Site level)	X (Site level)	X (Site level)	X
Configure Directory Number Routing	X (Site level)	X (Site level)	X (Site level)	X
Add Directory Numbers	X (Customer level)	X (Customer level)	X	
View Directory Number Inventory	X (Site level)	X (Site level)	X (Site level)	

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

Tasks	HCS Admin	Provider / Reseller Admin	Customer Admin	Site Admin
Configure SIP Route Patterns	X (Site level)	X (Site level)	X (Site level)	
Create Voice Mail Service	X (Provider/Reseller level)	X (Provider/Reseller level)		
Associate Voice Mail Services to Customer	X (Customer level)	X (Customer level)		
Define a Voice Mail Pilot Number	X (Customer level)	X (Customer level)	X (Customer level)	
Associate Pilot Numbers to a Site	X (Site level)	X (Site level)	X (Site level)	
Configure SIP Trunks	X	X	X	
Reset SIP Trunks	X	X	X	
Restart SIP Trunks	X	X	X	
Configure Route Groups	X	X	X	
Configure Route Lists	X (Customer or Site level)	X (Customer or Site level)	X	
Configure Device Pools	X (Customer or Site level)	X (Customer or Site level)	X	
Provision Emergency Calls	X			
Create Schemas	X	X		
Modify Site Defaults	X (Site level)	X (Site level)	X (Site level)	
Assign Custom Schemas to Customers	X (Customer level)	X (Customer level)		
Configure Unified CM Groups	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Regions	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Route Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Route Partitions	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Calling Search Spaces	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Translation Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Calling Party Transformation Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Called Party Transformation Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- For more information on bulk loading, see the topics on Bulk Administration.

HCS dial plan macros in Automate

Macros can be used in Automate to dynamically add site IDs, customer IDs, and other types of information when customizing dial plan schemas and Class of Service. Macros increase ease of use and reduce error.

Macros are evaluated within the context of a particular hierarchy node based on the scope specified in the schema group binding, for example, site, customer, provider.

The correct syntax for a macro is the word “macro” followed by a period (.), followed by the named macro.

Add double curly brackets ({{ }}) around the entire macro combination.

For example, `{{ macro.HcsDpCustomerName }}` is the macro combination created using the first named macro in the table below. Note that there are no spaces in a named macro.

This table provides a list of named macros - see also the named macros in the Automate documentation index:

Named Macro	Description
HcsDpCustomerName	Name of the customer (as specified when you create your customer)
HcsDpCustomerId	Systemwide, unique internal customer ID generated when you create a customer
HcsDpSiteName	Name of the site (as specified when you create a site under a customer)
HcsDpSiteId	Systemwide, unique internal site ID generated when you create a site
HcsDpUniqueCustomer PrefixMCR	Default unique Cisco HCS customer prefix in the form ‘Cu{{ macro.HcsDpCustomerId }}’
HcsDpUniqueSite PrefixMCR	Default unique HCS site prefix in the form ‘Cu{{ macro.HcsDpCustomerId }}Si {{ macro.HcsDpSiteId }}’
HcsDpSiteCountryMCR	Returns the country associated with a specific site
HcsDpSiteCountryIso	Returns the ISO 3166-1 alpha-3 three-letter country code associated with the country that is associated with a specific site
HcsDpPstnBreakout	Returns the PSTN prefix digit for the country that is associated with a specific site
HcsDpSiteAreaCode InLocalDialingMCR	Returns True if a specific site requires area code for local PSTN dialing
HcsDpSiteNatTrunk PrefixMCR	Return the national trunk prefix associated to a particular site
HcsDpDefaultSite DevicePoolMCR	Default Cisco HCS site device pool Cisco Unified Communications Manager element name
HcsDpDefaultSite LocationMCR	Default Cisco HCS site location Cisco Unified Communications Manager element name
HcsDpDefaultSite RegionMCR	Default Cisco HCS site region Cisco Unified Communications Manager element name

Copyright © 2025 VisionOSS Limited. All rights reserved.

The table lists macros that can be used to loop through the area codes specific for a particular site when adding translation patterns:

Named Macro	Description
HcsDpSiteAreaCodeMCR	Returns list of area codes associated with a specific site
HcsDpSiteAreaCode Item_AreaCodeMCR	Return the area code attribute from the area code list item
HcsDpSiteAreaCode Item_LocLenMCR	Return the local number length attribute from the area code list item

Related Topics

- Macro Evaluate Function in the Advanced Configuration Guide
- Create an Evaluation Macro in the Advanced Configuration Guide
- Macro Evaluator in the Advanced Configuration Guide

Dial plan schemas

This procedure configures a customized group of related dial plan elements in Cisco Unified Communications Manager (Cisco UCM), including time periods, time schedules, partitions, calling search spaces, translation patterns, calling and called party transformations, CTI route points, route lists, route patterns, and SIP route patterns.

Note: When configuring a dial plan schema using this procedure, the elements are only available on the UCM after the dial plan schema is placed in a dial plan schema group (refer to Create Schema Groups), and once the group is associated with a customer (refer to Associate Custom Schemas to Customers).

It is strongly recommended that all dial plan entries in a dial plan should be unique.

Perform these steps:

1. Log in to Automate as a Provider or Reseller administrator.
2. Go to **Dial Plan Schema**.
3. To add a new custom schema, click **Add**.
4. On the **General** tab, enter a unique name for the schema, and (optionally) add a description.
5. On the **Time Periods** tab, click the Plus icon (+) to open the form for time period information, and fill out required details:
   - Define a name and (optionally) a description for the time period.
   - At **Time of Day Start** and **Time of Day End**, choose a start and end time.
   - (Optional) At **Start Day**, **End Day**, **Start Month**, and **End Month**, choose the day and month characteristics of the time period, as required.
   - (Optional) Fill out values for **Start Day of the Month** and **End Day of Month**.
   - Click **OK**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. On the **Time Schedules** tab, click the Plus icon (+) to open the form to add time schedule information, and fill out details for the schema:
   - Enter a name and a description for the time schedule.
   - At **Time Periods**, click the Plus icon (+) to add a time period name, and click **OK**.
7. On the **Partitions** tab, click the Plus icon (+) to open the form for adding partition details, then enter a partition name and description, and provide the time schedule.

   Note: You can use macros to add partition information. For more information on using macros as part of the Partition Names, Descriptions, or Time Schedules, see Macros.

8. On the **Calling Search Spaces** tab, click the Plus icon (+), then fill out CSS details for the schema:

   Note: You can use macros to add calling search space (CSS) details.

   - Enter a CSS name and (optionally) a description.
   - At **Partition Usage**, enter a reason for the CSS.
   - If this CSS is used in a class of service, select the **Class of Service CSS** checkbox.
   - To add more detail about the partitions for this CSS, click the Plus icon at **Partitions**, then add a route partition name and an index.
   - Click **OK**.
9. On each of the following tabs, click the Plus icon (+) to open the editing form, and fill out the relevant details for the schema.
   - Translation Patterns tab
   - Calling Party Transformation Patterns tab
   - Called Party Transformation Patterns tab
   - CTI Route Points tab
   - Route Lists tab (to add route lists)
   - Route Patterns tab (to add route patterns)
   - SIP Route Patterns tab (to add SIP route patterns)
10. Click **Save** to create the new dial plan schema.

Next steps

- Create schema groups to add dial plan schemas to a schema group.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Auto-cloning of dial plan schemas and schema groups to the provider hierarchy node

All existing dial plan schema and schema groups are cloned automatically from the System Administration level in Automate 10.x/11.5(x) to the Provider hierarchy node when the following events occur:

- You create a new provider
- You perform an upgrade from a previous version of Automate

New dial plan schema files and schema groups are also cloned automatically to existing Provider hierarchy nodes when the following events occur:

- You load or import a country dial plan template that introduces additional dial plan schema files or schema groups at the System Admin level, the new additional schema files are cloned automatically to any existing Provider hierarchy nodes.
- New dial plan schema or schema groups are created using native GUI, REST API, native bulk loader, imported JSON files, or using the app install template, the new schema and schema groups are cloned automatically to existing Provider hierarchy nodes.

The cloned version at the Provider level has the same name and is an exact replica of the dial plan schema or schema group at the System Admin level except that the Description field in the **General** tab of the schema indicates that it is the Cloned instance version.

Note: The auto-cloning mechanism does not clone a schema or schema group to the Provider level if there is already one at the Provider level with the same name.

Auto-cloning of the dial plan schema and schema groups to the Provider level ensures that any dial plan schema and schema group changes you make to existing Cisco templates are not lost when a Cisco template upgrade is introduced. As a Provider, you can also add your own schemas and schema groups at the Sys Admin level and be confident that these will be cloned down to the Provider level and not be overwritten by upgraded Cisco templates.

Your dial plan schema changes are retained because when you deploy new customers and sites, the system searches up the hierarchy node tree to find the first instance of a particular template name to use for the deployment.

For example, when deploying the Customer Call Screening feature schema for a customer, the system searches up the hierarchy node tree for the first instance of the CustomerCallScreening-Feature-V1-SCH. It will find two instances of CustomerCallScreening-Feature-V1-SCH:

1. CustomerCallScreening-Feature-V1-SCH (at the Provider level - e.g. sys.hcs.p1)
2. CustomerCallScreening-Feature-V1-SCH (at the System Administration level - e.g. sys-hcs)

Because the schema names are identical and the Provider hierarchy node is found first, the Provider level CustomerCallScreening-Feature-V1-SCH schema is used to deploy the customer. Any customizations you made to the CustomerCallScreening-Feature-V1-SCH schema at the Provider level are retained if the template at the System Administration level gets updated by an upgrade.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Clone dial plan schemas

Tip: *Use the Action search to navigate Automate*

This procedure copies one of the default dial plan schemas (or a previously customized schema) to use as a starting point when creating a new dial plan schema.

1. Log in to Automate as Provider or Reseller administrator.
2. Go to **Dial Plan Schema**.
3. From the list of dial plan schemas, choose the one to be cloned, by clicking on its box in the leftmost column. For more information on the default dial plan schemas, refer to Default Dial Plan Schemas.

   Note: There may be duplicate dial plan schemas in the list because some of the dial plan schemas may have been auto-cloned to the Provider hierarchy node. For more information, see Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node.

4. Click **Action** > **Clone**.
5. From the **General** tab, enter a new unique name for the cloned dial plan in the Dial Plan Name field.
6. If desired, add a description of the new cloned dial plan schema in the Description field.
7. Modify or add time periods, time schedules, partitions, calling search spaces, translation patterns, calling party transformation patterns, called party transformation patterns, CTI route points, route lists, route patterns, and SIP route patterns as desired by clicking on the appropriate tab.
8. Click **Save**. The new dial plan schema appears in the list of Dial Plan Schemas.

Line classes of service

provider

Tip: *Use the Action search to navigate Automate*

Configure class of service for a site

This procedure creates a new Calling Search Space (CSS) or edits an existing CSS that is tied to a site. The CSS can be used as a Class of Service (COS) for a device or line, or any of the other templates that rely on COS to filter different features.

1. Log in as provider, reseller, or customer administrator.
2. Select the relevant site.

   Note: When adding CoS, ensure you select a valid site under the customer in the hierarchy. You can only add CoS at a site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Go to **Line Classes of Service**.

   Note: There is one default Internal Calling Line Identification Presentation (CLIP) CoS that appears in the list. The default CoS is provisioned automatically based on the criteria you selected when you added the site.

4. Choose an option:
   - To add a CoS, click **Add**.
   - To edit an existing CoS, click on the relevant CoS, make your changes, then save.
   - To clone an existing CoS, click on the relevant CoS, then click **Action > Clone**.
5. Fill out a unique name for the CoS in the **Class of Service Name** field.

   Note: Ensure the name is descriptive, using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_). You can also use macros in Automate to create a CoS name. See the Automate documentation for a list of possible macros.

   MMacros allow you to dynamically add site IDs, customer IDs, and other types of information to the CSS.

   Example: `Cu1-24HrsCLIP-PT-{{macro.HcsDpSiteName}}`

   The actual CSS that is sent to the UCM (based on the macros entered) is mirrored in the **Actual Calling Search Space** field. For example, the macro example above changes to `Cu1-24HrsCLIP-PT-SiteABC`.

6. Optional. Fill out a description for the CoS.
7. Choose route partition members to include in the CoS:
   a. Click the Plus icon (+) to add route partitions.
   b. From the drop-down, select a route partition member.
   c. Repeat this step until you have selected all the members you need for this CoS. If you want to remove any member from the CoS, click the Minus icon (-).
8. Click **Save** to add the new CoS. The new CoS will display in the summary list view, from where you can update it or delete it in future, if required.

   When adding (including clone), updating, or deleting CoS, you can view transaction progress and details in the Transaction Logs.

Related topics

- Transaction Logging and Audit in the Core Feature Guide
- Class of Service in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Clone a class of service for a site

This procedure clones an existing Class of Service (CoS) to the same site hierarchy node, with a new name.

1. Log in as provider, reseller, customer, or site administrator.

   Note: When cloning a CoS, ensure that you select a valid site under the customer in the hierarchy. Attempting to clone a CoS at any other node (at a customer or reseller for example), a system error reminds you that you must be at a site.

2. Go to **Class of Service**.
3. Click on the Class of Service to be cloned.
4. Click **Action** > **Clone**.
5. Fill out a unique name for the Class of Service in the **Class of Service Name** field.

   Note: Ensure the name is descriptive, using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).

6. Optionally, fill out a description.
7. Save the cloned CoS. This creates a new CoS.

   When adding (including clone), updating, or deleting CoS, you can view transaction progress and details in the Transaction Logs.

   Note: Save the cloned CoS to the same site hierarchy as the original CoS. You can't save the clone to a different site or to a different hierarchy.

   The new CoS displays in the summary list view, from where it can be updated or deleted in future, if required.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Dial plan schema group

Tip: *Use the Action search to navigate Automate*

This procedure bundles a set of schemas to form a custom dial plan. You can clone one of default Type 1 to Type 4 schema groups to use as a starting point to create your own dial plan schema group.

1. Log in to Automate as Provider or Reseller admin.
2. Go to **Dial Plan Schema Group**.
3. From the list of dial plan schema groups, select the schema group to be cloned.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: There may be duplicate dial plan schema groups in the list because some of the dial plan schema groups may have been auto-cloned to the Provider hierarchy node. For more information, see *Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node*.

4. From the **General** tab, enter a new unique name for the cloned dial plan schema group in the Dial Plan Schema Group Name field.
5. Optionally, add a description of the new cloned dial plan schema group in the **Description** field.
6. Modify or add site defaults, core schemas, feature schemas, country schemas, or custom workflows as required by clicking on the appropriate tab as follows:
   a. From the **Site Defaults** tab, modify site defaults. For more information on site defaults, refer to Modify Site Defaults.

      Note: If a site defaults doc (SDD) for a site is based on `CUSTOMER_TEMPLATE`, then any empty values set under this tab will *not* result in empty values being set in the site dial plan. Values that are set on the **General** tab in the `CUSTOMER_TEMPLATE` will be applied instead.

   b. From the **Core Schemas** tab, modify the fields. Select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the hierarchical level for the core schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.
   c. From the **Feature Schemas** tab, modify the fields. Select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the hierarchical level for the feature schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the feature schema that will be triggered by the event. This drop-down list includes all default and created feature schemas from the Create Schemas procedure.
   d. From the **Country Schemas** tab, modify the fields as required. For desired country schemas, select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the country dial plan from the Country Name drop-down menu. Select the hierarchical level for the country schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the country-specific schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.
   e. From the **Custom Workflows** tab, modify event workflows. From the Dial Plan Event drop-down menu, select an event trigger for your workflow. Contact Advanced Services if you require an event trigger that is not in the list. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Workflow drop-down menu, select the custom workflow to execute when the dial plan event is triggered.
7. Click **Save**. The new dial plan schema group appears in the list of groups.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- Introduction to Cisco HCS Dial Plan in the Core Feature Guide

Site dial plans

provider

Cisco

Tip: *Use the Action search to navigate Automate*

Overview

A site can be associated with only one dial plan.

A Cisco HCS site dial plan is not automatically created for a site when the site is created. Instead, once the first site is deployed for a specified customer, the customer-level dial plan elements are provisioned on Cisco Unified Communications Manager (CUCM), followed by the site-specific, Cisco HCS dial plan elements. Each subsequent site takes less time to create as they have only site-specific dial plan elements to provision.

For customers with two or more sites, the site dial plan must be applied to each site.

Only one site dial plan can be added at a time against a specific CUCM. Parallel transactions are disallowed. When adding a site dial plan, its transaction workflow acquires a lock that prevents a parallel transaction for adding another site dial plan from completing. The lock value is unique per CUCM.

If you try adding another site dial plan while a transaction is in progress for the first one you added, the transaction for the second dial plan starts and is in progress for 3 minutes, trying to acquire the lock. If it cannot acquire the lock, the second transaction fails with this message:

Failed to Add Cisco HCS Site Dial Plan, a Site Dial Plan is currently being added for this Unified CM, please wait for that transaction to complete, or wait 15mins for the lock to auto expire in the case that a failed transaction did not release the lock automatically

If the first transaction fails, the lock is set to auto-expire after 15 minutes.

Related topics

- *Customer HCS Dial Plan*

Add a Cisco HCS site dial plan

This procedure creates a Cisco HCS site dial plan and associates the dial plan with a site.

Pre-requisites:

- Create the customer dial plan. See *Customer HCS Dial Plan*

  You can only create a site dial plan once the customer dial plan exists because there are attributes defined in the customer dial plan that are required when the site dial plan is created.

Copyright © 2025 VisionOSS Limited. All rights reserved.

1. Log in to the Admin portal as a Provider administrator or Customer administrator.

   Note: For details around tasks that can be performed for each admin level, see *Dial plan roles and privileges*.

2. Go to the **Dialplan Tools** > **Cisco Site Dialplans**, then view existing site dial plans in the list view.
3. Click the Plus icon (+) to add a new site dial plan; then, select the site.
4. On the **Dial Plan** / **New Record** page, configure the dial plan. The table describes the configuration options:

Field	Configuration
External Breakout Number	Fill out the one digit external breakout number for the country associated with the site. The external breakout number is the PSTN prefix that is used when deploying a country dial plan. The default is 9. For Cisco HCS Type 1 to 4 dial plan schemas, country dial plans are deployed at the Customer level. The country dial plan is pushed to CUCM once the first site associated with a given country is deployed. For example, if a site is associated with the United States (USA), and it is the first site dial plan being created for the USA, the USA country dial plan is deployed as part of creating the site's dial plan. Automate supports only one external breakout number for each country. For example, all sites within the USA have the same external breakout as the first site within the USA.
Use extension prefix	Defines, for sites without Inter-Site Prefixes (ISPs), whether this dial plan uses the extension prefix from the customer dial plan. Displays only if your customer dial plan does NOT use ISPs, for example, HCS Type 3 dial plans (SLC, no ISP, DN=SLC+EXT). When enabled, this setting is applied ONLY if there is an extension prefix defined in the customer dial plan.
Area Codes	Click the Plus icon (+) to add valid local area codes for the site, if required. For each area code you add: • Fill out the area code. • Specify the length of the subscriber part of the PSTN number. **Note:** The area code is used to generate the PSTN local route patterns for the site. For example, in the USA, if area codes are added for Dallas, Texas, the area codes could be specified for local dialing as 214, 469, and 972, with a subscriber length of 7. The **Local Number Length** field defines the length for the subscriber section of the entire E.164 number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Configuration
Site Location Code	Displays only when the customer dial plan uses site location codes. Fill out the site location code (SLC). The maximum number of digits is 8. The SLC must be unique across sites for a customer.
Extension Length	Fill out the number of digits for the extension (between 1 and 30 digits).
Area Code Used for Local Dialing	Defines whether the area code is required for local dialing from this site. **Note:** In the USA, this setting defines whether you use 7-digit or 10-digit local dialing.
Published number	Select from the available E.164 inventory numbers, or fill out a custom number. **Note:** The site published number is the default E.164 mask when a line is associated to a phone at a particular site.

Field	Configuration
Emergency Call Back Number	Select from the available E.164 inventory numbers, or fill out a custom number. **Note:** Site emergency call-back number is the calling number when initiating an outgoing emergency call. It can be used when you use Extension Mobility and make an emergency call from a site other than your own. It can be used when the emergency call goes out to the PSTN network, when the system includes the site emergency number so that the origin of the call is known. The system adds this calling party transformation to the DN2DDI4Emer-PT partition. The emergency call back number is not the number to dial for an emergency. Instead, it is the number used to identify the calling party for emergency calls originating from a particular site.
Use DDI for emergency calls	Define whether to use DDI for emergency calls when user is at home location.
Site ID	A read-only field that displays a unique, auto generated number for each customer site, which is prefixed to elements as an identifier (for example, Cu4Si2 indicates Customer 4, Site 2).

5. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

View transaction progress and details in the Transaction Logs.

The new site dial plan is added. The system takes a few minutes to provision the site dial plan, especially for the first site. The site information is loaded on CUCM, and is identifiable by its Customer ID, Site ID prefix.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Update a Cisco HCS site dial plan

provider

Cisco

This procedure updates a Cisco HCS site dial plan.

1. Log in as the Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the site where you want to update the dial plan.
3. Go to the **Dial Plan** page.
4. In the list view, click on the site dial plan where you want to make changes.
5. On the **Dial Plan** page, you can update the following:

Field	Description
Area Code	You can modify or delete existing area codes, or add new area codes.
Local Number Length	The length of a locally dialed number for the specified area code.
Area Code Used for Local Dialing	Defines whether the area code is included in locally dialed calls.
Published Number	The site published number is the default E.164 mask when a line is associated to a phone at a particular site.
Emergency Call Back Number	The site emergency call-back number is the calling number when initiating an outgoing emergency call.

6. Click **Save**.

   View transaction progress and details in the Transaction Logs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Area code changes in Cisco HCS site dial plans

For the Cisco Type 1-4 dial plans, area code changes result in the affected local dialing translation patterns getting reapplied for the site:

When adding new area codes	New translation patterns are deployed to the site, based on the country dial plan schema associated with the site.
When deleting area codes	Related translation patterns are un-deployed from CUCM, based on the country dial plan schema associated with the site.
When modifying area codes	Related translation patterns are un-deployed from CUCM, and new translation patterns are deployed, based on the updated area codes.

For the Cisco Type 1-4 dial plan schema groups, area code changes generate LBO IOS area code events. If you change the area code for a site associated with one or more Local SIP Gateways, area code IOS commands are generated:

When adding an area code	The area code add IOS command is generated.
When deleting an area code	The area code delete IOS command is generated if no other sites associated with the same SIP Local Gateway are using the deleted area code. If another site still references the same gateway's area code, the delete area code IOS command is not generated. This prevents invalidating the other site's local dialing behavior.
When updating an area code	The area code delete and add IOS commands are generated as necessary, based on the added and deleted logic.

Published number changes in Cisco HCS site dial plans

When changing an existing published number in a Cisco HCS site dial plan:

- The following site defaults are updated, if they were using the published number you changed:
  - Default CUCM Phone Line E164 Mask
  - Default CUCM Device Profile Line E164 Mask
  - Line E164 Mask
- Updates any phone line masks, device profiles, and remote destination profiles that were using the published number you changed.
- Automatically regenerates previously generated E164 IOS commands for a SIP Local Gateway associated with the site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Emergency call back number changes in Cisco HCS site dial plans

When updating a Cisco HCS site dial plan and you have a Type 1 - 4 dial plan configured, two calling party transformations are created automatically with the Emergency Call Back Number.

Changing the Emergency Call Back Number updates the calling party mask in these calling party transformation patterns if it used the previous Emergency Call Back Number:

- "*{{ macro.HcsDpSiteId}}*!"
- "*{{ macro.HcsDpSiteId}}*\+!"

If the calling party mask has been manually changed, the fields are untouched.

These calling party transformation patterns insert the Emergency Call Back Number as the caller ID for any emergency calls placed from phones within the site.

Next Steps

Apply any generated or regenerated IOS commands to your IOS gateway.

Associate custom dial plan schema group

Tip: *Use the Action search to navigate Automate*

This procedure bundles a set of schemas together to form a Type 1 to Type 4 dial plan that can be applied to a customer.

Note: You can use the default Type 1 to Type 4 schemas that are predefined and specify the Core Schemas, Feature Schemas, and Country Schemas for a customer.

1. Log in to Automate as Provider or Reseller admin.
2. Go to **Associate Custom Dial Plan Schema Group**.
3. From the list of default Type 1 to Type 4 dial plan schemas, choose the one to be customized for a customer, by clicking on its box in the leftmost column.
4. From the **General** tab, enter a new unique name for the dial plan schema group in the Dial Plan Schema Group Name field.
5. If desired, add a description of the new dial plan schema group in the Description field.
6. Modify or add site defaults, core schemas, feature schemas, country schemas or custom workflows for the customer as desired by clicking on the appropriate tab as follows:
   a. From the **Site Defaults** tab, modify site defaults as required. For more information on site defaults, refer to *Modify Site Defaults*.
   b. From the **Core Schemas** tab, modify the fields as required. For desired core schemas, select a trigger event from the **Dial Plan Schema Usage** drop-down menu, then select the hierarchical level for the core schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.

Copyright © 2025 VisionOSS Limited. All rights reserved.

c. From the **Feature Schemas** tab, modify the fields as required. For desired feature schemas, select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the hierarchical level for the feature schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the feature schema that will be triggered by the event. This drop-down list includes all default and created feature schema from the Create Schemas procedure.

d. From the **Country Schemas** tab, modify the fields as required. For desired country schemas, select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the country dial plan from the Country Name drop-down menu. Select the hierarchical level for the country schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the country-specific schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.

e. From the **Custom Workflows** tab, modify any other schema you need that are not included in any of the previous schema group tabs. From the Dial Plan Event drop-down menu, select an event trigger for your custom schema. Contact Advanced Services if you require an event trigger that is not in the list. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Workflow drop-down menu, select the custom workflow to execute when the dial plan event is triggered.

7. Click **Save**.

   The new dial plan schema group is saved. The new dial plan schema group appears in the list of groups.

Short codes

Tip: *Use the Action search to navigate Automate*

Overview

Short codes are used for abbreviated dialing to other extensions and services.

Configure short codes

This procedure configures short codes.

Prerequisites:

- The site dial plan must be added. See *Site dial plans*

Perform these steps:

1. Log in as provider, reseller, customer, or site administrator.

   Warning: When adding a short code, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. Adding a short code at any other node in the hierarchy triggers a system error indicating that you must be at a site.

2. Go to the **Short Code** page, then click the Plus icon (+) to add a short code.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Enter a short code in the **Short Code** field, using up to 16 characters with the following format:
   - The first character may be 0-9, or *
   - The last character may be 0-9, #, or the wildcard character X.
   - All other characters may be 0-9, . (period), or the wildcard character X. Only one . (period) is allowed.

   Example:

   *2.XXX
4. From the **Short Code Type** drop-down, choose one of:

Option	Description
Called Mask	The called mask maps to the Short Code. Valid entries include the digits 0 through 9; the international escape character + and the wildcard character X. For example, a called mask of 567XXX using Short Code *2.123 converts to 567123.
Directory Number	The directory number maps to the Short Code. Valid entries are digits 0 through 9.
Pre-dot with Called Prefix	The called prefix maps to the Short Code.

5. Enter the value for the Short Code Type in the **Value** field.
6. Select the **Use Originator's Calling Search Space** check box to indicate that the Short Code will use the originator's calling search space for routing a call rather than an explicit customer CSS.

   If the originating device is a phone, the originator's calling search space is a combination of the device calling search space configured on their phone and line calling search space configured on the originating line.
7. Click **Save** to add the Short Code that you defined. The new Short Code appears in the table of Short Codes and it can be edited or deleted as required.

Site short codes

Site short codes work the same for deployments that use shared lines across sites as they do for "real site" deployments. That is, short codes can be added to a site to allow shorter, convenient numbers to be dialed that are transformed into longer directory numbers. Normally, short codes are added to real sites that contain devices in order to allow users of those devices to dial shorter numbers to reach exiting directory numbers.

Because the inventory site doesn't contain devices, but only line inventory, site codes don't need to be added to the inventory site. Short code translation patterns are created on a site's Allow Internal (AInt) route partition.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Emergency and CLI settings

Tip: *Use the Action search to navigate Automate*

Overview

Emergency and CLI settings provides a facility for mapping a site-specific CLI (Calling Line Identity) for emergency and non-emergency calls. This allows users to roam using extension mobility and still provide a site-specific emergency number appropriate to the site they have visited.

Note: To access this feature, go to **Emergency and CLI Settings**.

When deploying a Cisco HCS site dialplan, a site-specific emergency number is configured as a default emergency number for all devices at that site. This feature allows users making an emergency call from within their own site to present a CLI of their own individual DDI (Direct Dial In) instead of the site wide emergency CLI.

A CLI mapping and secondary CLI mapping can also be created using this feature. The behavior is controlled through settings that can exist at any hierarchy.

This feature allows a Provider administrator (or higher) to add up to three (3) new calling party transformation patterns to provide specific translation to a DDI for those DNs having a DDI mapping. The transformations are created and deleted when either '1 to 1' or '1 to N' number associations are created and deleted. See *Add E164 association (N to 1 DN)* and *Add an E164 association (N to N DN)*

Using the HCS dialplan schema, site wide mapping is provided using a wildcard match to a site specific prefix used only for emergency calls. An example is '***156*!**'. This feature may be used to add more specific patterns such as '***156*81214000**' in order that transformations to the E164 can take place. DNs that do not have a mode specific match fall back to the wildcard match as previously set, and therefore use the site wide emergency CLI.

Note: There is no requirement to use any schema. This feature can be used wherever transformations are required as part of DN association.

The supported transformation patterns are:

- **Emergency CLI** transformation
- **CLI** transformation
- **Secondary CLI** transformation

A data model contains settings for this feature. A default set of settings is created at the `sys.hcs` hierarchy, which disables all 3 patterns. These settings must be cloned and used at a lower hierarchy to provide the settings required for each hierarchy, that is clone them to the provider level for platform wide settings, or customer level for customer specific settings.

Each of the 3 patterns can be enabled or disabled independently. The following additional controls are available:

- Macro for defining the partition
- Macro for defining the E164 number format

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Macro for defining the DN (pattern) format

The following macros can be used as part of these settings:

- EmergencyAndCLITransformations_SiteCountryCode - returns the country code, e.g. 44
- EmergencyAndCLITransformations_SiteCountryCodeWithPlus - returns the country code with a plus, e.g. +44
- EmergencyAndCLITransformations_NationalTrunkPrefix - returns the trunk prefix, e.g. 0

Each of these macros is country aware and returns the settings appropriate to the site where the DN association is performed.

In addition to these macros, there is a set of pwf context variables that can be used in the settings macros:

- pwf.e164_number - the E164 number from the mapping transaction
- pwf.dn_number - the directory number from the transaction
- pwf.sitePrefix - the site prefix number as used for HCS emergency calling

Note: Only site level associations are supported, no support is provided for linked sites.

Emergency handling

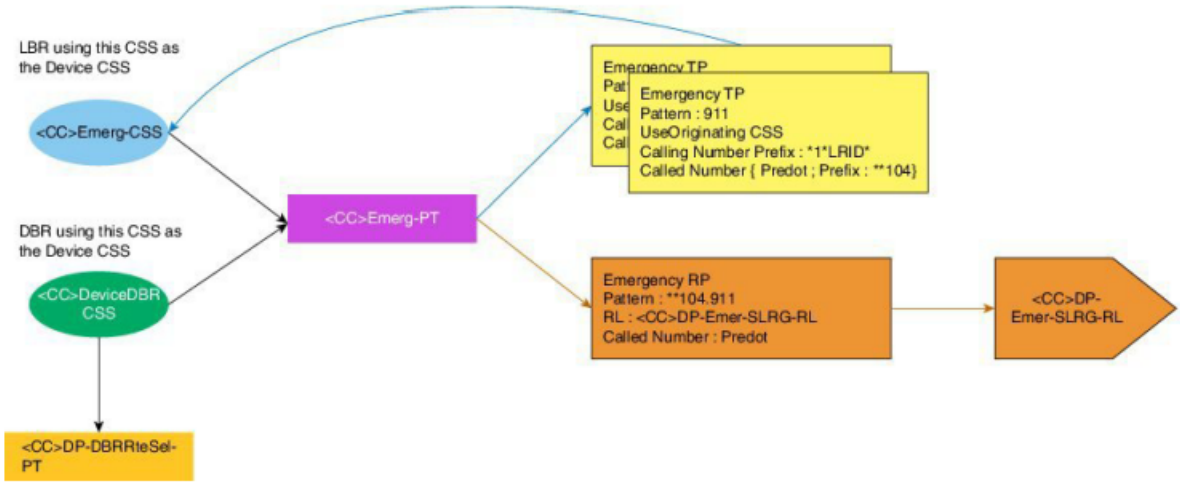
Emergency handling is device-based. It uses the device pool local route group to handle call routing. When a phone has no Direct Inward Dial (DDI) or the phone has DDI but it is in a remote location, emergency handling uses the site's emergency number.

The implementation is as follows:

- An Emergency partition is created for each site.
- For Device-Based Routing (DBR), a DeviceDBR CSS is created and for Line Based Routing (LBR) an EmerCSS is created. Both CSSs are country and site specific and they contains the Emergency partition.
- Emergency Number translation patterns are added to the emergency partition when a site dial plan is added. This translation pattern leverages the UseOriginatingCSS, prefixes the called number with **104 and the calling number is prefixed with *1*LRID* to uniquely identify the calling site.
- An Emergency route pattern matching **104 is added to the emergency partition with the route list set to use the Device Pool Emergency Local Route Group.

The image illustrates Emergency Calling.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Provisioning emergency calls

Additional provisioning is not required for emergency calls since Automate provisions 911 as part of the United States country scheme, and 999/112 is provisioned as part of the United Kingdom country scheme. For more information, see “Emergency Handling”.

1. When creating a site dial plan, enter the emergency number in the **Emergency Number** field.

   This is the Site Emergency Published Number; it is sent if the line that makes the emergency call does not have DDI. Then, if there is a callback, the Site Emergency Published Number is dialed.

2. Ensure that a Local Route group is set up with SLRG-Emer set to the Route group. Refer to “Associate Local Route Groups to a Device Pool”.

Directory number routing

Tip: *Use the Action search to navigate Automate*

Overview

Directory number routing is a translation pattern that is put into the PreISR and ISR partitions to route intrasite and intersite calls to extensions (directory numbers). This is similar to the way site location codes (SLCs) are used as short codes for Type 1, 2, and 3 customer dial plans.

Typically, directory number routing is used for Type 4 (flat dial plans) so that from a customer and site perspective, you can see which patterns are directory numbers because there are no SLCs available.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a directory number routing

This procedure adds a directory number routing.

1. Log in as provider, reseller, customer, or site administrator.

   Warning: When adding directory number routing, you must select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. Adding a directory number routing at any other node in the hierarchy triggers a system error indicating that you must be at a site.

2. Go to the **Directory Number Routing** page, then click the Plus icon (+).
3. In the **Directory Number Routing Prefix**, enter a prefix, using up to 30 characters (for example, *234*)
4. In the **Directory Number Mask Length** field, enter a DN mask length. For example, if you enter *4*, the Directory Number Routing would be 234XXXX, where XXXX is the mask.
5. Click **Save**. The Directory Number Routing is added.

   The new Directory Number Routing appears in the table and it can be edited or deleted as required.

Customer HCS Dial Plan

provider

Cisco

Tip: *Use the Action search to navigate Automate*

Overview

For Cisco HCS dial plans, you must create a customer dial plan before you create the site dial plan.

Cisco HCS dial plan schemas are configured such that the customer-level dial plan elements are not pushed to UCM until the first site for the customer is deployed. Therefore, you won't see any dial plan elements provisioned on the UCM until at least one site is deployed for the customer.

Once you add a customer dial plan, the only change allowed is to enable CSS filtering.

Related topics

- *Site dial plans*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Cisco HCS customer dial plan

This procedure adds a new Cisco HCS dial plan for a customer.

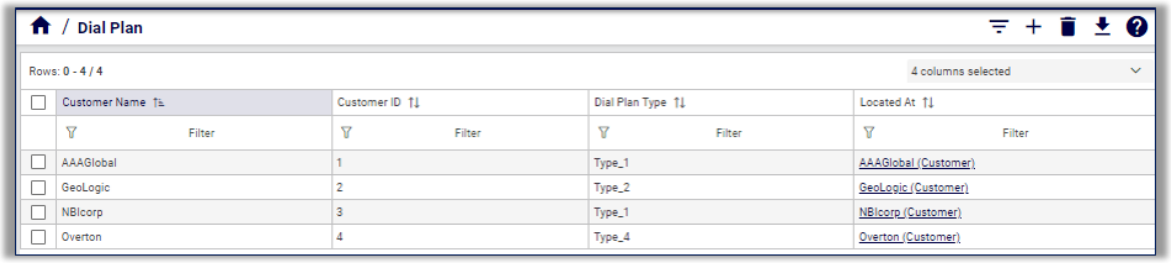
Note:

- You can only add one dial plan per customer.
- The options you choose define the type of Cisco HCS dial plan schema to be used (Type 1 to 4).

1. Log in to the Admin portal as Provider or Customer admin.

   Note: For details around tasks that can be performed for each admin level, see *Dial plan roles and privileges*.

2. Go to **Dialplan Tools** > **Customer HCS Dial Plan**.



3. Click the Plus icon (+) to add a new customer dial plan.
4. Select the customer to open the **Customer HCS Dial Plan > New Record** page.

   Note: **Customer ID** is a read-only, unique, auto-generated number allocated to the customer. Customer ID is particularly useful in shared deployments (where a cluster may be shared across multiple customers) to correlate specific elements to a customer. Customer ID displays in Cisco UCM as a prefix to elements (for example Cu2Si7 identifies Customer 2, Site 7).

5. Optionally, at **Default External Breakout Number** add a PSTN Access prefix, if required.
6. **Is a site-location (SLC) required**?
   - **No**. Leave **Site-Location Code (SLC) based dial plan** clear (unchecked). Go to Step 7.
   - **Yes**. Select **Site-Location Code (SLC) based dial plan**. Select options for the following additional fields that display. When you're done, go to Step 7:
     - Optionally, select **Use extension prefix**, and fill out an extension prefix, if required.
     - Optionally, select **Inter-Site Prefix required for inter-site dialing**, and fill out the inter-site prefix (ISP), if required. The ISP can be just one digit.
     - If you're applying an inter-site prefix (ISP), define whether the ISP is included in the directory number.
     - If the ISP is to be included in the directory number, define whether the ISP is included in the Voice Mail ID.
7. Define whether to **Enable CSS filtering**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- When enabled, CSS filtering filters the Calling Search Spaces (CSSs) when configuring a user, phone, or line, to Site level Class of Service (CoS) CSSs.
- When disabled (default), all available Cisco UCM CSSs are available when configuring a user, phone, or line.

8. Save the form to add the new customer dial plan.

   For add, update, or delete, you can view transaction progress and details in the Transaction Logs.

Note: When adding lines (DNs) at the site level, you must define your DNs appropriately (that is, you are responsible for using ISP+SLC+EXT if you deploy a Type 2 dial plan). Otherwise your inter/intra site calls won't route. For details around defining directory numbers, see *Number range management*.

Related topics

- Transaction logging and audit in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

7. Number Management

7.1. Introduction to number management in Automate

7.1.1. Overview

Automate provides support for consolidating and managing your full number inventory. The system also supports various dial plan designs, whether E164 dial plans or traditional internal numbers mapped to external numbers.

The table summarizes Automate's main inventory capabilities:

Inventory capability	Description
Number Inventory	Automate's main inventory, also known as the *internal number inventory* (INI), contains all numbers that are assigned to devices, users, and services. While this is called an *internal* inventory, it can also include extensions (in traditional dial plans or for internal-only services), or full E164 numbers (if those are assigned directly to users, devices, and services).
E164 Inventory and Associations	An inventory that provides E164 numbers to map to the number inventory entries if they are *internal only* numbers, as required for traditional internal or external dial plans. In this inventory, internal numbers are assigned to devices and are then mapped to external numbers for external access. To use this inventory you'll need to load appropriate transformations and other dial plan elements. The association workflow when mapping E164 numbers to number inventory instances work with dial plan schemas or your own dial plan (dial plan tools). If E164 numbers are assigned directly to users, devices, and services, then those numbers are added directly in the number inventory and this E164 inventory and associations functionality is not required (and is then typically not visible in the system menus).

Once numbers are loaded into Automate, inventory details are shared and incorporated into other parts of the system, allowing users to choose numbers and to automatically track their status.

Automate provides the ability to reconcile (audit) the inventory against currently configured services in the event that changes are made outside the system, thus ensuring that the inventory stays up to date and

accurate to reduce errors when selecting numbers or when manually reconciling.

Many of the inventory capabilities in the system focus around the internal number inventory as these are the numbers assigned to users, devices, and services directly.

Related topics

- *Number cooling*
- *Number reservation*
- Prevent duplicate numbers in the Core Feature Guide

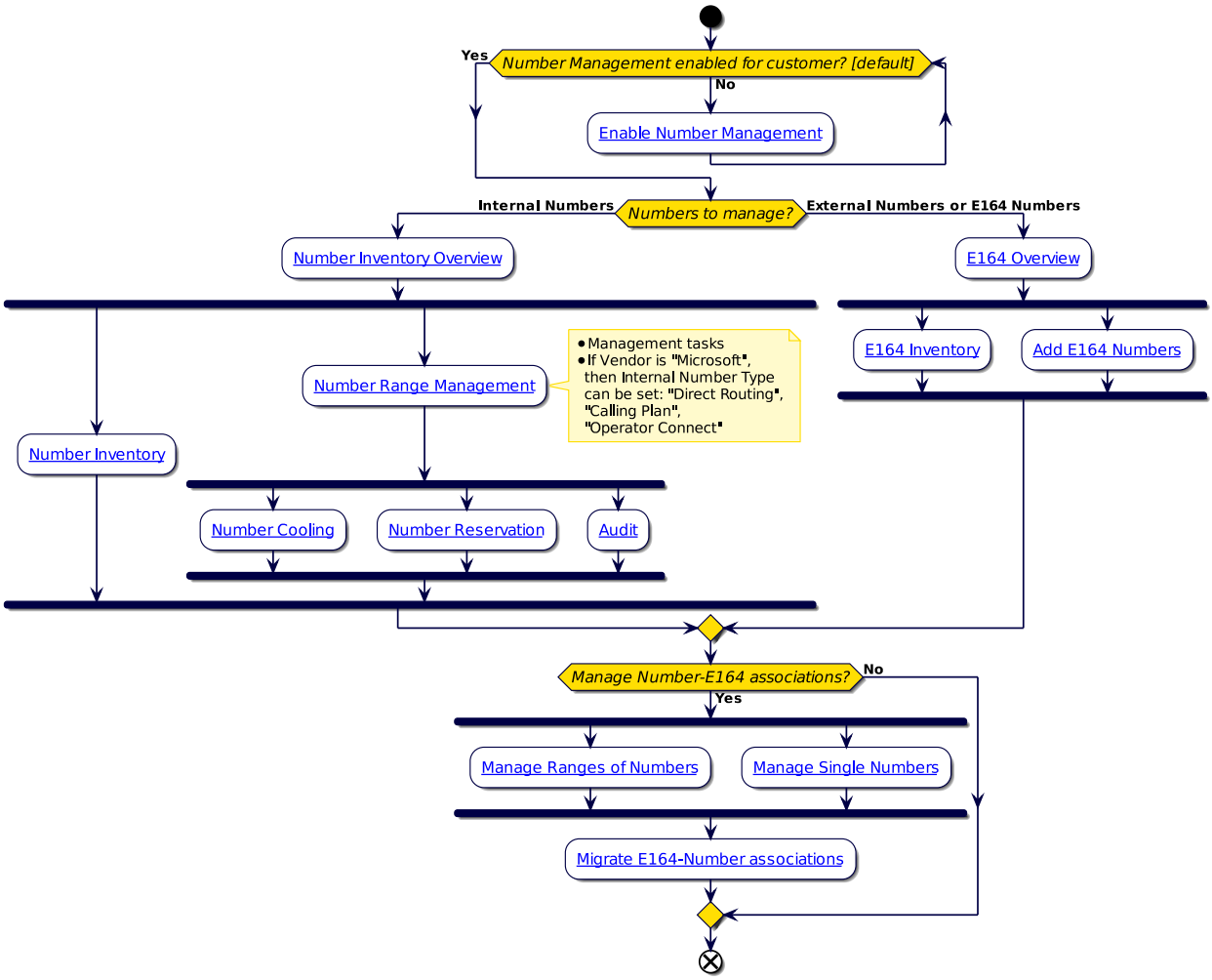
7.1.2. Number management workflow in Automate

The flowchart in this section provides an overview of Automate's number management feature, highlighting internal number and external E164 number management and association.

Note:

- Number management functionality in Automate can be disabled for a customer if it's not required. To disable this feature, select the **Disable Number Management** setting. See: *Customers*.
- E164 number management is used only in a Cisco UCM environment, which has the concept of internal numbers and associated E164 numbers. It is valid in Microsoft and in some Cisco deployments to add E164 numbers directly to the number inventory (and to completely ignore E164 number management).

Copyright © 2025 VisionOSS Limited. All rights reserved.



7.2. AudioCodes device number integration

7.2.1. Overview

Automate supports the integration of numbers used by AudioCodes devices into the number inventory. Once such devices are configured in Automate and data is synced, the number inventory displays these numbers with their status set to `Used`, and the **Vendor** field set to *AudioCodes*. These numbers won't be available to assign to subscribers during number management.

Workflows and data syncs are in place to ensure these numbers in the number inventory remain aligned with any changes in these devices.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *AudioCodes device number integration* in the Core Feature Guide

7.2.2. AudioCodes and number cooling

In the case of the removal (or delete) of a AudioCodes **RegisteredUsers** instance, the internal number is placed into a configurable cooling period, with their status set to `Cooling`.

Important: For AudioCodes internal numbers, the cooling period (days) is configured by means of a named macro called: `audiocodes_cooling_duration` (default setting is 2 days) and *not* by the **Number Inventory Cooling Duration (Days)** value in Global Settings (*Global settings*).

A high level administrator with access to the named macro instances can carry out this configuration if needed.

The reason for the alternative cooling setting is that AudioCodes devices can become offline but aren't deleted. The default maximum offline duration is here set to 2 days.

In addition, if the device does then come back online within the days set in the macro, the internal number will be set back to:

- Status: `Used`
- Usage: `Device`
- Vendor: `AudioCodes`

When the line is in cooling, the following internal number inventory fields are set:

- **Tag**: an information message of the number of days when the INI will reach the release date.
- **Release Date**

When the **Release Date** is reached, the INI is put back into the **Available** pool of INI's, as with standard cooling - see: *Number cooling*.

Related topics

- *View number details and usage*
- *Number cooling*

7.2.3. AudioCodes and audit number inventory

When the **Audit Number Inventory** is run, the **Status** and **Usage** of internal number inventory items that have the **Vendor** field set as *AudioCodes* are checked and verified to be:

- **Status**: `Used`
- **Usage**: `Device`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Microsoft Teams deployments*
- *Number inventory audit*

7.3. Move number inventory instances

Tip: *Use the Action search to navigate Automate*

7.3.1. Overview

Automate allows you to move number inventory instances to a selected hierarchy. It is particularly useful to *bulk load* number inventory instances that need to be moved.

The feature is available as a view, `view/move_data_ini`, which can be added manually as a menu item on an administrator menu layout if needed.

Note: Access profile permissions have already been added for all administrator levels to create, read, and export a bulk load template of this view.

7.3.2. Move a number on the view

To use move a number on the view:

1. Select the **Internal Number**.
2. Select the **Move To Hierarchy** to move the number to.
3. Click **Save** to carry out the move operation.

7.3.3. Bulk load

More typically, the view can be used in a bulk load sheet. After exporting the view as a bulk load sheet, the exported sheet header row will be similar to the following:

```
entity: view/move_data_ini;
hierarchy: sys;
parallel: False;
parallel_transaction_limit: ;
template: ;
meta_prefix: $;
evaluate_macros: False
```

Columns are then available for:

- **Comment**: to comment an entry if needed

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Hierarchy Node** (`$hierarchy`): for the source hierarchy
- **Action** (`$action`): value is always `add`
- **Internal Number** (`$internal_number`): for the number to move
- **Move To Hierarchy** (`move_to_hn`): for the target hierarchy

The image shows an example bulk load sheet:

entity: view/move_data_ini; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template: ; meta_prefix: $; evaluate_macros: False

	$hierarchy	$action	internal_number	move_to_hn
	# Base		# move_data_ini	
# Comment	# Hierarchy Node	# Action	# Internal Number	# Move To Hierarchy
#	sys.hcs.CS-P.WebexTestUCMcallingAutomation	add	1000	sys.hcs.CS-P.WebexTestUCMcallingAutomation
#	sys.hcs.CS-P.WebexTestUCMcallingAutomation	add	1001	sys.hcs.CS-P.WebexTestUCMcallingAutomation
	sys.hcs.CS-P	add	\+13468760628	sys.hcs.CS-P.WebexTestAutomation.Site2

7.4. Number Inventory Management

7.4.1. Number status and usage

Overview

Values in the **Status** and **Usage** columns in the number inventory allow administrators to understand how numbers are used at a specific hierarchy level.

Tip: *Use the Action search to navigate Automate*

The table describes values in the **Status** and **Usage** columns in the Number Inventory:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Number Use	Device	Status	Usage	Vendor[Page 1029, 1]
Not used by anything	-	Available	blank	blank
Phone Line[2]	device/cucm/Phone (line instance)	Used	Device	blank
Device Profile Line	device/cucm/DeviceProfile (line instance)	Used	Device	blank
Remote Destination Profile Line	device/cucm/RemoteDestinationProfi (line instance)	Used	Device	blank
Hunt Pilot[2]	device/cucm/HuntPilot	Used-Utility	Hunt_Pilot	blank
Pickup Group Pilot	device/cucm/CallPickupGroup	Used-Utility	Pickup_Group_Pilot	blank
System Call Handler	device/cuc/Callhandler (System only)	Used-Utility	Call_Handler_Pilot	blank
Voicemail Pilot	device/cucm/VoicemailPilot	Used-Utility	Voicemail_Pilot	blank
Meet Me	device/cucm/MeetMe	Used-Utility	Meet_Me	blank
CTI Route Point	device/cucm/CtiRoutePoint	Used-Utility	CTI_RoutePoint	blank
Call Park	device/cucm/CallPark	Used-Utility	Call_Park	blank
Directed Call Park	device/cucm/DirectedCallPark	Used-Utility	Directed_Call_Park	blank
VOSS Phone	data/PRS_MultiVendorPhone_DAT	Used-Utility	VOSS_Phone	phoneVendor
MS Teams Line URI	device/msteamsonline/CsOnlineUser (LineURI)	Used	User	Microsoft
Webex User	device/spark/Number	Used	User	Webex Calling
Number inactive		Inactive[3]	blank	Webex Calling
AudioCodes devices	device/audiocodes	Used	Device	AudioCodes[4]
Not used by anything		Available	blank	blank, Microsoft, Webex Calling

[1] Default vendor value is blank (for Cisco).

[2] If a number is used by both a Phone and Hunt Pilot then the **Usage** column will display both usage values, i.e. `Device,Hunt_Pilot`. This could be the case if you change the Partition and enter the DN manually so that they share the same DN.

However, the **Status** column will display only *one* status: the status triggered by the most recent transaction. The Status would change from Used to Used-Utility if you added the Hunt Pilot last. If it was already a Hunt Pilot and then you added it to a Phone, then Status would change from Used-Utility to Used.

Numbers can also be shared between Call Handlers and one or more device types. Status depends on whether Call Handler or devices were added first to the number. Usage will typically be `Call_Handler_Pilot,Device`.

[3] Status is Inactive by adding a number in Number Range Management, where **Vendor** is Webex Calling and **Push as Active** is *unchecked* on the **Webex Control Hub** frame on the input form.

Modifying the number in a range by setting the status as Available will activate it in the Webex Control Hub and update its status.

[4] For AudioCodes, see the AudioCodes topic in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Number Use	Device	Status	Usage	Vendor[1]
Number in cooling[5]		Cooling	-	blank, Microsoft, Webex Calling
Number reserved[6]		Reserved	-	blank, Microsoft, Webex Calling
Webex Calling ownerType is unset	device/spark/Number	Available	-	Webex Calling
Webex Calling ownerType is PEOPLE	device/spark/Number	Used	User	Webex Calling
Webex Calling ownerType is *not* unset or PEOPLE	device/spark/Number	Used-Utility	Matches the ownerType: Device (for PLACE), Auto_Attendant, Call_Queue, Group_Paging, Hunt_Pilot, Voicemail_Pilot, Broadworks_Anywhere, Contact_Center_Link, Route_List, Voicemail_Group	Webex Calling

For further details on Vendor and Internal Number Type fields – see *UC vendor guidelines for numbers*.

Related Topics

For details on call handlers and shared numbers, see Auto-Attendant Call Handler in the Core Feature Guide.

7.4.2. Number range management

Tip: *Use the Action search to navigate Automate*

[5] If a number is currently in **Cooling**, the release date indicates when the number will come out of cooling.
[6] If a number is currently **Reserved**, you can enter an optional **Tag** to identify the user for which the number is reserved. An optional **Reservation notes** field is also available to allow you to enter additional information regarding the reserved number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

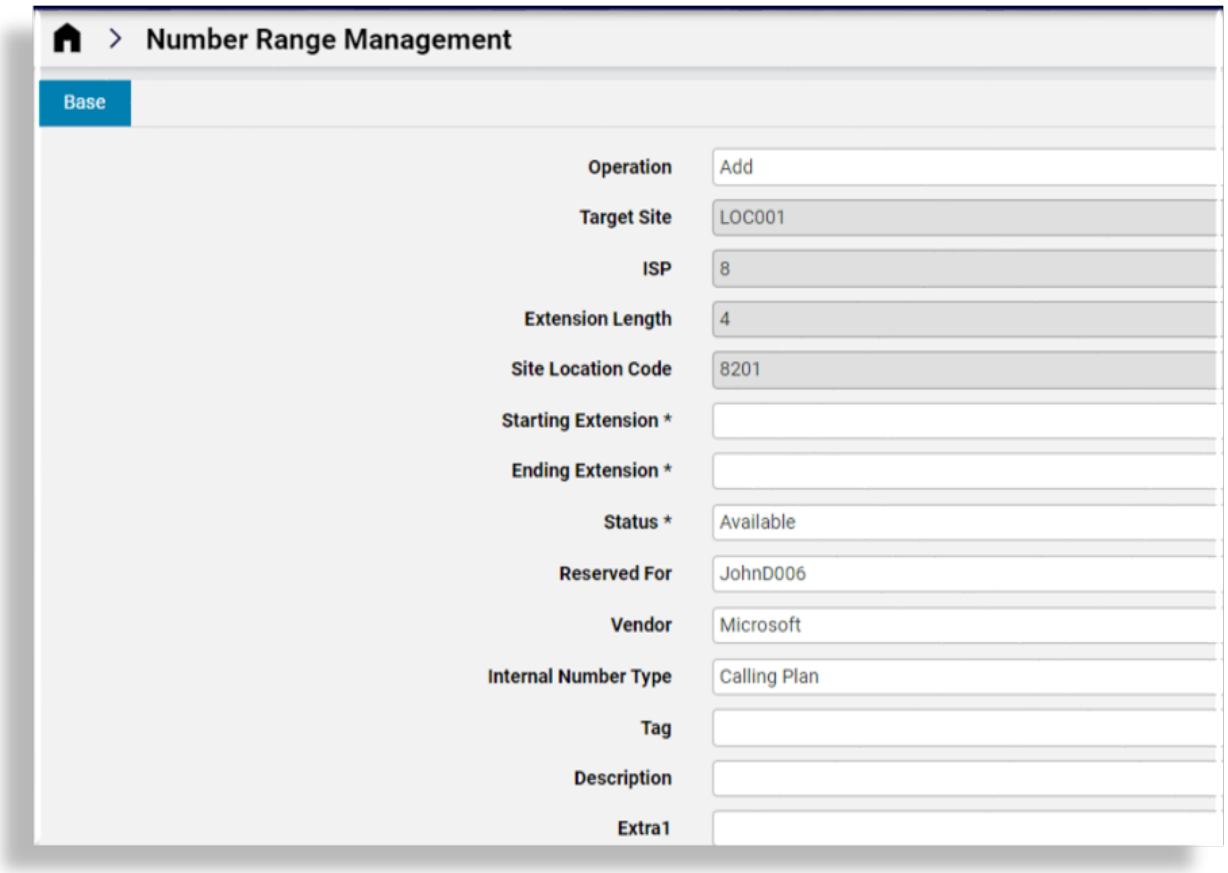
Automate's number range management feature allows you to add and manage a range of internal numbers, at a customer, at a site, or at an intermediate node.

Note: An internal number range created at an intermediate node is also available at the sites below this intermediate node.

You can add an internal number range that includes existing numbers, but in this case, it is not possible to modify the existing numbers. New, unused numbers are added only to complete the range. This means that the number range will display as complete, with unused numbers displaying along with numbers imported from Cisco UCM.

For Microsoft deployments, if you wish to prevent the creation of duplicate numbers when creating a number range, enable (set to *Yes*) the *Prevent Duplicate Numbers* global setting. See:

- Prevent duplicate numbers in the Core Feature Guide



Note: Using a bulk loader sheet or the API, you can create the number inventory at the customer hierarchy only. The **Details** column of sub-transactions shows whether the number already exists or if it is creating a new number. If any numbers exist in the range, the sub-transaction fails and the parent transaction shows the status *Success with Async Failures*.

While you can delete a number range, only numbers in this range with a status of *Available* can be deleted.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Numbers in the range with the following statuses are ignored and can't be deleted unless their status changes to *Available*:

- Used
- Used-Utility
- Reserved
- Cooling

Numbers with status *Available* and *Reserved* can be modified manually once they're added.

Numbers can be added, edited, or deleted. When modifying a number, you can only edit the free text fields. The usage and availability property for each number is associated with a line or taken into use by a service.

The number inventory isn't partition-aware so if the same directory number is used on a cluster but in different partitions, Automate updates the inventory when any of these instances are changed. For example, if there's a number, *1111*, in the *Cluster X* partition, and a number, *1111*, in the *Cluster Y* partition, this number is marked as *Used*. If either of these instances are deleted, Automate checks whether other instances of this line exists (based on the number only, not partition) before it clears the *Used* flag. If other instances exist, the number status remains as *Used*.

Tip: *Use the Action search to navigate Automate*

Related topics

- For details around managing number ranges specific to the UC vendors you're using, see *UC vendor guidelines for numbers*
- Reserve a Number for a User in the Core Feature Guide
- Prevent duplicate numbers in the Core Feature Guide

Manage numbers and number ranges

Tip: *Use the Action search to navigate Automate*

This procedure adds, updates, and deletes numbers and number ranges.

Note: If you don't want the system to create duplicate numbers when creating a number range (duplicates of numbers in the range already exist), enable (set to *Yes*) the *Prevent Duplicate Number* global settings.

1. In the Admin Portal, go to **Add Internal Number Inventory**.
2. Select the relevant hierarchy, customer or site.
3. Optionally, choose a target site.

   Note: Target site may be auto-populated as a read-only field if you've chosen to open this page from the site hierarchy. If you've opened this page from the customer hierarchy, you may need to select a target site (mandatory in some dial plans, such as site code based dial plan).

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. At **Operation**, choose an option:
   - **Add or Modify**?
     - By default, **Status** is set to *Available*.
     - When changing status to *Reserved*, optionally, fill out a value for **Reservation duration (days)**, for example, *30*. At the end of this period, status returns to *Available*. If no value is specified the numbers are reserved indefinitely.
     - If you choose **Modify** and wish to modify the range free text fields (see below for details), then manually set the **Status** drop-down to *Unchanged*. This allows for the modification of the fields of numbers in the range - regardless of current number status - without modifying the original number **Status**.
   - **Delete**?
     - Only the following fields are now available: Target Site, Starting Extension, Ending Extension
     - When deleting a number range, you won't be able to mark lines as either **Available** or **Reserved** (these options won't display on the form).
     - If a number in a deleted number range was set at *Used*, it won't be deleted.
5. Fill out a starting and ending extension.

   Note: The maximum allowed range is 1000 for a single action. The starting extension should always be smaller than the ending extension.

   If you're adding or deleting a single number, the starting and ending extension number will be the same. If numbers in the range already exist, they won't be affected - only non-existing numbers will be added.

6. If required, at **Reserved For**, you can reserve a number for a specific user. Choose an existing username, or fill out a custom value. Here you can also remove the *Reserved For* flag (clear the field) to allow the number to be assigned to other users.
7. At **Vendor**, select the relevant vendor for the number range (Cisco, Microsoft, Cisco/Microsoft, or Webex Calling).
8. Based on the vendor you chose, select an appropriate option at **Internal Number Type** (direct routing, calling plan, or operator connect).

   Note: For more information for your use case, see *UC vendor guidelines for numbers*

9. Optionally, fill out values for the additional free text fields, for example **Tag**, **Description**, **Reservation notes**, **E164Number** (if applicable), and **Extra1** to **Extra9**.

   These values can be updated for a range of numbers - regardless of the number **Status** in the range - by setting the **Status** drop-down to *Unchanged* during the update process. The original number **Status** in the range will remain unchanged.

10. Save your changes.

    Note: Numbers at a specific hierarchy can be viewed on the **Number Inventory** list view. See *View number details and usage*.

    When a line is added and selected from the drop-down list of available numbers, it has a status of **Used**. If the line is used by a device or service that does not allow a shared line (for example, a Hunt Pilot), it has a status of **Used-Utility**. See *Number status and usage*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Internal numbers are available when adding users.

Related topics

- *UC vendor guidelines for numbers*
- *Number status and usage*
- *View number details and usage*
- Reserve a Number for a User in the Core Feature Guide
- Number Reservation
- Prevent duplicate numbers in the Core Feature Guide

Modify a number in the number inventory

This procedure modifies an individual number via the number inventory list view.

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, go to **View Internal Inventory**.
2. Click on the relevant number in the list to view its detailed management page.
3. Choose an available edit option:
   - To reserve the number, click the vertical ellipsis toolbar button to display the overflow menu, then select **Reserve Number**. Transaction is scheduled for processing. When done, the status of the number changes to *Reserved*.
   - To select the internal number type, select an option at **Internal Number Type**, either Direct Routing, Calling Plan, or Operator Connect.
   - Edit free text fields, such as Tag, Description, Reservation notes, E164Number (if applicable), and Extra1 to Extra9.
   - To reserve a number for a specified user, at **Reserved For**, choose an existing username or fill out a username for a new user. This number won't be available for allocation to any other user until you remove this *reserved for* flag.
4. Save your changes.

Related topics

- *View number details and usage*
- Reserve a number for a user in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Number range management Extra1 to Extra9 fields

When editing numbers in the Number Inventory or when adding or updating number ranges, you can modify values in additional fields called **Extra1** to **Extra9**.

- When the status of a number changes, for example, from *Used* to *Available* - this may occur when an associated device is unassociated with the line - then any values originally in any of the **Extra1** to **Extra9** fields, remain unchanged by default.
- A default custom Configuration Template (CFT), `IniUpdateCustomCFT`, which applies to `data/InternalNumberInventory`, can be cloned to the user hierarchy and then to modify the custom persistence of extra field values.

  For more information around CFT cloning and custom configuration, see the Advanced Configuration Guide.

  Important: Any changes to this custom CFT *only* apply to updates in workflows resulting in number status changes - manual updates are *not* affected.

  The following default values in this CFT can be modified according to your needs:

```
"description": "{{ pwf.ini_dat_before.description }}",

"extra1": "{{ pwf.ini_dat_before.extra1 }}",
"extra2": "{{ pwf.ini_dat_before.extra2 }}",
"extra3": "{{ pwf.ini_dat_before.extra3 }}",
"extra4": "{{ pwf.ini_dat_before.extra4 }}",
"extra5": "{{ pwf.ini_dat_before.extra5 }}",
"extra6": "{{ pwf.ini_dat_before.extra6 }}",
"extra7": "{{ pwf.ini_dat_before.extra7 }}",
"extra8": "{{ pwf.ini_dat_before.extra8 }}",
"extra9": "{{ pwf.ini_dat_before.extra9 }}",
"tag": "{{ pwf.ini_dat_before.tag }}"
```

  The default macros for each extra field can thus be replaced inside the cloned CFT with custom text and macros as needed. Use the macro `{{ macro.CLEAR }}` if it is necessary to clear a field.

- The **Description** field is *always* cleared when the status of the number changes to **Available**, regardless of CFT value. For other number status changes, the CFT value will apply.

  There is full customization functionality of the **Description** field available to allow values in accordance with Automate feature usage.

  For details, see the *Number Inventory Flexibility and Description Customization* topic in the Advanced Configuration Guide.

- This CFT can't be used to modify any other VOSS managed fields in `data/InternalNumberInventory`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

7.4.3. Number cooling

Tip: *Use the Action search to navigate Automate*

Overview

Number cooling allows for the automatic aging of numbers after service delete to prevent immediate reuse of a number. For example, if a user leaves the company, the phone number that was in use can be placed into a cooling period for a pre-configured number of days to prevent a new user from receiving unwanted calls on that number. This feature can be enabled per hierarchy level.

Note: Number cooling is enabled and configured in Global Settings.

During the cooling period, the number can't be reused until either the cooling period has elapsed, or until a Provider administrator has manually removed the number from the cooling period. Once a number is removed from the cooling period, it is reintroduced into the pool of available numbers for allocation to a subscriber, phone, device, etc.

A number cooling auto expiry schedule runs daily. This schedule polls the cooling **Release Date** field on the number inventory list view to determine which numbers have completed their cooling period. These numbers are then returned to the list of available numbers at the specific hierarchy level. For more details refer to "Number Cooling Auto Expiry Schedule" in the *Advanced Feature Guide*.

The **Cooling & Reserved Number Management** form allows a Provider administrator to manually add numbers to a cooling period (which removes these numbers from the list of available numbers), or to manually remove numbers from a cooling period (which returns these numbers to the list of available numbers).

Related topics

- *Number inventory*
- *Number inventory audit*
- Number Cooling Auto Expiry Schedule in the Advanced Configuration Guide
- Global Settings in the Core Feature Guide

Apply cooling

1. Navigate to the required hierarchy level (Provider, Customer or Site) from which you want to add numbers to a cooling period.
2. Go to **Cooling & Reserved Number Management**.
3. At **Select action**, choose **Apply cooling**.
4. Optionally, fill out a cooling duration in days (max = 999) to apply to the selected numbers.

   Note: This value overrides the value set in their global settings. If this field is left blank, the cooling duration set in *Global settings* for each number will apply.

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. Configure values in **Filters** to define the numbers to include in the **Available** box in the **Select Numbers** area, these include:
   - **Include available numbers**
   - **Include cooling numbers**
   - **Contains**. Used to further refine the numbers displayed in the **Available** box.
   - **Show numbers at/below hierarchy**. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
6. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.

   Note: The **Available** field displays only unused and available numbers. Used numbers don't display.

7. Click **Save**.

   The selected number(s) are placed into a **Cooling** status, and are no longer available for use until they reach either the **Release Date** or until they are manually removed from cooling.

Remove from cooling

1. Navigate to the required hierarchy level (Provider, Customer or Site) from which you want to remove numbers from a cooling period, i.e. add them back into the list of available numbers.
2. Go to **Cooling & Reserved Number Management**.
3. From the **Select action** drop-down, choose **Remove from cooling**.
4. Configure values at **Filters** to determine which numbers will be included in the **Available** box in the **Select Numbers** area, these include:
   - **Include cooling numbers**
   - **Expires from cooling within (days)**.
   - **Contains**. Used to further refine the numbers displayed in the *Available* box.
   - **Show numbers at/below hierarchy**. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
5. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
6. Click **Save**. The selected number(s) are removed from the cooling period and are available for allocation to a subscriber or phone, etc.

7.4.4. Number reservation

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Number reservation allows numbers to be reserved for future use. Reserved numbers cannot be allocated to a device or line.

The **Cooling & Reserved Number Management** list view allows a Provider administrator to manually reserve numbers at the selected hierarchy (Provider, Customer or Site) for a specified number of days. While a number is within the **Reservation duration (days)** period, it is unavailable and cannot be used by a device or line.

If the **Reservation duration (days)** period is left blank, the numbers remain in the **Reserved** status. Currently reserved numbers can be unreserved manually, thereby *adding them back* to the list of available numbers.

Related topics

- *Number inventory*
- *Number inventory audit*
- *Number cooling*
- Reserve a Number for a User in the Core Feature Guide

Reserve numbers for future use

Note: Numbers can be reserved to make them unavailable to assign to any user until they're unreserved.

A separate feature, *Reserved for*, allows you to reserve numbers for a specific user. When used with *use next available line* during provisioning or onboarding, numbers reserved for a particular user can't be assigned to any other user. See:

Reserve a Number for a User in the Core Feature Guide

---

1. In the Admin Portal, choose the relevant hierarchy level (Provider, Customer or Site) where you want to reserve numbers.
2. Go to **Cooling & Reserved Number Management**.
3. At the **Select action** drop-down, select **Reserve**.
4. At **Reservation duration (days)**, define the number days to reserve the number/s.
5. Fill out **Reservation Notes** for the reserved numbers to describe why the numbers are being reserved. This is displayed in the **Reservation notes** field on the **Number Inventory** list.

   Note: Un-reserving the number (setting *Reserved* status to *Available*) automatically clears the **Reservation notes** field.

   ---

6. At **Filters**, define filters to determine which numbers will be included in the **Available** box in the **Select Numbers** area. Options are:
   - Include available numbers
   - Include reserved numbers
   - Contains. Filter criteria to further refine the numbers displayed in the *Available* box.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Show numbers at/below hierarchy. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.

7. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
8. Click **Save**.

   The selected number(s) are placed into a **Reserved** status, and are no longer available for allocation to a subscriber or phone, etc.

Note: Individual numbers can also be reserved directly from the **Number Inventory** list view by clicking on the required number on the list view and then selecting **Reserve Number** on the toolbar.

Related topics

- Reserve a Number for a User in the Core Feature Guide

Unreserve numbers

1. In the Admin Portal, choose the relevant hierarchy level (Provider, Customer or Site) where you want to remove numbers from reservation (unreserve) to add them back into the list of available numbers.
2. Go to **Cooling & Reserved Number Management**.
3. From the **Select action** drop-down, choose **Unreserve**.
4. Set **Filters** to determine which numbers will be included in the **Available** box in the **Select Numbers** area. Options are:
   - Include reserved numbers
   - Contains. Additional criteria to further refine the numbers displayed in the *Available* box.
   - Show numbers at/below hierarchy. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
5. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
6. Click **Save**.

   The selected number(s) are removed from the **Reserved** status, and are available for allocation to a subscriber or phone, etc.

   If reservation notes were included for a number when it was reserved, un-reserving the number automatically clears any notes in the **Reservation notes** field.

7.4.5. Reserve numbers for a user

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate allows you to reserve one or more INI numbers for a specific user. This means that you can pre-assign existing numbers (or fill out a custom value for a new number) for an existing or new user.

A number that has been *Reserved for* a user remains reserved for that particular user even if you delete that user, until you remove the *Reserved for* flag on that number.

When deleting a user that has numbers reserved for them, the status of those numbers may be *available*, but these numbers retains their association with the deleted user's username, and you won't be able to assign these numbers to another user until you clear the number as reserved for that user.

This allows you to reserve numbers for a user who may later be added back to the system. For example, you may have temporary or seasonal employees that require one or more numbers from time to time, or employees that leave temporarily on sabbatical - in this case, you can de-provision the user so that they don't have access to system services, but they'll have the same numbers when they're onboarded again in future.

Numbers that are reserved for a specified user can't be assigned to another user, either manually or via *use next available line* functionality.

Note: *Reserved for* differs from Automate's *Number Reservation* and *Number Cooling* functionality, which is associated with a number's status:

- Used
- Available
- Reserved
- Cooling

Numbers that are generally reserved for future use or in cooling can't be assigned via *use next available line* or manually because their status is something other than *Available*. However, if this number is flagged as *Reserved for* a particular user, as soon as that number's status changes to *Available* (when it's status moves out of reserved, used, or cooling), it is automatically reserved for the user it's been flagged for and can be assigned manually, or automatically when using *use next available line*.

When onboarding or provisioning a user, the system checks whether the username matches any number reserved for that user, and if found, the number is automatically assigned to this user at the site. If the username doesn't match any *reserved for* number, you can choose another available number or choose to use the next available number, which will exclude any number that is reserved for or belonging to another user.

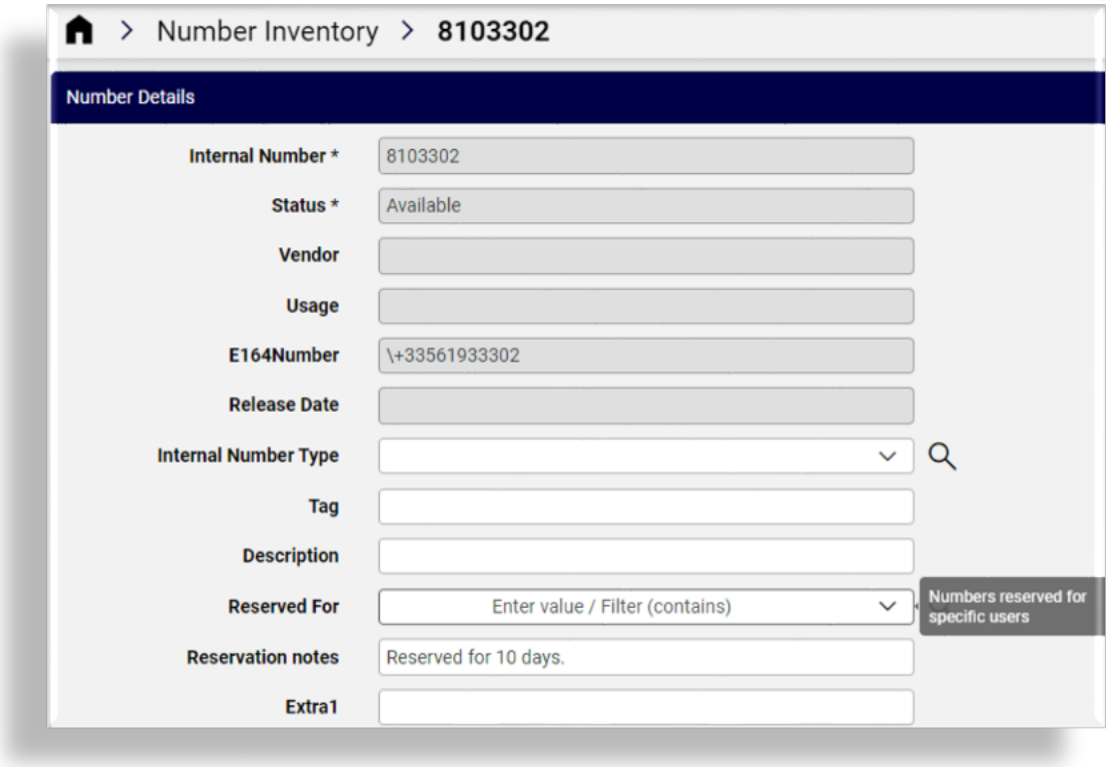
Related topics

- *Number reservation*
- *Number range management*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure *Reserved for* numbers

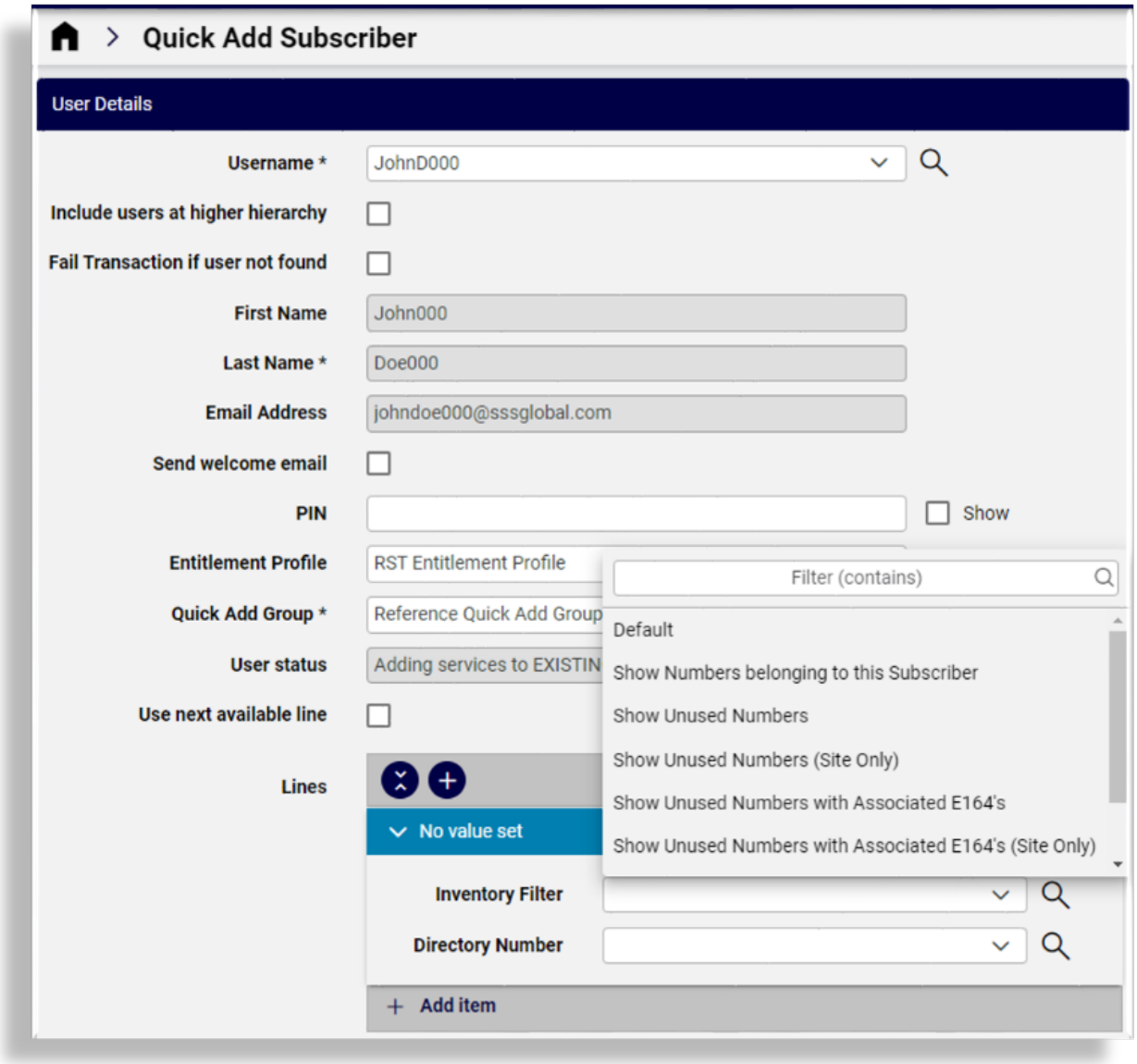
You can reserve a number for a new user (one that doesn't yet exist on the system), or for an existing user, via the *Number inventory* or *Number range management*. If the user doesn't exist, just fill out their username in the **Reserved For** field. If the user already exists, choose the user from the **Reserved For** drop-down.



Show numbers belonging to a user

When assigning lines and numbers to a user you're onboarding or provisioning, Automate provides an inventory filter called **Show Numbers belonging to this User**, which allows you to display *only* the numbers specifically reserved for a user you're working with.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- *Custom inventory filters*

Moving users with *Reserved for* numbers

Directory number lookup depends on the “move to” (destination) hierarchy. This means that if you want to see any numbers in the directory number drop-down when moving a user to another location, those numbers need to exist at the destination hierarchy.

Example: Move user and availability of numbers at destination

In this example, we have a customer, *Cust-1*. At this customer we have three sites, *Site-A*, *Site-B*, and *Site-C*:

- Create a user at *Site-A*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Reserve numbers for this user at *Site-A*, *Site-B*, and at the customer level, *Cust-1*
- Move the user from *Site-A* to *Site-B*.
  - Select inventory filter, **Show Numbers belonging to this User**
  - The system displays numbers reserved for this user at *Site-B* and at *Cust-1*
- Move the user from *Site-A* to *Site-C*:
  - Select inventory filter, **Show Numbers belonging to this User**
  - The system displays numbers reserved for this user at *Cust-1*

Note: The list of numbers available to a user to choose from never include numbers reserved for other users (*Reserved For*), and always include their *Reserved For* numbers, as well as other available numbers.

Related topics

- *Custom inventory filters*

7.4.6. Number inventory audit

Tip: *Use the Action search to navigate Automate*

Overview

The Number Inventory Audit tool provides the ability to perform an audit of the number inventory to ensure that the *status* and *usage* values of each number aligns to the devices or services configured with these matching numbers.

Numbers that are in a *Cooling* or *Reserved* state are included in the audit:

- If the audit finds that these numbers are unused, they are left in a *Cooling* or *Reserved* state.
- If the audit finds that any of these numbers are used - an admin may have manually updated a user in MS Teams to assign the number - then the number's status is changed to a state that indicates they're in use, to *Used* or *Used-Utility* for example, and they're associated with the correct user.

Note:

- For more information about the values for Status and Usage, see *Number status and usage*.
- For vendor-specific audit details, see *UC vendor guidelines for numbers*.
- You can only run the number inventory audit for customers that have number management enabled. See *Create and Modify a Customer*.
- You can view the list of internal numbers, and move, delete, and export them as required, on the **Number Inventory** list view.

For Microsoft environments, available numbers are added (else updated if present) to the inventory, with:

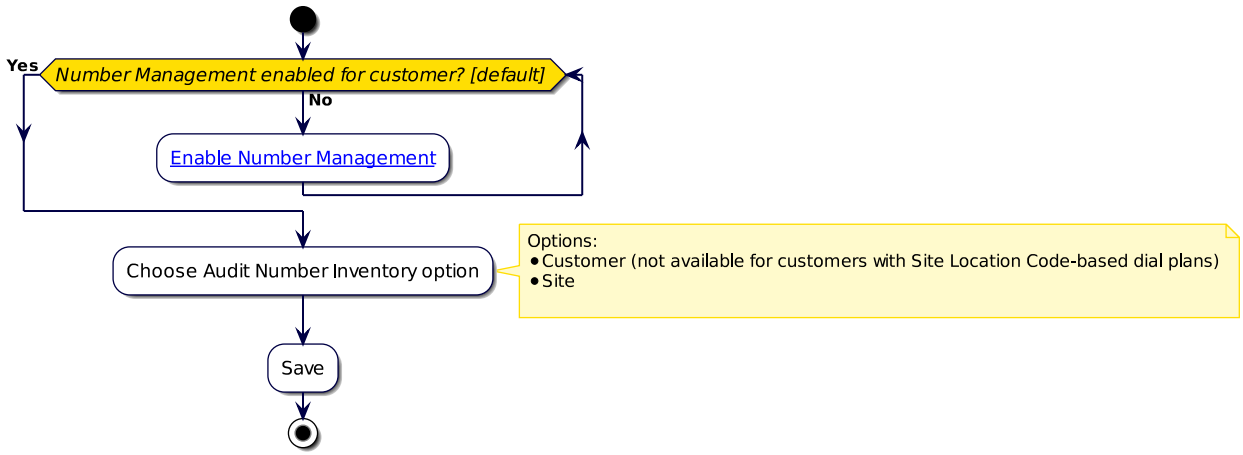
- Status: Available

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Vendor: Microsoft
- Number type: Operator Connect or Calling Plan

Note: For details, see: *Microsoft Teams deployments*

The audit creates new numbers for devices or services that don't already exist, and updates existing number entries so that the **Status** and **Usage** fields display accurate information at the time the audit is run. Importantly, number entries are *not* deleted.



Related topics

- Prevent duplicate numbers in the Core Feature Guide

Number inventory audit and hierarchies

The table describes the difference between running a number audit inventory at the customer level compared to the site level:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Customer	• Running the number inventory audit at *customer* level adds directory numbers at the customer level for services that exist at *site* or *customer* level, provided that there is not already a directory number for that service at *site* level. If there are already directory numbers at the *site* level, then those numbers are also updated. This is a mixed mode of audit, which audits directory numbers at both *customer* and *site* level. For example, if directory numbers only exist at *customer* level, then the audit only adds and updates directory numbers that exist at the *customer*. If there are directory numbers at *site* level, the audit will still add new directory numbers at the *customer* level, but will also update the existing directory numbers at *site* level.
Site	• Running the number inventory audit at *site* level adds directory numbers at *site* level, and updates any existing directory numbers at *site* level only. No *customer* level directory numbers will be audited and no directory numbers will be added to *customer* level for *customer* level services. • You can choose to audit either *all* the *sites* for the *customer*, or selected *sites*

Note: For sites using *Site Location Code-based* dial plans, number inventories can be created only at the *site* hierarchy. The *customer* hierarchy won't be available.

Audit number inventory troubleshooting

The table describes common errors and steps to resolve, when running *audit number inventory*:

Error	Resolution
Duplicate device profiles (same profile name) in different clusters	Ensure that device profiles are not duplicated across the sites.
Duplicate phones (same MAC) in different clusters	Ensure that phones are not duplicated across the clusters.
Same internal number in one or more clusters	Ensure that internal numbers (even in different partitions) are not duplicated across clusters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Prevent duplicate numbers in the Core Feature Guide

Run a number inventory audit

This procedure runs a number inventory audit.

1. Log in to the Automate Admin Portal as a provider or reseller administrator.
2. Select the relevant *Customer* hierarchy level.

   Note: You can only run **Audit Number Inventory** from a customer hierarchy. If you try to run it from a hierarchy that is not of type Customer, you will be prompted to choose a valid customer hierarchy.

3. Go to **Audit Number Inventory**.
4. From the **Is Number Inventory deployed at Customer or Site Level** drop-down, select an option, either of the following:
   - If your number inventory is deployed at customer level, select **Customer**, then click **Save** to run the audit number inventory at all sites at the selected customer.
   - If your number inventory is deployed at site level, choose **Site**, then, at **Would you like to audit all sites or a subset of sites**, select an option:
     - Select **All** to run audit number inventory at all sites at the selected customer.
     - Select **Specific** to choose the sites where you want to audit the number inventory, then select sites, one or more (maximum 200), from **Available** to **Selected** in the transfer box.

       Note: The number of sites you have in your environment may exceed the number of sites displayed in the transfer box. You can use a *contains* search to filter the list for the sites you want to include in the number inventory audit.

   Click **Save** to run audit number inventory.
5. View transaction progress. The number inventory is updated at the hierarchy you specified, and below.

7.4.7. Number inventory alerting

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Alerts can be configured to be sent if a specific internal number inventory threshold is reached - for example, if less than ten percent of numbers are available. This alert then allows for proactive management of the inventory.

Optionally, you can enable email so that a summary of the inventory status is emailed each day when the schedule runs.

There are two key hierarchy elements to the setup:

- Hierarchy the alerting is enabled for - since this is managed through Global Settings, it can be enabled at the required hierarchy level(s) based on your needs and it will be enabled for all hierarchy levels below that. For instance, if you wanted this enabled for all sites, you could enable it at say the customer level. All the sites would then be enabled. Alternatively, if you only wanted this enabled for some sites, you can enable the global setting at those sites only.
- It also includes the concept of an aggregation level - this determines how the calculation for available percentage is executed. For instance, if you set aggregation to the customer level, determining if the threshold is exceed is determined by looking at all the inventories at the customer and below. However, if you set it to site, then the threshold calculation is run for each site and the alert will indicate any site(s) that exceed the threshold.

Therefore, you can determine the best setup based on your specific needs and how you are using the inventory. If you generally use a more a site-based inventory (due to geographical numbers, local breakout, etc) then site aggregation is likely your best option. On the other hand, if your setup is more of a shared number pool environment, then customer level is likely a better aggregation choice.

Use cases would be:

- An administrator wishes to determine if any *sites* within the organization are running low on numbers. Each site has their own dedicated pool of numbers. So the administrator configures alerting at the Customer level with an **Alert Aggregate Level** of “Site” in the **Global Settings**.
- An administrator has a single pool of numbers, shared shared across locations in the organization. So the administrator configures an **Alert Aggregate Level** of “Customer”.

In the event that a Provider would want to monitor any customer that is running low on numbers, they would configure the alert at Provider level and set the **Alert Aggregate Level** to “Customer”.

Configure number inventory alerting

1. In the Global Settings, on the Number Inventory Alerting tab, set **Enable Alert on Available Numbers** to **Yes**, and configure also:
   - Select a hierarchy level at which the *aggregate* of available numbers should be calculated.
   - Select or fill out a percentage available of the total numbers at which point alerts will be raised.
   - Enable an Email Group to be notified and select it.

     Email content templates can be configured.

     See Number Inventory Alerting Email Template Variables section under Email Setup in the Core Feature Guide.
   - Ignore hierarchies with no numbers.
2. If required, modify scheduled time for alerts.

   When alerts are enabled, a schedule called `InternalNumberInventoryAlert` is created that, by default runs daily at the time `00:00:00` and raises an alert if the availability threshold in the global settings

Copyright © 2025 VisionOSS Limited. All rights reserved.

is exceeded. This scheduled time can be modified. See *Create or Update a Schedule* in the Core Feature Guide.

3. View raised alert messages, which display via the **Messages** toolbar icon, or via the **Alerts** page.

   See Number Inventory Alerts under Alert Types in the Core Feature Guide.

Related topics

- See the Number Inventory Alerting tab description for Global Settings in the Core Feature Guide.

7.4.8. Prevent duplicate numbers

Tip: *Use the Action search to navigate Automate*

Overview

Automate provides a Global Setting for Microsoft deployments, *Prevent Duplicate Numbers*, which prevents the system from creating duplicate numbers in the internal number inventories of different sites, either manually via number range management or automatically via syncs.

When *Prevent Duplicate Numbers* is enabled, any attempt to provision a number that already exists at another site will fail, stopping duplication at the source and surfacing a clear error for administrators to resolve. This includes a scenario where you're provisioning a number via, for example, flow through provisioning set up for *Use Next Available Line*. In this case, if duplicates exist and the number is available at one of these sites, the transaction will fail as the number is already in use at one site. The user is synced in, moved, and provisioned, but no number is assigned.

This feature allows administrators to ensure that the internal number inventory contains unique directory numbers across sites. When relevant workflows are triggered, the system checks for existing numbers before creating new ones, partially failing transactions that would result in duplicates (only the duplicate number creation step fails), and logs errors for review.

Preventing duplicate numbers is relevant only for the internal number inventory. E164 numbers, for example, are unique and cannot be re-used. However, if you're using E164 dial plans, it is recommended that you enable prevention of duplicate numbers as you may not realize that duplicates are being created and added to your internal number inventory during syncs and when creating number ranges.

For deployments that allow duplicate numbers, you can leave *Prevent Duplicate Numbers* disabled (*No*).

The table describes scenarios that may result in the creation of duplicate numbers, and how enabling *Prevent Duplicate Numbers* handles these cases:

Note: When HCS dial plans are in use, *Prevent Duplicate Numbers* is a read-only setting and is disabled for syncs or when creating number ranges.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Scenario	***Prevent Duplicate Numbers* enabled**
Sync in a user to a site (SiteA) with their number, but number already exists at another site (SiteB)	The number is not created at SiteA. The rest of the sync workflow executes successfully. A transaction error informs you that the number already exists at SiteB.
Create a number range at customer level, and part of the range already exists at the customer or at any site below it	The duplicate number is not created, but the rest of the (valid) number range is created. The log message flags numbers in the range that are duplicates, and indicates their current location (site or customer).
Create a number range at the site level, and part of the range already exists at the customer, the current site, or at other sites in the customer tree	The duplicate number is not created, but the rest of the (valid) number range is created. The log message flags numbers in the range that are duplicates and indicates their current location (site or customer).
Run a data sync workflow at the customer level that triggers the creation of an internal number inventory (INI) at the customer level	A number that already exists at the customer level is updated and marked as *Used*. A number that exists at a single site belonging to the customer is updated with additional details from the sync. For a number that exists at multiple sites, the transaction fails with async errors with a message indicating that the number won't be created due to existing duplicates. If a number does not exist at the customer or at any sites belonging to the customer, the transaction passes, and the number is created and marked as *Used*.
Run a data sync workflow at the site level that triggers the creation of an internal number inventory (INI) at the site level	A number that already exists at the customer is updated and marked at *Used*. If any number exists at any other sites, the transaction completes with async errors with a message indicating the that the number won't be created due to existing duplicates. The number at the other site is updated with the new user details. If a number exists at the target site it is updated with details and marked as *Used*. If a number does not exist at the customer or any site, the transaction succeeds, the number is created and marked as *Used*.

Related topics

- Global Settings in the Core Feature Guide
- *View a transaction*
- *Transaction logging and audit*
- Introduction to data syncs in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure prevention of duplicate numbers

1. In the Admin Portal, select the relevant customer hierarchy.

   Note: The **Prevent Duplicate Numbers** global settings is hidden in the global settings at the site or linked site level. The setting displays only above site or linked site level and only when Microsoft is enabled for your environment.

2. Go to **Global Settings**.
3. On the **Number Inventory** tab/panel, set **Prevent Duplicate Numbers** to *No*.

   Note: In the Global Settings, this field is enabled and can be configured only when **Enforce HCS Dialplan Rules** is set to *No* (disabled).

4. Save your changes.

Troubleshooting duplicate numbers

Assuming you have *Prevent Duplicate Numbers* enabled, if you're creating a number range or syncing in users and your transaction results in a number inventory error where the number could not be created because it already exists, then try the following steps to resolve the error, depending on your scenario:

- Delete the number range range from the site where the duplicate exists, then recreate the number range at the new site. You can then run an audit of the number inventory.
- The user you're syncing in may have been assigned an incorrect number (a number that already exists at another site in Automate) in the Microsoft Teams cloud portal, or they've been synced in to the incorrect site. In this case:
  - Either move the user to the site where their number exists
  - Or, offboard the synced in user and assign a different number

Related topics

- *Offboarding (Microsoft)*
- *Number inventory audit*
- *Microsoft - Move user & services*
- *Move users*
- *Number range management*

Copyright © 2025 VisionOSS Limited. All rights reserved.

7.4.9. Number inventory

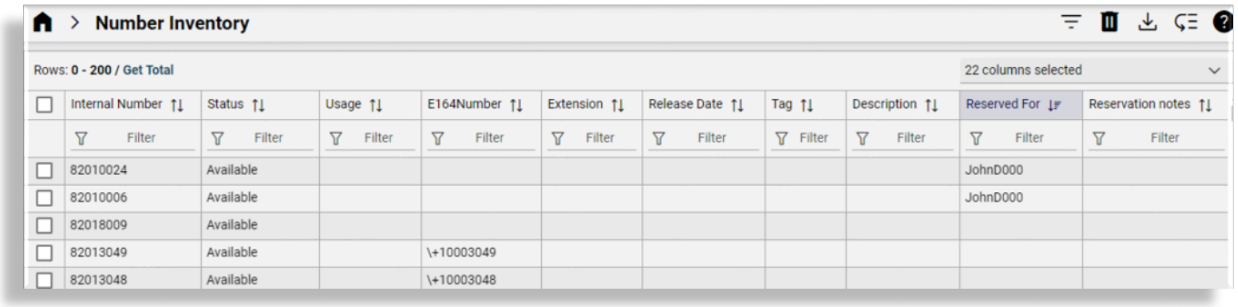
Tip: *Use the Action search to navigate Automate*

Overview

The Automate number inventory allow you to view and manage the numbers used by users, devices, and services for the given hierarchy level. The number inventory includes a combination of data that is automatically managed by the system (such as usage), and other fields that are configurable and available to store any additional useful information you choose about the numbers (such as ranges, billing IDs, and circuit IDs), to complete your inventory view.

Important: The number format in the Automate Internal Number Inventory (INI) is with prefix \+, including a leading slash \ when the INI is in E164 format.

Verify that entries in the **Internal Number** column of the Number Inventory - also Webex Calling numbers - follow this format.



The Automate number inventory functionality supports a range of capabilities outside of the basic loading and tracking of inventory status.

The table describes the additional number inventory capabilities:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Functionality	Description
Number Reservation	Numbers can be reserved and made unavailable until you change their *reserved* status (unreserve). Reserved numbers can't be assigned to any user, device, or service. When reserving a number you can add a note about why its reserved.
Reserved For	Allows the admin to flag numbers (INI) as reserved for a specific user. When used with the *next available number* option for onboarding and provisioning, the system first looks for a number reserved for the user you're working with. If there's a match, this number is assigned to the user at the site. If no match is found, the next available number is assigned to this user. A number that is reserved for a specific user cannot be assigned to a different user unless the **Reserved For** flag is removed.
Number Cooling	Numbers can be placed into a cooling period, either manually or automatically. Placing a number into *cooling* quarantines the number for a specified number of days so that is can't be reused for that period. When automated number cooling is enabled, numbers are placed into cooling for a predefined period when the subscriber or phone associated with the number is deleted. Automated number cooling is enabled and disabled in the Global Settings. The default is disabled. A number that is in *cooling* is unavailable and can't be allocated to a subscriber, phone, or device. A number is released from cooling and is available for use when: • The cooling period reaches its end date • The number is manually released from the cooling period
Number Audit	Checks the inventory against the currently configured devices and updates the inventory where needed to keep the inventory in sync for changes made outside the system.
Number Inventory Alerting	Configure alerts to be sent if a threshold is met (e.g less than 10% of numbers are available) to allow for proactive management of the inventory.

Note: Typically, numbers are pushed to the UC applications when they're assigned to users, devices, or services.

While some available numbers may be in the UC apps for various reasons, the platform is not trying to maintain the available numbers in the underlying UC applications as it is only important when assigning the numbers to be used.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Number inventory alerting*
- *Number cooling*
- *Global settings*
- Reserve a number for a user in the Core Feature Guide

Number inventory and hierarchy in Automate

To ensure proper visibility and allocation, numbers should be added to the inventory at the correct hierarchy level in Automate, based on where and how they will be used. Proper planning of hierarchy and inventory allocation is essential for a scalable and efficient setup when building out the number inventory.

Hierarchy relationship

- Inventory numbers can be placed at the same level or higher than the users, services, or devices they're assigned to.
- The hierarchy level of a number determines its visibility for MACD (Move, Add, Change, Delete) operations like user onboarding.

Choosing the right hierarchy level

Consider the following scenarios when deciding where to load inventory numbers:

- **Site-level numbers**

  Use the site level if numbers are tied to a specific site due to:

  - Local trunks
  - Area codes
  - Emergency routing

  Assign these numbers directly to the site in Automate so they're only available for that site's users and services.

- **Intermediate nodes**

  If a number range is shared across multiple sites within a region, city, or country:

  - Group the sites under an intermediate node.
  - Assign the inventory to that node to allow shared access across all included sites.

- **Global use**

  If numbers aren't tied to specific sites:

  - Assign these numbers to a common hierarchy node, such as customer level.
  - This is ideal for centralized environments or enterprises operating within a single region.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial plan considerations

If using dial plan schemas, the schema rules may dictate where numbers must reside. For example, site-based dial plans with site codes require numbers to be loaded at the site level.

System behavior

Automate does not automatically move inventory numbers to match the hierarchy of the assigned service.

- Example: A number at the customer level assigned to a site user will remain at the customer level unless manually moved.
- Admins can relocate numbers if needed, but this is not required (the admin may simply prefer the number to be at the same hierarchy).

Typical usage

Users, devices, and services that will consume numbers usually exist at the site level. Therefore, inventory numbers should be placed at the same site, or above (intermediate or customer level).

You can also combine strategies:

- Site-specific numbers at the site level.
- Shared pools at intermediate or customer levels.

Number inventory and end-user provisioning

The number inventory is integrated into various features in the system to:

- Display options of numbers for selecting/assignment across the system. Numbers presented for selection follow rules specific to the feature in many cases, for instance, whether lines can be shared or not.
- Manage the state of the numbers in the inventory via the workflows - marking the number used, available, and updating other managed fields depending on the MACD being performed. This includes any specific logic setup for the un-managed fields. See the section on flexibility for options to control the update that occurs.

Related Topics

- *Number status and usage*
- *Number cooling*
- *Number reservation*
- *Number inventory alerting*
- AudioCodes Device Number Integration in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

UC vendor guidelines for numbers

This section provides UC vendor-specific guidance and behaviors related to how their numbers are handled in Automate.

Cisco UCM/dedicated instance

When the Automate number inventory is used in a Cisco UCM/Webex Dedicated instance environment:

- The value for the **Vendor** field is either *Cisco* or blank, depending on how numbers are loaded
- The **Internal Number Type** field is not relevant in UCM or Dedicated Instance deployments

Partition and cluster

The Automate number inventory is not partition or cluster aware:

- If the same numbers are used multiple times but in different *partitions*, these all map to the same number. This should be considered for the hierarchy level at which the number inventory exists.
- If the same number exists on different *clusters*, this will map back to the same inventory value unless numbers are assigned to the site level.

Cisco-Microsoft hybrid number inventory

This section applies if you're using Automate's Cisco-Microsoft hybrid feature for integrated services.

A Cisco-Microsoft hybrid setup is an integration of Cisco and Microsoft capability, where Microsoft calls are routed via Cisco UCM.

In a hybrid setup, the internal number inventory (INI) can be set up in two ways:

- E164 number based, for example:
  - an INI entry 3334567 is mapped to an external number of +15553334567.
  - The number 3334567 is set up in Cisco (along with routing for the mapped external number).
  - The number +15553334567 is set up in Microsoft as the line.
  - The numbers 3334567 and +15553334567 should be seen as the *same* number from an INI tracking perspective.
- Internal number based (site code+extension or just extension)
  - an E164 number is generated by adding a prefix (+88800) to the internal number for setup in Microsoft.

    Note: A name macro, `MultiVendorLine-InternalExt-E164Prefix`, is used to store the prefix - currently set to *+88800*.

  - For example, 3334567 is set up as an internal number for the user and no external number is mapped. The line is selected in the Hybrid setup. Then the prefix is added, so the number +1888003334567 is the number in MS Teams for that user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Important: The numbers 3334567 and +888003334567 should be seen as the *same* number from an INI tracking perspective. The mapping is also reflected in the *Number inventory audit*. In this case, an update of the inventory takes place so that these are not counted as two separate numbers.

The table summarizes the number inventory data for these cases:

Note: **Extra2** and **Extra4** hold the service type and E164 number (includes generated) respectively.

Scenario	Status	Vendor	E164 Number[7]	Usage	Extra2	Extra4
Cisco-MS-Hybrid	Used	Cisco, Microsoft	Exists	Device, User	Cisco-MS-Hybrid	<blank>
Cisco-MS-Hybrid[8]	Used	Cisco, Microsoft	<blank>	Device, User	Cisco-MS-Hybrid	+88800<INI>
Cisco-No-Services	Avail	<blank>	<blank>	<blank>	<blank>	<blank>
Cisco-Only	Used	<blank>	Exists	Device	<blank>	<blank>
MS-Only-Entvoice	Used	Microsoft	Exists	User	MS-Only-Entvoice	<blank>
MS-Only-Entvoice	Used	Microsoft	<blank>	User	MS-Only-Entvoice	+88800<INI>
MS-Only-Hybrid	Used	Microsoft	Exists	User	MS-Only-Hybrid	<blank>
MS-Only-Hybrid	Used	Microsoft	<blank>	User	MS-Only-Hybrid	+88800<INI>
MS-Only-No-Entvoice	Avail	<blank>	<blank>	<blank>	<blank>	<blank>
No-Hybrid-Service	Avail	<blank>	<blank>	<blank>	<blank>	<blank>

For details on the service type scenarios, see Multi Vendor Service Definitions in the Core Feature Guide.

Footnote

Microsoft Teams deployments

The use of the inventory and how it is maintained or managed can differ depending on the types of numbers in your environment. The following is some guidance and best practices to consider for the different number types. If you have a mix of number types, then consider the notes for different number types.

In the number inventory:

- The **Vendor** field value is typically `Microsoft`. If numbers aren't loaded with this value initially, the system updates the numbers as they are allocated to vendor `Microsoft`.

[7] If assigned (and associated with Extra4 - prefix e.g. +88800)
[8] Generated TelURI will start with prefix e.g. +88800

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **Internal Number Type** field is used to reflect the type of number in a Microsoft environment, either of the following:
  - Direct Routing
  - Operator Connect
  - Calling Plan

  The internal number type can be selected when loading the numbers. It is recommended that the relevant values are chosen. Typically, the system also updates the value for this field as required during audit or allocation of numbers, if they're incorrect or left blank.

General Notes

The hierarchy consideration is a key section in this chapter to read in planning for numbers in the inventory. Often the numbers are meant to be used in specific sites or regions only due to agreements or emergency services requirements. This is the business context which the Automate number inventory can provide when the numbers are loaded into the inventory at the appropriate hierarchy level. It is often found, after adding Automate to an existing environment, that we identify various numbers that have been incorrectly assigned previously and allow them to be corrected. Any numbers that were added to the Automate inventory through the sync/audit process will likely require moving to the correct hierarchy level. You can find more information related to the specific numbers types below.

This section covers specific logic related to creating and managing the inventory in relation to specific number types in the Microsoft environment. In Automate you can mix and match the types for different needs, so one or more of the sections may apply.

Direct Routing

In this type of setup, you are getting ranges of numbers outside the Microsoft framework from one or more providers. For these number types, the Microsoft tenant only knows about the numbers that you have assigned to users/services. The tenant has no knowledge of the ranges or available/unused numbers.

So the Automate number inventory capability can only auto-populate the inventory from a sync/audit with those used numbers discovered from the tenant. In this scenario, you will need to load the available numbers into the Automate number inventory to be managed and available for administrators to assign going forward.

Guidelines for this setup:

- You can preload the ranges of numbers you own ahead of any overbuild process that will sync/audit the inventory. In this case, the system will update the inventory as part of the sync/audit process to mark assigned numbers used. It will still add any used numbers it discovered form the tenant if there were any missed in the preload process.
- You can load the full ranges after the overbuild process - this will fill in the inventory around the used numbers that were discovered and auto created in the inventory from the tenant. You may need to move the created numbers to a different hierarchy level depending on your needs (intermediate node, moving to site/customer). When you load the ranges after the sync/overbuild, the system will fill in the gaps by adding numbers as available that are missing in the inventory while leaving the ones added via the sync/audit process alone.
- Any future ranges you add to the system beyond the initial overbuild will need to be added to Automate to be available for administrators to use.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Operator Connect and Calling Plan numbers

In this type of setup, you are getting ranges facilitated by the Microsoft Teams framework. For these types of numbers, the Microsoft tenant is fully aware of the ranges of numbers available as they are populated into the system by Microsoft (Calling Plans) or the selected Provider (Operator Connect). So it is important to note the numbers can only actually be used (e.g assigned to a user) when the numbers are available in the Microsoft Tenant post ordering – from Microsoft (Calling Plan) or the selected Provider (Operator Connect). If you add them to the Automate inventory and try to allocate them before they are present in the tenant, you will get an error message about the numbers not existing in the tenant.

Currently, the data we receive from the Microsoft tenant about the numbers does not provide any information regarding how the numbers are to be used - e.g site specific, etc.

The hierarchy recommendations earlier in this chapter should be referenced and numbers should be loaded according to how the numbers are ordered and registered with Microsoft or the Provider (e.g site specific, global, etc).

The best practice recommendation to streamline the inventory management of these number types is:

- Number ranges are loaded into the Automate number inventory at the appropriate hierarchy *before* they're synced in from the Microsoft tenant
- This ensures that the numbers are at the correct hierarchy level and context in the system for use in the system - that users and services can only be assigned appropriate numbers.

  Important: New Calling Plan numbers cannot be assigned to users unless an emergency location is set.

  To set the emergency location for new Calling Plan numbers:

  1. Select the relevant customer or site hierarchy, then go to **Emergency Location Ops Tool**.
  2. On the Ops Tool form, verify that **Number Type** is set to `CallingPlan`.
  3. Select an **Emergency Location** from the drop-down. Also ensure a temporary user is created at the location and has the Calling Plan assigned.
  4. Click **Save** to update the emergency location of the numbers at this hierarchy where this has not been set.

- When the sync/audit process completes, the system updates those inventory entries with status, usage, type, etc., and won't move them.

Automate can generate inventory entries for numbers of these types. However, there are some considerations and for this reason it is recommended to preload the numbers for improved accuracy and ease of use.

The following are considerations of the generated inventory and potential actions if the sync/audit was run before you loaded your inventory:

- It will generate inventory entries for numbers assigned to users/services in the tenant only. We do this for assigned numbers to ensure they are at least captured and since they are assigned there is not a risk of being assigned incorrectly.
- Numbers that are not assigned will not be generated in the inventory. This is to avoid available numbers being created at the wrong place in the hierarchy and inadvertently being assigned to users in the wrong sites, etc.
- It will create the generated inventory entries at the same hierarchy level as the tenant details (typically customer). Typically, they are required at a different level in the hierarchy and they will need to be moved after this creation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The ranges will need to be loaded to create the available numbers in the range within the inventory so they are available to be assigned to users/services. You can just load the whole range and the system will fill in the blanks, creating inventory entries for missing numbers while leaving existing numbers (created by the sync) alone.

You can look at the number data provided by Microsoft for these number types by reviewing the `device/msteamsonline/Number` device model. Note - these model instances will always be at the same level as the tenant - they do not get moved around and are completely independent of the inventory entries for the numbers.

Number inventory for Webex Calling

This section describes number inventory handling in a Webex Calling environment.

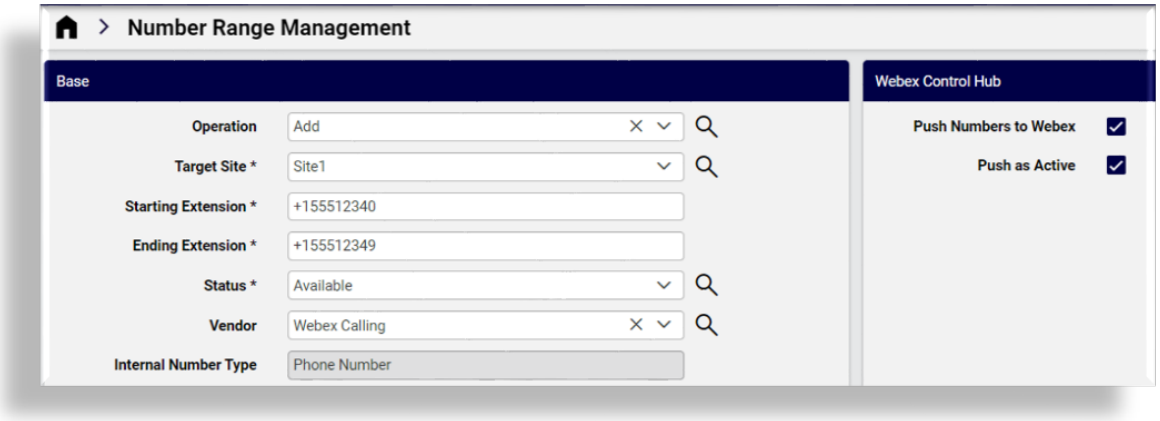
Key considerations in a Webex Calling environment:

- In a Webex Calling environment, resources all reside in locations including numbers regardless of the source (for example, CCP, non-integrated CCP, or Cisco).
- PSTN numbers must be loaded into Webex as available numbers before they can be used/assigned to users. This process can vary depending on how you're sourcing the numbers - for example, CCP, or Cisco Cloud. For this reason, the numbers are typically already in Webex - to pull into the Automate system and inventory.

From the **Number Range Management** page at a site:

- For numbers and ranges of numbers, **Starting Extension** and **Ending Extension** number values must be prefixed with + and are then created and maintained in Automate with the prefix format `\+`. When adding numbers, this can also be seen in the **Transaction** detail.
- **Vendor** – this field will typically be `Webex Calling`. If they are not loaded with this value initially, the system will update the numbers as they are allocated to vendor `Webex Calling`.

Note: Numbers can be pushed to the Webex Control Hub when adding number ranges at site level with the Vendor set as `Webex Calling`.



- If the **Operation** is *Add*:

  When *adding* numbers and selecting the **Vendor** as `Webex Calling`, a **Webex Control Hub** panel displays the options if:

  1. The Webex App is configured at the customer hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

See the Webex App chapter in the Core Feature Guide.

2. The available macro `WebexCallingNumberMgmtEnabledSite` has not been cloned to the site and set to value False. (If required, this task can be carried out if Webex Calling number management should be disabled for a site.)

   The options are:

   – **Push Numbers to Webex**: this allows for numbers to be added to the site in Automate and to the Webex Control Hub. (Refer to the `Create Spark Number` action in the **Transaction** list.)

   – **Push as Active**: dependent on the option **Push Numbers to Webex** set to enabled.

     If enabled and **Push Numbers to Webex** is enabled, numbers are added in Automate INI added as **Status** of **Available**, and on Webex Control Hub created as **Active**.

     If disabled and **Push Numbers to Webex** is enabled, numbers are added in both Automate INI and the Webex Control Hub as **Inactive**.

     Number extensions are added to the INI when a user is assigned a number and an extension is then added.

- If the **Operation** is Modify:

  This operation can be used on selected numbers that are in **Status** of **Inactive** - to set them as:

  – **Active** in the Webex Control Hub. Refer to the `Activate Spark Number` action in the **Transaction** list.

  – Status is **Available** in the Automate INI.

- If the **Operation** is Delete:

  Selected numbers are deleted from Automate INI and the Webex Control Hub. Refer to the `Delete Spark Number` action in the **Transaction** list.

- **Internal Number Type** – this field is used to reflect the type of number in the Webex environment. If you are adding or activating numbers via Number Range Management then the type is `Phone Number`. Any numbers marked as `Extension` have been synced in from the Webex Control Hub.

Since the numbers are known in the Webex environment, as well as the Locations for use, the Automate system will generate the inventory based on the data from Webex. This includes:

- The sync process handles the creation of inventory entries in the Automate platform as numbers are pulled in. You should ensure the sync process handles Locations in Webex prior handling numbers (out of the box syncs ensure this).

- During a site handling Webex Locations, if a corresponding Automate site does not exist, Automate will create a site.

  See the Webex Location Node Mapping topic in the Core Feature Guide for more details on Site to Location mapping for Webex for more details on how they are aligned.

- When Webex numbers are synced into Automate, the prefix format \+ is used. Any inventory entries that don't exist are created in the Automate site corresponding to the Webex Location. This includes PSTN numbers and also internal-only extensions.

- The internal number in the Automate number inventory uses the PSTN number (if it has one); or it uses the extension number, if that is the only data available.

- For PSTN numbers, the extension (if there is one) is also captured in the number inventory record via the **Extension** field.

- Removal of numbers

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Typically, inventory audit functionality won't be required if good sync practices are followed, as the inventory changes are handled through the sync process.

7.4.10. View number details and usage

Tip: *Use the Action search to navigate Automate*

Overview

To view the details of a number in the number inventory, go to the **Number Inventory** list view, then click on a number to open its details page.

Related topics

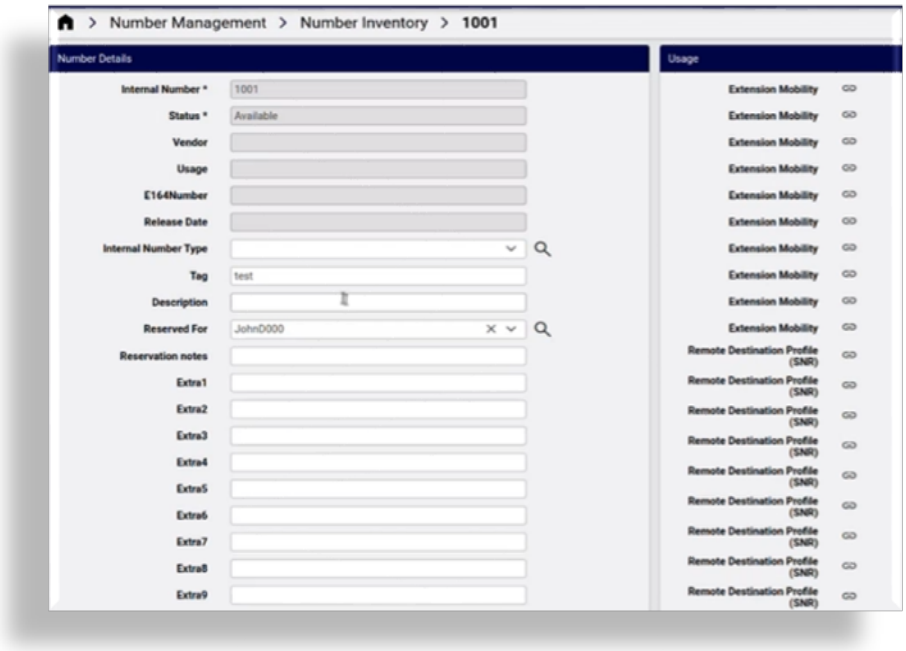
- *Number range management*
- Prevent duplicate numbers in the Core Feature Guide

Number settings

The management page for a number contains two tabs/panels:

Note: You can toggle between a tab/panel layout via a toolbar icon.

- Number Details
- Usage



Copyright © 2025 VisionOSS Limited. All rights reserved.

Number Details tab/panel

The **Number Details** tab/panel displays both read-only and editable fields. For example, you cannot update the internal number, or its status, vendor, usage, E164 number, or release date (if applicable).

Note: In the case of Cisco-Microsoft hybrid entries, the vendor added would be “Cisco, Microsoft”.

You can update the following details for a number on the **Details** tab/panel:

- Update the internal number type
- Add or edit a tag
- Add or edit a description
- Choose a user to reserve this number for
- Add reservation notes
- Fill out additional custom attributes

The table describes the fields on the **Number Details** panel/tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Internal number	Numbers created in the number inventory are in Automate only. These are not synced to Cisco UCM.
Status	Current status of the number. Options are: • Available • Used-Utility • Used • Cooling • Reserved
Vendor	Optional, typically used to designate vendor-specific information for a device in a multi vendor setup.
Usage	**Available** and **Usage** is empty when a number is first added to the number inventory.
E164Number	Displays E164 Associations (N to 1 DN), depending on the number of E164s associated and whether a primary E164 is set or not.
Release Date	Defines the date on which a number that is currently in **Status**: Cooling or Reserved will become available again.
Internal Number Type	Used in conjunction with the **Vendor** field. See the vendor specific section of Number Inventory topic for more details on usage in different vendor use cases.
Tag	A free text field, auto-populated when a new number or range of numbers is added. Used to identify or comment on a number or number range.
Description	Free text field, available to provide additional information for a given number or range of numbers.
Reserved For	If you want to reserve a number for a specific user, choose the user from this drop-down.
Reservation notes	A free text field, typically used to provide more details about a status **Reserved** number.
Extra	**Extra1** to **Extra9** fields are free text fields that are available to provide additional information for a given number or range of numbers. Field Display Policies can be used to change the field names and also add tooltip help text to reflect how you want to use the fields.

Usage tab/panel

The **Usage** tab/panel provides links to all instances where the number is used, representing a dynamic view of all the service(s) that are assigned to that number. This includes links to easily navigate to the service instance for further details or to unassign the number if required.

Note: If the same number is shared by multiple devices/services of the same type, only the first 10 instances display.

- In the case of Cisco-Microsoft hybrid usage, the last vendor added would be appended, as seen above in the “Device, User” instances.
- In the case of **Webex App Calling** usage, the link directs to the Webex App user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

See *Webex App* in the Core Feature Guide.

Note: If the same number is shared by multiple devices/services of the same type, using different partitions, only the first 10 instances are displayed.

Related topics

- Webex App in the Core Feature Guide.
- Prevent duplicate numbers in the Core Feature Guide

Managed and non-managed number inventory fields

Automate provides two types of number inventory data fields, managed by Automate, and un-managed:

- Managed - managed by Automate:
  - **Status** - managed automatically by the system
  - **Vendor** - can be set on loading the range; afterwards it is managed automatically.
  - **Usage** - managed automatically
  - **E164Number** - if the number has an E164 number associated in the system it is shown here (read only). If not using E164 number inventory, then not relevant and you can hide the field.
  - **Release Date** - if the number is in Cooling, this is the date/time the number will become available - managed automatically. See number cooling for how to change the cooling status for a number.
  - **Internal Number Type** - set when adding then managed automatically if relevant.
- Un-managed - not managed by the system:
  - **Tag** - free text and can be utilized as needed
  - **Description** - free text field that can be utilized as required for additional useful information
  - **Extra 1-9** - free text field that can be utilized as required for additional useful information

    These additional useful information fields can be utilized to store any extra business information you require to store in the inventory with the numbers. This can be static data defined when the numbers are loaded or updated or it can be dynamically updated as the system manages the numbers (allocated to a user, unassigned, etc). For instance, the system provides some out-of-the-box options for description to utilize, or if you want to set a value in **Extra1** when events happen in the system.

    See Number Inventory Flexibility and Description Customization in the Advanced Configuration Guide on how to utilize this capability.

    If you are using any of the fields to store additional information, you can re-label the fields and include relevant help text for tool tips to be meaningful for administrators according to the data you are storing (e.g Billing ID if using a field for that) by means of a Field Display Policy for the `relation/NumberInventory` model.

For more details on the automated logic for managing status and usage, see *Number status and usage*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Edit a number via the number inventory

You can update some (editable) details for a number when clicking on that number from the **Number Inventory** page.

To modify a range of numbers, see *Number range management*.

Reserve a number for future use via the number inventory

To reserve a number that you're viewing from the number inventory:

1. Go to the **Number Inventory** list view.
2. Click on an unused number to open its detail view.

   Note: Only numbers that are currently in status *Available* or already in *Reserved* state can be moved to reserved state.

3. From the toolbar overflow menu, select **Reserve Number**.

   Note: If the transaction succeeds, the number is reserved.

Related topics

- *Number range management*
- *Number reservation*
- *Number status and usage*
- *Number cooling*
- Reserve a Number for a User in the Core Feature Guide

7.4.11. Line Search

The **Line Search** utility enables you to quickly search for all devices and services associated with a selected line.

A **Search Line** drop down of lines is the list of available lines on the Internal Number Inventory (INI) at a selected customer hierarchy and downwards, with used lines indicated as (used). The E164 number associated with the INI is also shown if available.

The devices and services included in the line search are:

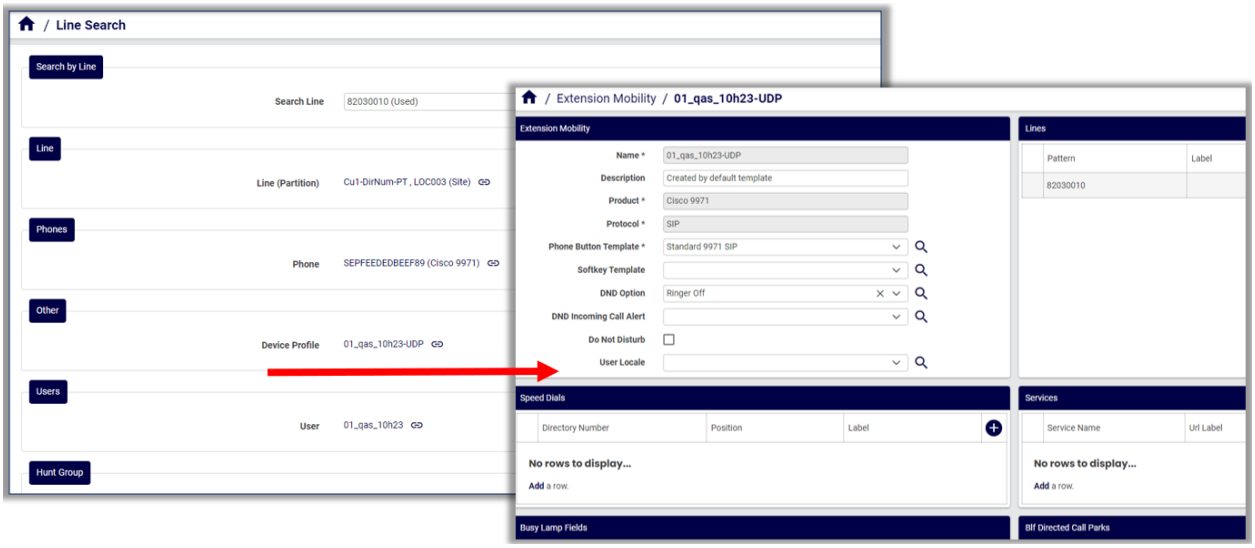
- Phones
- Users
- Hunt Groups
- Call Pickup Group
- Device Profile
- Remote Destination Profile

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Voice Mail account

Search results are displayed as a list of grouped identifiers with links that allow you to directly navigate to the individual service or device details, for example, for lines with extension mobility, clicking on the **Device Profile** link opens the **Extension Mobility** management page.

Note: If the same number is shared by multiple devices/services of the same type, using different partitions, only the first 10 instances will be displayed.



7.5. E164 Numbers

7.5.1. Introduction to E164 inventory management

E164 inventory management uses translation patterns in Automate to provide a Direct Dial-In (DDI)/Direct Inward Dialing (DID) mapping to internal numbers.

DDI-to-DN mapping allows you to route incoming PSTN calls to the appropriate internal number.

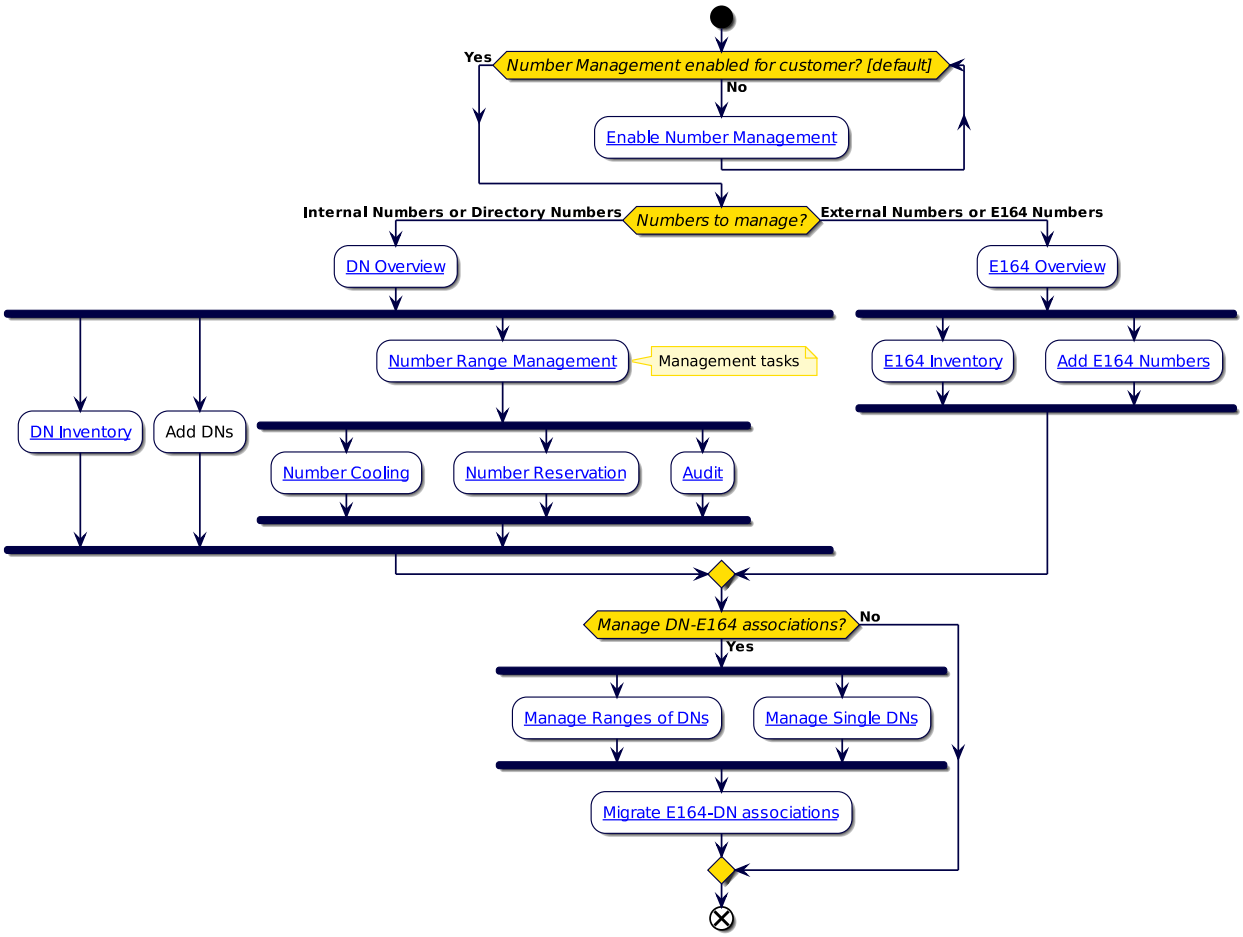
Managing the E164 inventory involves:

- Viewing, adding, or deleting E164 number inventory
- Associating a range of E164 numbers to a range of internal numbers
- Viewing an associated range of E164 numbers to a range of internal numbers
- Disassociating a range of E164 numbers from a range of internal numbers
- Associating a range or set of E164 numbers to a single internal number
- Disassociating a range or set of E164 numbers from a single internal number
- Viewing single internal number associations

The E164 inventory is available in the drop-down menus for Site Published Number and Emergency Number when creating a Site Dial Plan.

- Note: Underlined flowchart titles refer to topic headings in this guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.



7.5.2. E164 numbers in the number inventory

Note: In Automate, a wildcard ('*') can appear before a directory number in a Type 4 dial plan.

The **E164Number** column and value displays E164 Associations (N to 1 DN), depending on the number of E164s associated and whether a primary E164 is set or not.

Examples of E164 format:

Note: The first example below is for E164 Associations (N to N DN):

- `\+27726043938`

  No primary is set. The first number associated is displayed. Only one number is associated.

- `\+27726043938 (P)`

  The displayed number is primary. Only one number is associated.

- `\+27726043938 (P) [+8]`

  The displayed number is primary. Eight (8) more numbers have been associated in addition to the displayed number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `\+27726043938 [+8]`

  No primary is set. The first number associated is displayed. Eight (8) more numbers have been associated in addition to the displayed number.

This type of number cannot be reached from an outside line. Typically, a number with the '*' prefix is not called from another line (user), but is tied to a service feature such as call pickup, hunt groups, or contact center.

Note: Adding a new number to the number inventory on Automate does not add a number on Cisco Unified Communications Manager (CUCM / CallManager) until it is associated to a line.

7.5.3. Add an inventory of E164 numbers

Tip: *Use the Action search to navigate Automate*

This procedure defines an inventory of E164 numbers available to users at a customer hierarchy *only*.

Important: Each addition to the E164 inventory must contain a unique set of numbers. That is, you can't assign the same number more than once (globally).

1. Go to **Add E164 Inventory**.
2. Choose the relevant hierarchy.
3. Fill out and select relevant values on the **Add E164 Inventory** page:

Fields	Description
Site	For a site-specific E164 inventory, select the customer site. For a customer-wide E164 inventory, leave this field blank.
Country*	Mandatory. Select the country associated with the E164 inventory. If you chose a site in the previous field, this field is automatically populated with the country associated with the site.
Country Code	Read-only field. The country code for the selected country. Refer to this read-only field when specifying the **Starting Number** and **Ending Number** fields, which must contain a valid country code.
Starting Number*	Mandatory. Enter the starting number of the range of E164 numbers. The field is populated with '+' followed by the country code for the selected country. Append the rest of the starting number after the country code.
Ending Number	Optional. Enter the ending number of the range of E164 numbers. The format is the same as the **Starting Number**. If not provided, the single E164 Number specified in the **Starting Number** is added. If provided, the range of E164 Numbers is added: **Starting Number**, **Ending Number**, inclusive. A maximum of 1000 numbers can be added at a time.
Number Type	Number type,e.g. geo, non geo, etc. Informational only. The field may be hidden.

3. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

7.5.4. View an E164 inventory and delete E164 numbers

Tip: *Use the Action search to navigate Automate*

View E164 number inventory

To view an E164 inventory, go to the **E164 Inventory** page.

This page presents the list of E164 numbers (the inventory) at the customer or site (depending on the hierarchy you're at). At higher levels of the hierarchy, for example, Provider, the **Located At** column shows whether the number is at a customer or site. Click on the link for the customer or site to view the numbers in the inventory at that customer or site.

To view (read-only) details for an E164 number, click on the number in the list.

The list view on the **E164 Inventory** page provides the following information:

Column	Description
E164 Number	The individual E164 number in the inventory.
Country	The country associated with the E164 number.
Associated Flag	Indicates the E164 number has been associated with a Directory Number
Located At	Indicates the hierarchy of the site the E164 number was created for.

Delete E164 numbers from the inventory

This procedure deletes one or more E164 numbers from an E164 inventory.

Note: You can't delete E164 numbers that are associated with an internal number.

1. Log in as provider, reseller, or customer administrator.
2. Go to the **E164 Inventory** list view.
3. Choose an option:
   - Delete one number? Select the number, then click **Delete**.
   - Delete multiple E164 numbers? Select the checkbox adjacent to each number you want to delete, then click **Delete**.

     Note: Use column filtering, or click on the **Located At** column to narrow and refine the list of items to select for a batch delete.
4. Click **Yes** to confirm the deletion.

Copyright © 2025 VisionOSS Limited. All rights reserved.

7.5.5. E164 associations (N to N DN)

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes managing a range of internal numbers (Directory Numbers, or DNs) associated with a range of E164 numbers.

View E164 associations (N to N DN)

To view the ranges of E164 numbers that are associated with a range of internal numbers (Directory Numbers, or DNs):

1. In the Admin Portal, go to the **E164 Associations (N to N DN)** list view.
2. View E164 associations (N to N DN) in the list.

Note: You can filter the list and change the hierarchy by selecting a link in the **Located At** column.

The table describes column data in the **E164 Associations (N to N DN)** list view:

Column	Description
E164 Number	The starting E164 number in the range.
DN Number	The starting internal number in the range.
Range	One of the following: • 1 - To indicate that one E164 number and internal number are associated. • 10 - To indicate that a range of ten numbers including the starting E164 and starting internal number are associated. • 100 - To indicate that a range of 100 numbers including the starting E164 and starting internal number are associated. • 1000 - To indicate that a range of 1000 numbers including the starting E164 and starting internal number are associated.
Located At	Indicates the hierarchy of the site where the E164 number range and internal number range association was created.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add an E164 association (N to N DN)

This procedure associates a range of E164 numbers to a range of internal numbers, at a site.

Note:

- You can also perform the association in ranges of 10, 100, and 1000, on a one-to-one basis. These associations create Direct Dial Inward (DDI) associations so that incoming PSTN numbers are routed to internal numbers.
- Only internal numbers or E164 numbers that are not currently associated, are available for association.
- In Automate, the `HcsSipLocalGwAddE164AssociationEVT` event related to SIP Local Gateway is generated

1. In the Admin Portal, go to the **E164 Associations (N to N DN)** list view.
2. Set the hierarchy to the relevant customer.
3. In the **E164 Associations (N to N DN)** list view, click the Plus icon (+) to add a new record. Choose a site.
4. Configure E164 Association (N to N DN). The table describes configuration options:

Field	Description
Range	Mandatory. Choose the range before choosing other settings on this page. Defines the range value for the E164 to DN association. Options are: 1, 10, 100, or 1000 The range value you select maps to the mask value when the association translation pattern is created. For example, when 10 is selected, all E164 numbers and directory numbers that end in 0 are listed. The mask affects all digits 0 to 9, so you can't start the mask on a non zero number. Likewise, when 100 is selected, the E.164 number and DN end in two zeros. This pattern results in a mask of XX. • 1 - To list all E164 numbers and internal numbers • 10 - To list all E164 numbers and internal numbers that end in one zero (0) • 100 - To list all E164 numbers and internal numbers that end in two zeros (00) • 1000 - To list all E164 numbers and internal numbers that end in three zeros (000)
E164 Number	Mandatory. Choose the starting number of the range of E164 numbers. • If the association is performed at customer level, the drop-down only shows E164 numbers that were added at customer level. • If the association is performed at site level, the drop-down contains E164 numbers that were added at either customer or site level provided the country matches the site's country.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
DN Number	Mandatory. Choose the starting internal number. • If the association is performed at customer level, the drop-down only shows internal numbers that were added at customer level. • If the association is performed at site level, the drop-down shows internal numbers that were added at either customer or site level. • You cannot associate internal numbers that begin with the prefix '*' (asterisk) or '#" (hash).
Dial Plan Model Selection	This field displays only when the **Enforce HCS Dialplan Rules** setting in the **Global Settings** is set to *False* Defines the translation pattern template configured in the dial plan modeling tool. The values for the pattern, transform mask, and associated range masking are hard coded in the workflow. +1555 111 5555 (Range 10) = +1555 111 555X Other values, such as partition and CSS) come from this template. The translation pattern must have its description set to display in this drop-down.

4. Save your changes.

   You can view transaction progress and details in the Transaction Logs.

Note:

- When listing the Number Inventory and displaying an internal number, the E164 Number format is as listed in *E164 numbers in the number inventory*.
- A translation pattern (which is the mapping between the E164 range and internal number range) is created on the CUCM. This translation pattern is used to route inbound PSTN calls to their associated internal numbers.
- If the association is performed at a Site, the translation pattern is only added to the CUCM referenced by the site's network device list (NDL).
- If the association is performed at Customer level, the translation pattern is added to all the customer's CUCMs.
- If the Site has one or more SIP Local Gateways associated with it, the `HcsSipLocalGwAddE164AssociationEVT` event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Delete an E164 association (N to N DN)

This procedure deletes one or more E164 (N to N DN) associations to disassociate a range of E164 numbers from a range of internal numbers.

Note: In Automate, the `HcsSipLocalGwDelE164AssociationEVT` event related to SIP Local Gateway is generated as a result.

1. Go to the **E164 Associations (N to N DN)** list view.
2. Change your hierarchy, if required.
3. View E164 Associations (N to N DN) in the list, which displays the following information:

Column	Description
E164 Number	The starting E164 number in the range.
DN Number	The starting DN number in the range.
Range	• 1 - Indicates that one E164 number and internal number are associated • 10 - Indicates that a range of ten numbers including the starting E164 and starting internal number are associated • 100 - Indicates that a range of 100 numbers including the starting E164 and starting internal number are associated • 1000 - Indicates that a range of 1000 numbers including the starting E164 and starting internal numbers are associated
Located At	Indicates the hierarchy of the site where the E164 number range and internal number range association was created.

4. Choose an option:
   - To disassociate multiple ranges, select the check boxes in the far left column of the table for the ranges you want to disassociate.
   - To disassociate one range, click its row in the table. The details about the association appear.
5. Click **Delete**, then click **Yes** to confirm the disassociation.

Note:

- The translation pattern mapping between the E164 range and internal number range is deleted from CUCM.

  The E164 number association with the internal number is removed on the Number Inventory list view display and in any **Lines** drop-down list and **Lines** displays.
- If the site has one or more SIP Local Gateways associated with it, the `HcsSipLocalGwDelE164AssociationEVT` event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Copyright © 2025 VisionOSS Limited. All rights reserved.

7.5.6. E164 associations (N to 1 DN)

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes managing single internal numbers associated with a range of E164 numbers.

View E164 associations (N to 1 DN)

This procedure displays sets of E164 numbers associated with a single internal number (directory number, or DN).

1. Go to the **E164 Associations (N to 1 DN)** list view.
2. On the **E164 Associations (N to 1 DN)** list, view E164 associations (N to 1 DN).

   Note: You can filter the list and change the hierarchy by selecting a link in the **Located At** column.

   The table describes column data in the E164 Associations (N to 1 DN) list view:

Column	Description
DN Number	The associated internal number (directory number).
Located At	The hierarchy of the site where the E164 number range and internal number association was created.

3. Click on a directory number in the list to view its details.

   The page displays read-only details about the E164 Association (N to 1 DN) configuration (the sets of E164 numbers that are associated with the internal number):

DN Number	The number you're viewing.
Primary E164	Displays the E164 number associated to the internal number in the Number Inventory. Other E164s are indicated as [x] showing that there are more associated E164s to this internal number but their details are only available when opening the relevant Number Inventory.

.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add E164 association (N to 1 DN)

This procedure associates multiple E164 numbers (a set of E164 number) to a single internal number, at a site. For example, you could associate a set of E164 numbers for the sales department with an attendant's internal number.

Note:

- You can also perform association in ranges of 10, 100, and 1000, on a one-to-one basis. These associations create Direct Dial Inward (DDI) associations so that incoming PSTN numbers are routed to internal numbers.
- You can optionally specify a primary E164 number to associate with the internal number. This is useful when performing an internal number to E164 translation (for example, when provisioning translation rules for LBO gateways) and the internal number is associated to more than one E164 presentation.
- You can only associate internal numbers or E164 numbers that are not currently associated.
- You can also *modify* a **E164 Associations (N to 1 DN)** association instance and add additional ranges of E164 numbers to a DN. Open the existing, saved association and then add the additional ranges using the plus icon (+) - as described in the steps below.

Prerequisites:

- Enable number management for the customer.

Perform these steps:

1. Go to the **E164 Associations (N to 1 DN)** list view.
2. Choose the site (if required).
3. In the **E164 Associations (N to 1 DN)** list view, click the Plus icon (+) to add a new record.
4. Configure E164 association (N to 1 DN). The table describes configuration options:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
DN Number	Choose an internal number. • If the association is performed at Customer level, the drop-down only shows internal numbers that were added at Customer level. • If the association is performed at Site level, the drop-down shows internal numbers added at either Customer or Site. • You can't associate internal numbers that begin with the prefix '*' (asterisk) or '#" (hash).
E164 Ranges	Click the Plus icon (+) to add one or more sets of E164 numbers. These E164 numbers do not need to be contiguous. For each E164 number you add, choose an E164 range and the E164 number, as follows: • E164 Range Choose an E164 range, either 1, 10, 100, or 1000. The range value you choose maps to the mask value when the association translation pattern is created. For example, choose 10 to list all E164 numbers and internal numbers ending in 0. The mask affects all digits 0 to 9, so you can't start the mask on a non-zero number. When 100 is chosen the E164 number and internal number end in two zeros, resulting in a pattern with a mask of XX. – 1 - to list all E164 numbers – 10 - to list all E164 numbers ending in one zero (0) – 100 - to list all E164 numbers ending in two zeros (00) – 1000 - to list all E164 numbers that end in three zeros (000) This field is mandatory and affects what appears in the E164 Number field.
E164 Number	Mandatory. Choose the starting number of E164 numbers. • If the association is performed at customer level, the drop-down only shows E164 numbers that were added at customer level. • If the association is performed at site level, the drop-down contains E164 numbers that were added at either customer or site level provided the country matches the site's country.
Primary E164	Optional. Fill out the primary E164 number to associate with the internal number. Ensure the E164 number you enter starts with \+ and falls within the range you specified in in **E164 Range**
Dial Plan Model Selection	This field displays only when the **Enforce HCS Dialplan Rules** setting in the **Global Settings** is set to *False* Defines the translation pattern template configured in the dial plan modeling tool. The values for the pattern, transform mask, and associated range masking are hard coded in the workflow. +1555 111 5555 (Range 10) = +1555 111 555X Other values, such as partition and CSS) come from this template. The translation pattern must have its description set to display in this drop-down.

5. Save your changes.

   View transaction progress and details in the Transaction Logs.

   Note:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- When listing the number inventory and displaying an internal number, the E164 number format is as listed in *E164 numbers in the number inventory*.
- One or more translation patterns are created on the CUCM. The translation patterns are the mappings between the set of E164 numbers and the single internal number, and are used to route inbound PSTN calls to their proper internal numbers.

  When you associate a set of E164 numbers to a single internal number, multiple translation patterns are created (each DN-to-E164 range association results in a translation pattern being created on the CUCM).
- If the association is performed at Site level, the translation pattern is only added to the CUCM referenced by the site's network device list (NDL).
- If the association is performed at Customer level, the translation pattern is added to all of the CUCMs that exist for the customer.
- If the site is associated with one or more SIP Local Gateways, the `HcsSipLocalGwAddMultiE164AssociationEVT` event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Delete an E164 associations (N to 1 DN)

This procedure disassociates a set of E164 numbers from an internal number.

Note:

- When disassociating a set of E164 numbers from an internal number, multiple translation patterns are deleted. For each association you delete, a translation pattern is deleted from the CUCM.

  In Automate, the `HcsSipLocalGwDelMultiE164AssociationEVT` event related to SIP Local Gateway is generated as a result.
- If the Local Gateway is set up to override the Voice Translation limit and the **Enable Command Builder** setting is enabled, disassociation will fail if it exceeds the default Voice Translation limit. In this case, first disable the **Enable Command Builder** setting.

1. Go to the **E164 Associations (N to 1 DN)** list view.
2. Change the hierarchy, if required.
3. In the **E164 Associations (N to 1 DN)** list, view the following details:

Column	Description
DN Number	The internal number.
Located At	The hierarchy of the site where the E164 number range and internal number range association was created.

4. Choose an option:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To disassociate multiple associations, click the check box in the far left column of the table, next to the numbers you want to disassociate.
- To disassociate one association, click its row in the table. The details about the association appear.

5. Click **Delete**, then click **Yes** to confirm the disassociation.

Note:

- The translation pattern mapping between the E164 set and the internal number is deleted from the CUCM.

  The E164 number association with the internal number is removed from the **Number Inventory** list view, and from any **Lines** drop-downs and **Lines** displays.
- If the site is associated with one or more SIP Local Gateways, the `HcsSipLocalGwDelMultiE164AssociationEVT` event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

7.5.7. Migrate translation patterns for E164 to internal number associations

This procedure migrates existing translation patterns for E164 to internal number associations, if you manually configured translation patterns in the E164 lookup partition to associate E164 numbers to internal numbers for Direct Dial Inward (DDI) routing.

Note: It is recommended that you migrate your existing translation patterns to use E164-to-Internal number (DN) association.

Perform this procedure only once. If you did this migrate when upgrading to VOSS Automate, there is no need to migrate again when upgrading to a later VOSS Automate release.

To migrate translation patterns:

1. Log in as provider, reseller, or customer administrator.
2. Add the appropriate E164 number inventory. See *Add an inventory of E164 numbers*.
3. View the E164 number inventory. See *View an E164 inventory and delete E164 numbers*.
4. To verify that the selected directory number (DN) inventory is available for association, go to the **Number Inventory**.
5. Remove the translation patterns you added previously, via the **Translation Patterns** page.
6. Create the appropriate E164-to-DN associations, via the **E164 Associations (N to N DN)** page. See *E164 associations (N to N DN)*. These associations restore the appropriate translation patterns in the E164 Lookup partition for the selected customer.
7. View the new translation pattern, via the **Translation Patterns** page.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- CUCM Translation Patterns in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8. Users & Services

8.1. Microsoft User Services

8.1.1. Move a Microsoft user between sites using offboard and onboard

Tip: *Use the Action search to navigate Automate*

To move a user between sites in Automate, the recommended approach is to offboard the user from a voice perspective, then onboard the user in the new site. Moving the user in this way allows the user to be assigned a new number and updated policies, for example, *emergency*, from the new site.

To move a user between sites:

1. Run *Offboard User* for the user that needs to be moved.
   - The user's existing voice configuration is removed, and if configured, their licenses are left in place. Other services aren't impacted.
   - The user and their related services are moved back to the customer level, ready to be onboarded in the new site.
2. Onboard the user into the new site, using your typical process - for example, *Microsoft Quick User*.

   The user is moved to the new site with the correct voice services for the new site.

Note: You can follow this workflow even if the user is going to be keeping the same number. If the number sits at a level available to the new site (for example, customer or intermediate node), then no additional step is required.

If the number sits in the inventory in the old site (the site the user is moved from), you'll need to move the number in the inventory to either a shared level, such as *customer*, or to the new site, before running the onboarding step above.

Related topics

- *Prevent duplicate numbers*
- *Offboarding (Microsoft)*
- *Offboard user (Webex or Microsoft)*
- *Onboard user (Microsoft)*
- *Microsoft - Move user & services*

8.1.2. Quick Actions (Microsoft)

Multi vendor users

Tip: *Use the Action search to navigate Automate*

Overview

Automate supports multi vendor users, which allows you to provision and manage services from one or more vendors on the Automate platform. For example, to use both Microsoft meeting and collaboration tools and Cisco tools.

Single vendor and multi vendor users

Automate supports provisioning for a number of categories of user, representing either a single or multi vendor deployment:

Single or Multi Vendor	Description
Single vendor user	Users services from a single vendor, for example, either all Cisco services, or all Microsoft services.
Multi vendor user	Users using services from two or more vendors.
Multi vendor hybrid user	Users using services from two or more vendors, with services configured for integration, for example, with dial plans and routing.

Related topics

- Enable multi vendor users in the Core Feature Guide
- Global Settings
- Role-based access for multi vendor users in the Core Feature Guide
- Entitlement in the Core Feature Guide
- View users in the Core Feature Guide
- *User calling settings*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *Microsoft Exchange*
- *User voice mail settings*
- *Access profile permissions and operations*
- *Reserve numbers for a user*

View and manage multi vendor users

This procedure displays and updates multi vendor users.

Note: On a multi vendor user's configuration details page, you can also manage the user via any quick actions available on the page, but note the following:

- Quick Actions for multi vendor user are defined via the Multi Vendor FDP (`MultiVendorFDP`) in the field display policy (FDP) for the page. See *Enable multi vendor users*.
- For details around the available quick actions for multi vendor user, the user type they apply to, and the impact of changes via the Quick Actions, see:
  - *Configure quick actions for multi vendor users*
  - *Quick actions for multi vendor user*

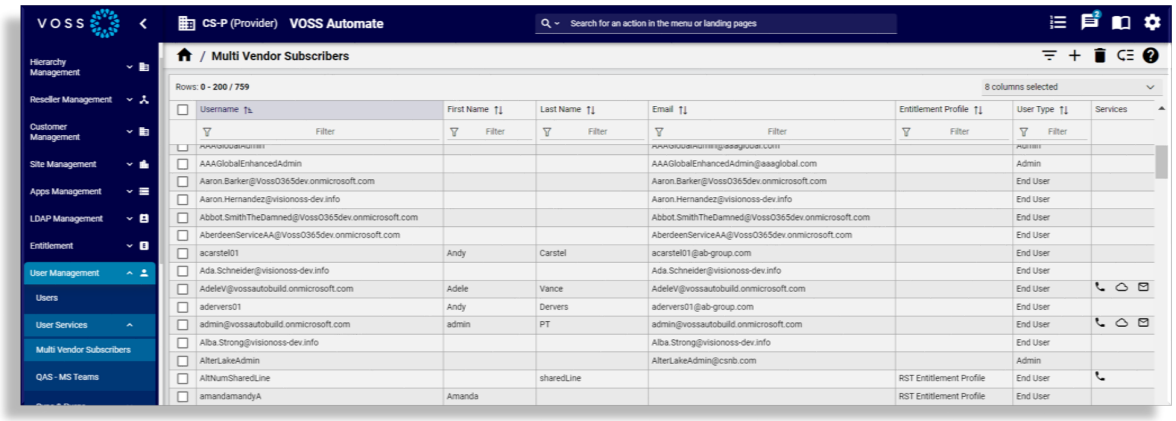
---

1. In the Admin Portal, go to **Manage Users**.

   Note: This list view makes use of an `[OR]` condition to filter users: `End User[OR]End User + Admin`

   For details on the filter, see: *Working with lists*.

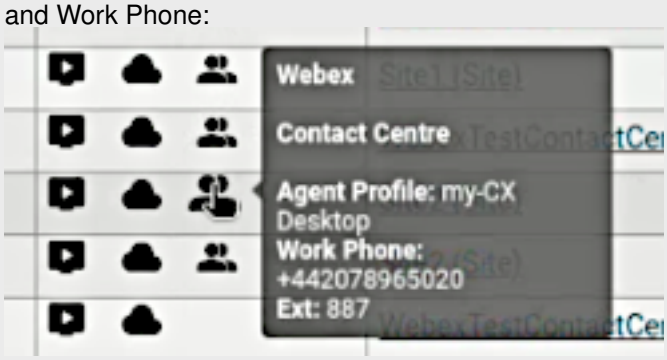
2. View the summary list of the multi vendor users.



The table describes a few caveats around icons in the **Services** column of the list view:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Users with Microsoft services	• The Voice icon (phone) displays only when the user has a feature type of *PhoneSystem* enabled, which means that they're licensed for the voice service in Microsoft Entra. • The Collaboration icon (cloud) displays only when the user has a feature type of *Teams* enabled, which means that they're licensed for Microsoft Teams IM/collaboration in Microsoft Entra. • The **Feature type** field displays read-only values in *Quick Add User*. • Clicking the **MS Exchange** icon (envelope) opens `device/msexchangeonline/UserMailbox` (the user's Microsoft Exchange mailbox settings). • The Microsoft Voicemail icon displays when the user has the Microsoft voicemail service enabled. You can manage the user's voicemail settings from within Automate or on the Microsoft online portal. Changes are immediately and automatically synced between Automate and the Microsoft online portal. Click on the icon to open the voicemail settings. You can also edit these settings from the Microsoft Voicemail Settings card on the multi vendor user's management page.

Users with Webex App	Included icons may be for collaboration, conferencing, voice, and/or voicemail, contact center agent, provided the user has the required license. For example: • The Conferencing icon (monitor) displays when the user has a license where the name of the license (the pattern) contains the text "meeting" (for example, "Meeting 25"). • The Collaboration icon (cloud) displays when the user has a license where the name of the license (the pattern) contains the text "messag" (for example, "Messaging"). • The 2 People icon displays when the user is a Contact Center agent. Additional details are provided when hovering over the icon, e.g. Agent Profile, Multimedia Profile, Skill Profile and Work Phone: 
Headset and phone	A headset icon displays in the **Services** column for users that have a headset connected to an associated phone.

Copyright © 2025 VisionOSS Limited. All rights reserved.

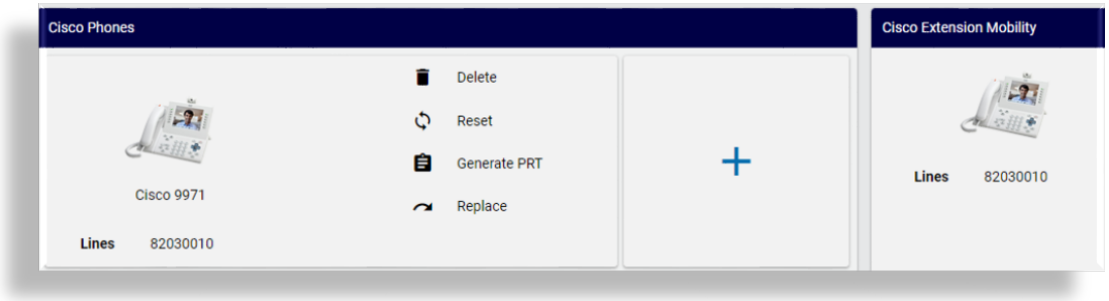
3. Manage multi vendor users from the list view. For example, you can:
   - Filter the list
   - Add a new multi vendor user
   - Move multi vendor users (one or more)
   - Delete multi vendor users (one or more)

   Note: For all multi vendor users you delete from the list view, their services are also deleted, and, if applicable, their hybrid status is updated. Additionally, when deleting Microsoft multi vendor users, they are also off-boarded (that is, their licenses are removed).

   The Automate user is retained only for LDAP or MS365 users.

4. To view or update the settings of a selected multi vendor user, click on the user in the list view to open their configuration details page. Here you can:
   - Choose an entitlement profile
   - View and manage phones and lines

   Note: For users with associated softphones, the phone product model name displays below the Phone icon on the cards. This is useful where the user has multiple phones and you need to easily distinguish between different phone models.



   - Delete the multi vendor user.

   Note: When deleting a multi vendor user:
   - If applicable, the user's hybrid status is updated
   - Non-Microsoft multi vendor user - deletes the user along with their services
   - Microsoft multi vendor user - deletes the user along with their services, and offboards the user (removes their license)
   - Bottom-up LDAP multi vendor user - `device/cucm/User` and `data/User` is deleted
   - LDAP or MS365 users - the Automate user is retained:
     * Top-down LDAP user - deletes the user, and retains the `data/User` and `device/ldap` user instances are
     * Microsoft provisioned user - `data/User` is retained if there is an associated Microsoft user

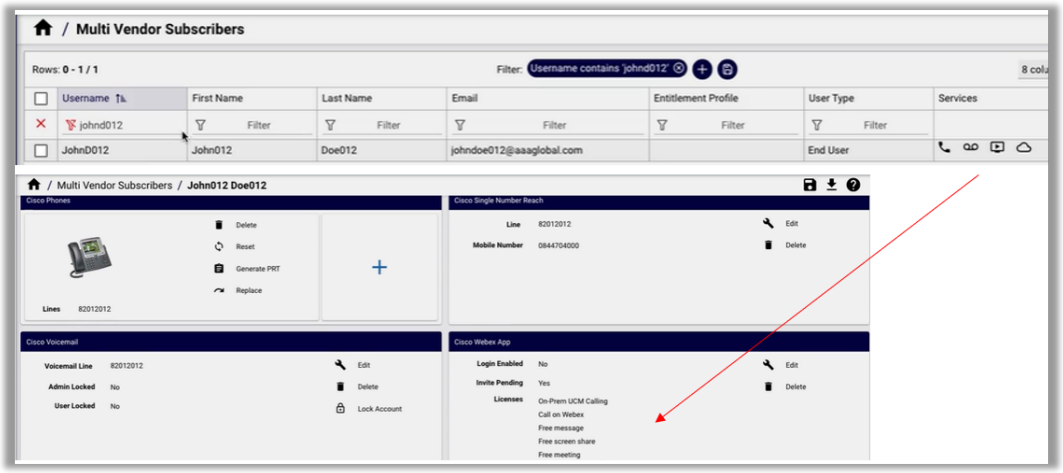
Copyright © 2025 VisionOSS Limited. All rights reserved.

- View and manage existing, available services, which may include Microsoft user calling settings, Microsoft voicemail settings, Microsoft Teams, Cisco Webex, Cisco Voicemail, and other enabled services.

Note:

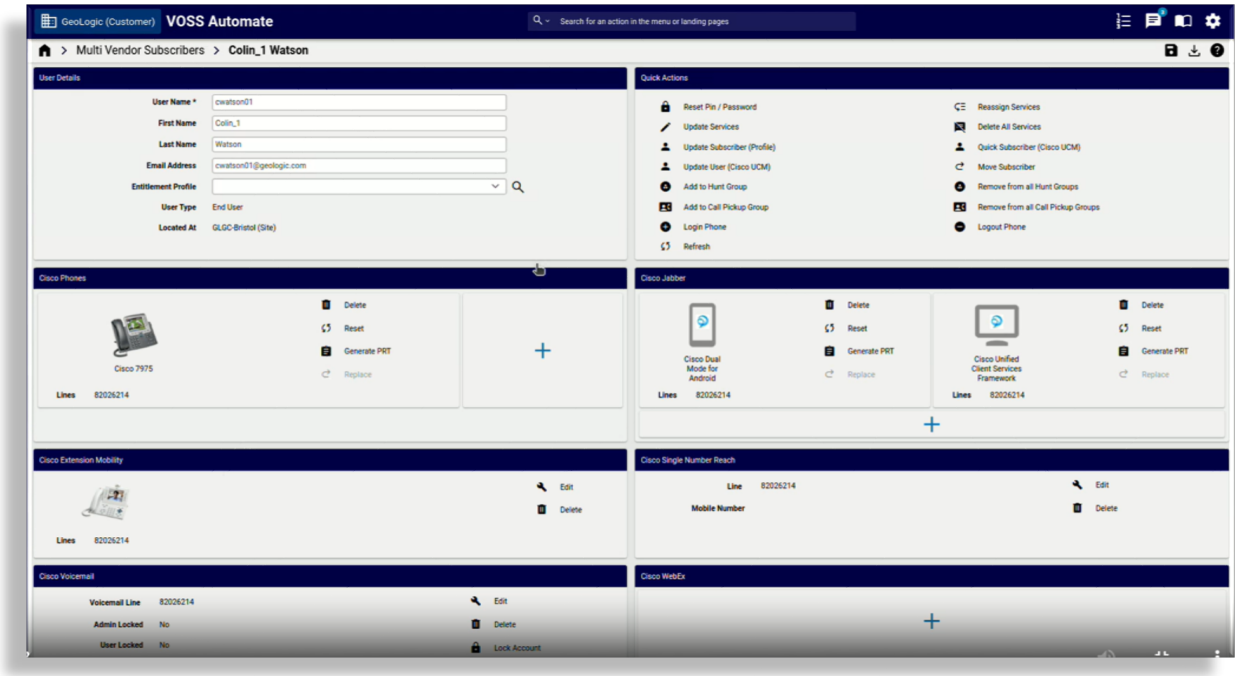
- For users with multiple remote destinations associated to their single number reach (SNR), the Cisco Single Number Reach card on the management page displays only the *first* associated SNR remote destination profile and the *first* associated remote destination to that SNR.
- For users licensed with a Webex Calling Professional license, the following cards also display on their User Details view:
  - **Webex Devices**: for devices available to the user
  - **Webex Voicemail**: if the Voicemail setting is enabled, options for sendAllCalls, sendBusyCalls, sendUnansweredCalls, edit link to Voicemail.
  - **Webex Calling Settings**: Barge In, Caller ID, Call Forward, Call Recording, Call Waiting, Intercept, edit link to Calling Settings.

  The image shows users with Webex App, and how they show up in the the list view and on their configuration details page:



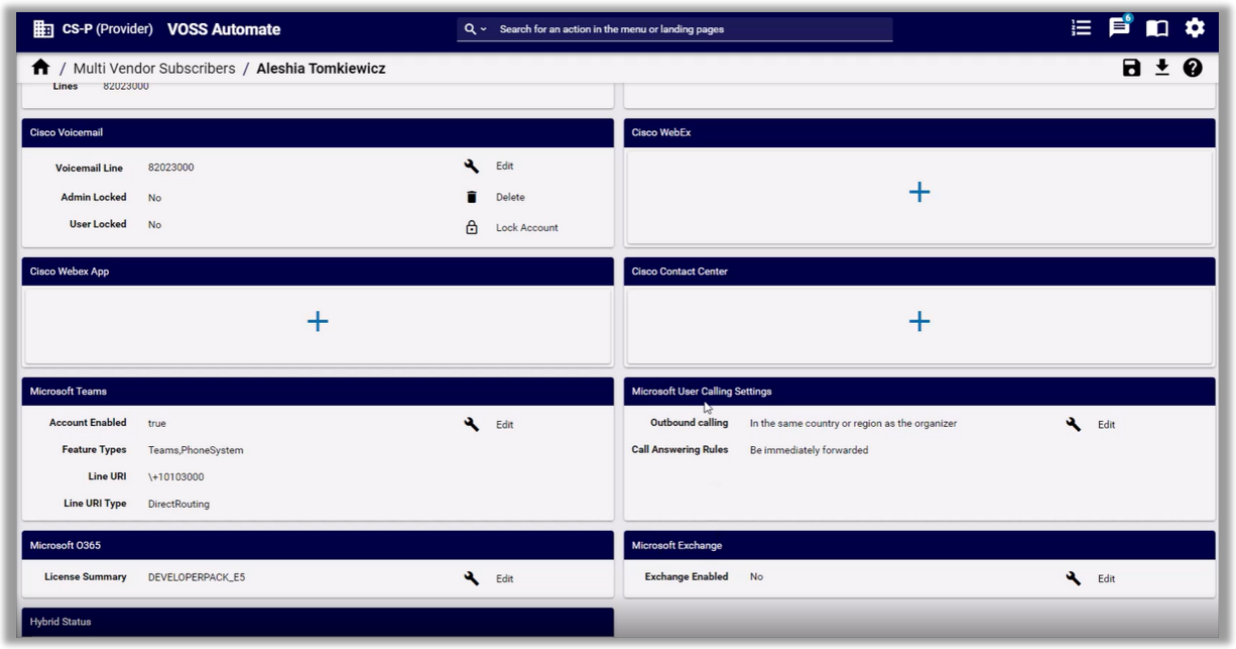
Copyright © 2025 VisionOSS Limited. All rights reserved.

Example: Multi vendor user with Cisco services

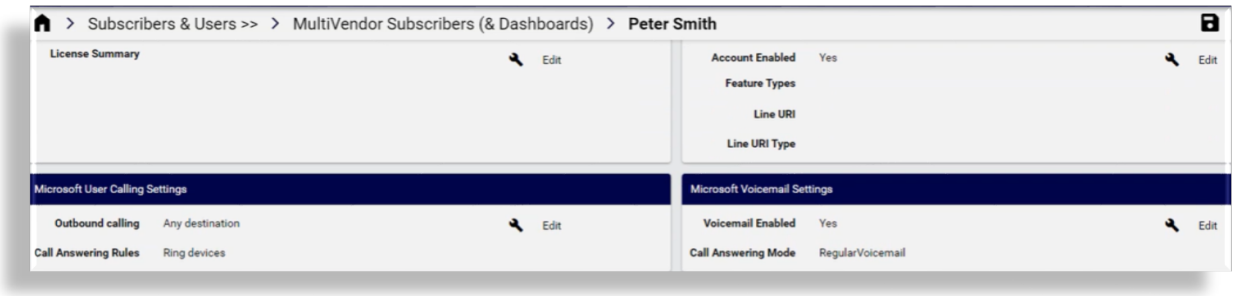


Example: Multi vendor user with Microsoft Teams

Copyright © 2025 VisionOSS Limited. All rights reserved.

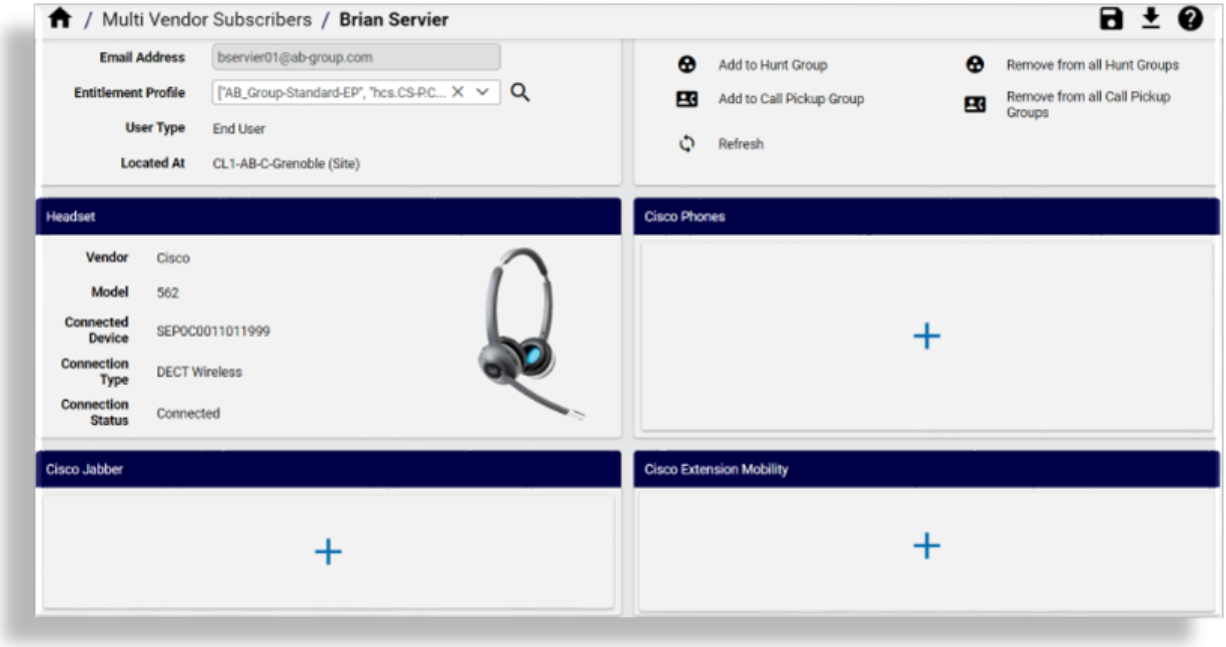


Example: Multi vendor user's user calling and voicemail settings



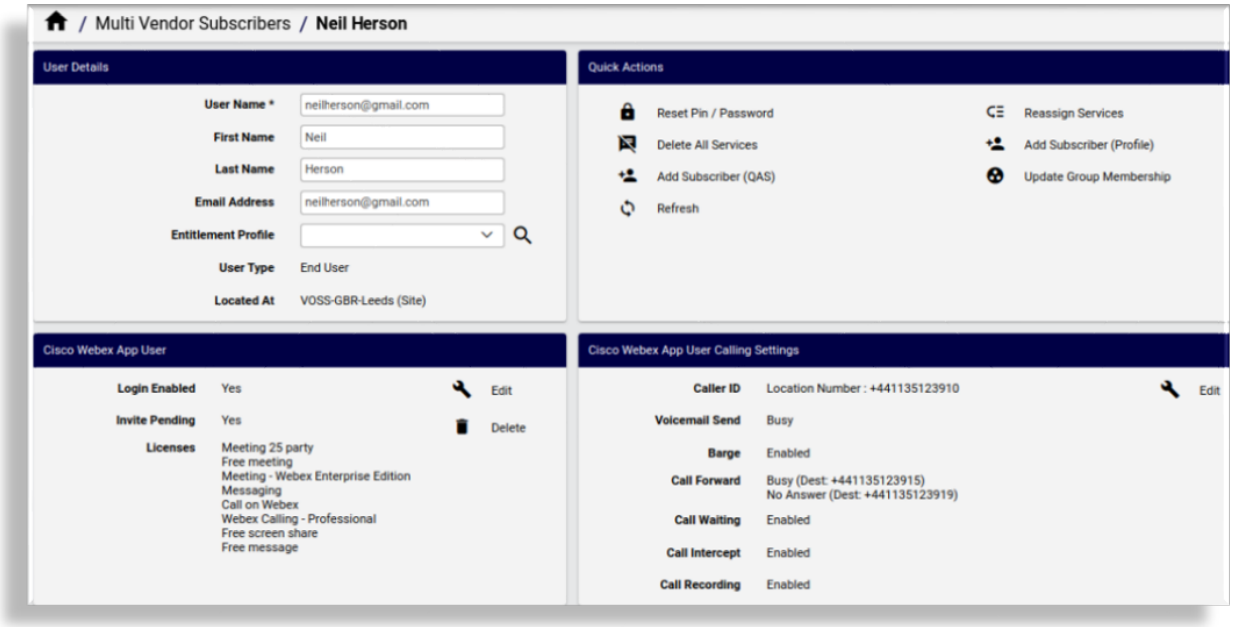
Copyright © 2025 VisionOSS Limited. All rights reserved.

Example: Multi vendor user's headset settings



Example: Multi vendor user - Cisco Webex App User with Webex Calling Professional license, showing Cisco Webex App User Calling Settings

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related Topics

- *Single number reach*
- *Voicemail*
- *User calling settings* (Microsoft users).
- *Configure quick actions for multi vendor users*

Merge two users into a single multi vendor user

Automate provides a merge tool for consolidating duplicate user accounts from two different vendors (two `data/User` instances with the same email address) that have been imported from different vendors, into a single, Cisco-Microsoft multi vendor user.

This case is required where you have imported two user accounts from different vendors, for example, Cisco and Microsoft, and you add or update their email addresses to the same email address. In this case, the merge tool workflow (`Merge_Relation_User workflow`) is triggered when it finds the duplicate email address for the two `data/User` instances.

You can use the view for the merge tool (`view/ConsolidateUsers`) to define the primary user (which is retained once merged), and the secondary user (which is deleted once merged). The services of the secondary user will then be merged into the primary user.

When consolidating these two accounts, the default provisioning workflow of the merge tool (`ConsolidateUsers`) copies details of the secondary user into the primary user, and moves any device models associated with the secondary user to the hierarchy of the primary user:

- Copies the username (Cisco or Microsoft) of the secondary user to the primary user
- Copies the Zoom username of the secondary user to the primary user

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Copies the email address of the secondary user to the primary user
- Copies the email address to the Cisco user, if the primary Cisco UCM user is local
- Deletes the secondary user (the `data/User` instance of the secondary user

Once successfully merged, a log entry is added to `data/HcsUserManagementLogDAT`, and the primary user is assigned a system username, as a multi vendor user.

Note:

- The secondary user cannot be a UCM user (Cisco user) as it cannot be deleted. Only secondary users that match the primary user can be merged.
- The secondary user cannot be configured as a hybrid user - remove this setting before merging users.
- The merge tool does not allow consolidation of the user accounts if both the primary and secondary user accounts are UCM users.

Quick actions for multi vendor user

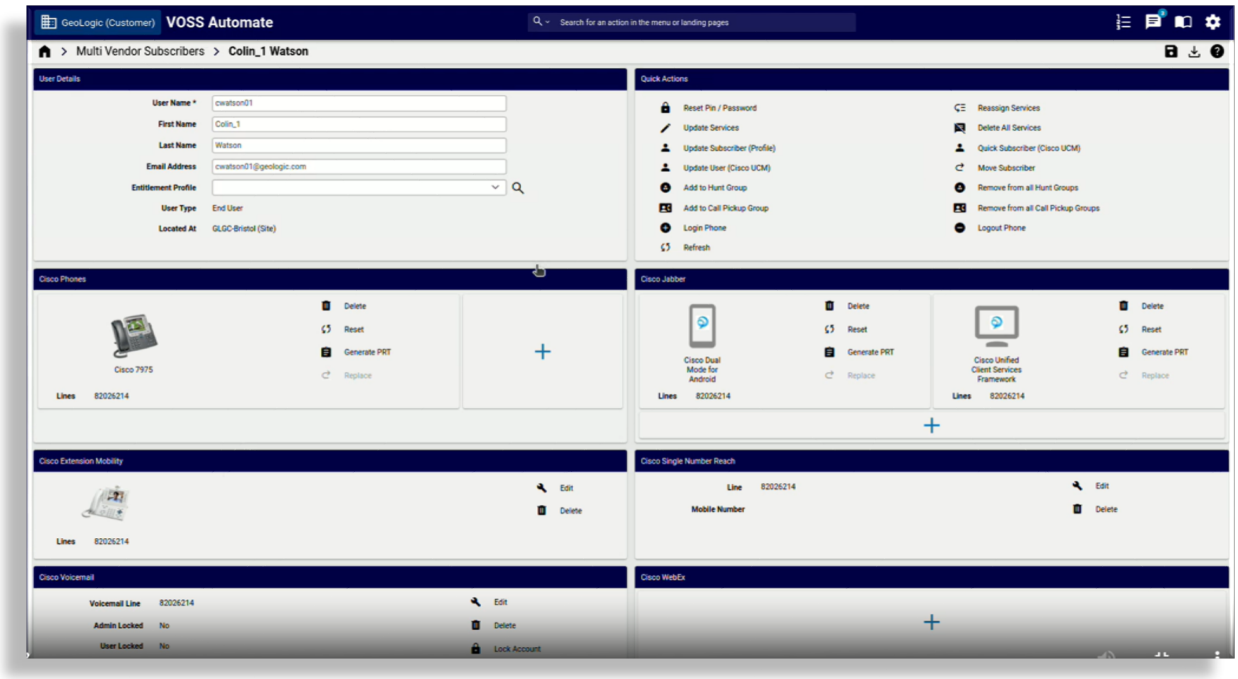
Quick actions allow you to easily access frequently used activities, for example, to reset a PIN or password, or to add a user. Multi vendor user includes a set of quick actions that are configured via the multi vendor user field display policy (`MultiVendorFDP`; fallback FDP is `default`).

Quick actions added to the `MultiVendorFDP` field display policy (FDP) appear as links on the **Quick Actions** card on the management page of the selected multi vendor user.

While some quick actions are also available as stand-alone features or functionality that can be accessed via a menu or dashboard link (or via the Search bar), other quick actions, such as *Update User (Cisco UCM)*, are only available as a quick action.

The availability of a quick action also depends on the user type or the environment, for example, Cisco or Microsoft, multi vendor or hybrid. You'll also require appropriate permissions on your access profile to have some quick actions available to you. By default, the access profiles that ship with the system (except for Operator access profiles) have *read*, *write*, and *export* permissions on all multi vendor user quick actions and service card actions that are views, for example, `view/DeleteCucmHuntGroupAllMembers` (quick action, *Remove from all Hunt Groups*), `view/DeleteSubscriberService` (quick action *Delete all services*), or `view/AddExtensionMobility` (service card action, *Add Extension Mobility*).

Copyright © 2025 VisionOSS Limited. All rights reserved.



Quick action links trigger the following behavior in the system:

- Some quick actions, such as *Update User (Cisco UCM)*, are only available as a quick action link that launches a dialog (or overlay) on the current page, and allows you to perform a specific action (related to the quick action).
- Some quick actions are shortcuts to a menu or dashboard for the feature, such as the *Cisco Quick User* or *Microsoft Quick User* link, which opens the *Quick Add User* page directly from the quick link.
- In some cases, the quick action launches a dialog (or overlay) on the current page for performing a specific action related to the quick action, such as *Add to Hunt Group* or *Remove from All Hunt Groups*, while the full functionality for the feature is *also* available via a menu or dashboard.

  In this case, you may also access the functionality via the menu (or fill out the feature name, for example, *Hunt Groups*, in the Admin Portal Search bar, and press Enter to locate the page).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Access profile permissions and operations*

Quick actions (all users)

The table describes quick actions that support all users:

Quick Action	Description
Refresh	• Available to admin users with an access profile that has *read* permissions on the `relation/User` model • Performs a live refresh (non-cached GET request) of device models for all services from external devices, including (where applicable), Cisco user and services, Pexip, UCCX, Webex App user and config, and Microsoft user and services.
Delete all Services	• Available to users with an access profile with read-write permissions on `view/DeleteSubscriberService` • Removes all the selected user's services. For Cisco UCM, services are deleted/disassociated. For Microsoft users, their licenses are also removed and they're off-boarded. • Click on the warning to confirm (Yes/No) whether to delete all services

Note: You can find more information about Automate's caching policies in *Default Cache Control Policy* in the Core Feature Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick actions (Cisco and Microsoft)

The table describes quick actions that support Cisco UCM and Microsoft:

Quick Action	Description
Update User (Profile)	• Multi vendor environment (Cisco UCM/Microsoft/Webex users) • Launches the **Onboard user** page, with the username populated based on the selected user. • The multi vendor user FDP should include the `qa_update_subscriber_from_profile` quick action. • The administrator access profile should have read-write permissions for `view/AddSubscriberFromProfile`. • Cisco UCM or Microsoft Tenant should be provisioned at the necessary hierarchy level (above or at the user's hierarchy).

Quick actions (Cisco UCM)

The table describes quick actions that support Cisco UCM:

Quick Action	Description
Quick Add User (Cisco UCM)	• Launches **Cisco Quick User**, with the username auto-populated for the selected user. • Cisco UCM should be provisioned at the necessary hierarchy level (above or at the user's hierarchy level). • The multi vendor user FDP should include the `qa_cucm_qas` quick action. • The administrator access profile should have read-write permissions for `view/QuickSubscriber`.

Update User (Cisco UCM)	• Launches the *Update User (Cisco UCM)* form, where you can:
	  – Enable IM and Presence
	  – Update the selected line as the IPCC extension to use when the user is also a contact centre agent
	  – Add or update Conference Now (ad hoc) via Cisco UCM, assign a meeting number, and create an access code
	  – Update the service profile
	• The user you're updating must be an existing Cisco user (`device/cucm/User`).
	• The multi vendor user FDP should include the `qa_update_cisco_user` quick action.
	• The administrator access profile should have the necessary read-write permissions for `view/MVS_Cisco_User`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick Action	Description
Move User	• Cisco users only, Microsoft users only, or hybrid Cisco-Microsoft environment • For Cisco users with UCCX agent settings, it is necessary to re-subscribe the user as an agent at the target site and ensure that the associated Team is updated manually. • For Microsoft users, MS Teams users are also moved. • The quick link opens the **Move User** feature • Access to the Move User feature is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/MultiVendorServiceUserMove_VIEW`
Add to Hunt Group	• Cisco users (Cisco only, or hybrid environment) • Access to the Hunt Groups feature is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/AddCucmHuntGroupMember`

Quick Action	Description
Remove from all Hunt Groups	• Cisco users (Cisco only, or hybrid environment) • Access to the Hunt Groups feature is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/DeleteCucmHuntGroupAllMembers`
Add to Call Pickup Group	• Cisco users (Cisco only, or hybrid environment) • Launches a dialog where you can choose the line and the call pickup group • Access to the Call Pickup Groups feature is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/AddCucmCallPickupGroupMember`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick Action	Description
Remove from all Call Pickup Groups	• Cisco users (Cisco only, or hybrid environment) • Triggers a warning on the user's page, asking you to confirm (Yes/No) whether to remove the user from all call pickup groups • Access to the Call Pickup Groups feature is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/DeleteCucmCallPickupGroupAllMembers`
Login Phone	• Cisco users (Cisco only, or hybrid environment) • Access to the EM Login feature is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/EmLoginUse`
Logout Phone	• Cisco users (Cisco only, or hybrid environment) • Access to the feature (EM Logout) is also available from a menu/dashboard • Your access profile requires read-create permissions on `view/EmLogoutUserFromPhones`
Reset PIN/Password	• Cisco users, depending on the user type and their services • Microsoft users, only the Automate password is relevant, and only for admins • Launches a dialog specific to the quick action on the page • Your access profile requires read-create permissions on `view/ResetUCPasswordPinVIEW`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick Action	Description
Update Services	• Users with a Cisco UCM user provisioned, in linked or standard sites. • Opens the **Update Services** page, where you can reconfigure a user's provisioned services and their settings, including description fields, labels, display names, E164 masks, INI settings, and Jabber device names. • Your access profile requires read-create permissions on `view/ReassignServicesUpdateVIEW`
Reassign Services	• Users with a Cisco UCM user provisioned • A MACD function that allows you to efficiently assign the services, device profiles, lines, Jabber clients, entitlement profile, and E164 masks settings of an existing user to a different user. The internal number inventory (INI) description field is also updated with the name of the new user. This functionality makes it easier to move an existing staff member's services, desk phone, and telephone numbers to a new staff member, while creating a new voicemail box. • Your access profile requires read-create permissions on `view/ReassignServicesVIEW`

Quick actions (Microsoft)

The table describes quick actions that support Microsoft:

Quick Action	Description
Quick Add User (MS)	• Launches **Quick Add User**, with the username auto-populated for the selected user. • Microsoft Tenant provisioned should be provisioned at the necessary hierarchy level (above or at the user's hierarchy). The multi vendor user FDP should include the `qa_ms_qas` quick action. • Your access profile must have read-create permissions for `view/MicrosoftSubscriberQas`.
Update Group Membership	• Microsoft users (Microsoft only, or hybrid environment) • Launches a dialog that lists the MS 365 groups that you can assign to or remove from association with a user. If the MS 365 group you're assigning or removing has licenses assigned, the licenses are also applied or removed. • Your access profile must have read-create permissions for `view/MsGraphManageGroup`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick Action	Description
Microsoft Exchange	• Microsoft users (Microsoft only, or hybrid environment) • Launches a dialog that opens `device/msexchangeonline/UserMailbox` to allow editing of the MS user mailbox.

Related topics

- *Manage group membership* in the Core Feature Guide
- *Microsoft Exchange*

Quick actions (Webex)

The table describes quick actions that support Webex:

Quick Action	Description
Quick Add User (Webex)	• Launches Quick Add User (`view/WebexTeamsSubscriberQas` model) with the username populated for the selected Cisco Webex App user. If you're not at a site, you'll need to choose the relevant site. • Links to the `view/WebexTeamsSubscriberQas` model. • Your access profile must have read-create permissions for `view/WebexTeamsSubscriberQas`. • Webex App should be provisioned at the selected site hierarchy or above. • The multi vendor user FDP should include the `qa_webex_qas` quick action.

Related topics

- *Configure quick actions for multi vendor users*
- *Menu layouts*
- *Reset UC Passwords*
- *Introduction to Automate dashboards*
- *Field display policies*
- *Cisco Quick User*
- *Hunt groups*
- *Update Cisco user via quick actions*
- *Call Pickup Groups*
- *Extension mobility*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *EM Login/Logout*
- *Move user*
- *Manage group membership* in the Core Feature Guide
- *Webex Quick User*

Configure quick actions for multi vendor users

This procedure configures the quick actions that display on the Quick Actions card when viewing a multi vendor user.

To configure the quick actions that display on the card:

1. In the Admin Portal, go to **Field Display Policies**.
2. In the list view, search for and click on the default multi vendor user field display policy (`MultiVendorFDP`).
3. Clone the FDP, then edit the clone for your requirements:
   - Fill out a name and a description for the FDP.
   - Leave the target model type as `relation/MultiVendorSubscriber`.
   - For **Display Groups As**, choose whether the default display is panels, tabs, or field sets.
   - Click the down arrow at **Quick Actions**, then configure the fields to display:

     Note: Leave the **Quick Actions** card in its default position at the top of the dashboard.

     See *Enable multi vendor users*

     - Add fields to the card by selecting and moving fields from **Available** to **Selected**.
     - Remove fields by selecting and moving fields from **Selected** to **Available**.

     Important: You must select valid fields for the model (allowed services), which in this case is `relation/MultiVendorSubscriber`.

     Only valid fields will display on the service cards once you apply the FDP. For multi vendor user, valid field names are prefixed `mvs_user_qa`, where:

     - `mvs` is the alias for *multi vendor user**
     - `_qa` is *Quick Action*

     If a service or action is disallowed in the global settings or in the entitlement profile, or if required servers are not installed for the service, the system verification check does not allow display of the service or action on the User Management dashboard (defined via the FDP), and the user can't be provisioned with this service.

4. Click **Save**.

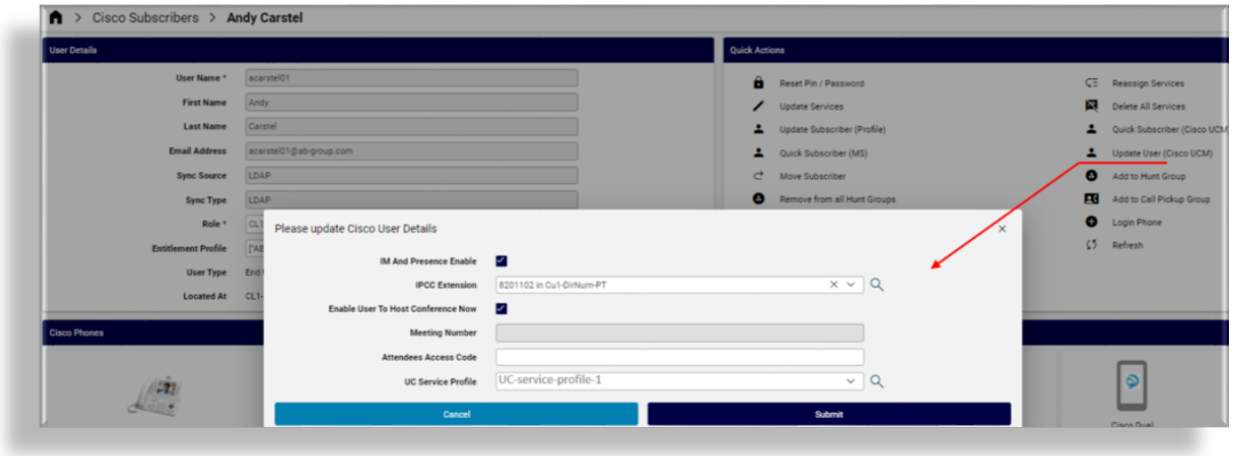
   The next time you view the Quick Actions for a selected multi vendor user, you'll be able to use the quick action to update the user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Update Cisco user via quick actions

This feature allows you to enable or disable IM and Presence, to choose the IPCC extension, to define whether the user has permissions to host a conference, and to assign a UC service profile.

Note: Conference Now is a Cisco Call Manager Ad Hoc conference service, available only to Cisco users. See the Cisco Unified Communications Manager documentation for more information about Conference Now.



Note:

- The *Update User (Cisco UCM)* quick action is only available for Cisco users who are also multi vendor users, via the **Quick Actions** card on the **Multi Vendor Users** editing form.
- The field for this quick action (*mvs_user_qa.qa_update_cisco_user*) must be added to the Multi Vendor Users's field display policy (`MultiVendorFDP`), in the **Quick Actions** card, via the **Field Display Policies** page.

To update a Cisco user for IM and Presence and/or Conference Now:

1. In the Admin Portal, go to **Multi Vendor Users**.
2. Click on the relevant user.
3. In the **Quick Actions**, click **Update User (Cisco UCM)** to open the dialog, then update the Cisco user:
   - To enable IM and Presence, select **IM and Presence Enable**.
   - Select the IPCC extension from the drop-down.

     Note: The **IPCC Extension** drop-down lists the line/route partitions associated with this user.

   - To enable Conference Now, select **Enable User to Host Conference Now**. When enabling Conference Now:
     - The meeting number displays in the read-only **Meeting Number** field.
     - You can fill out an access code in the **Attendees Access Code** field.
   - Optionally, you can also assign a UC service profile via the drop-down.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. Click **Submit**.

Microsoft Quick User

Tip: *Use the Action search to navigate Automate*

This procedure displays and updates a Microsoft user, and moves the user to the correct site, with all configuration and licensing applied.

Note: Quick User simplifies onboarding with the use of Quick Add Groups (QAGs). QAGs are service and policy assignment templates that allow you to pre-configure how calling rights, policies, and services are assigned to users based on their user role.

When updating a user via Quick Add User, you select the relevant QAG, and the automated workflows in Automate handles the required cloud sync and licensing. The workflow also removes the need for an administrator to check the licensing, or to flag the required policies and settings individually, and then to wait for the cloud to sync in.

Prerequisites:

- Sync in the Microsoft Teams user to the customer level
- Set up the site defaults and QAG with the appropriate configuration and licenses.

Perform these steps:

1. Log in to the Admin Portal as a Provider admin, at the customer level.
2. Go to **Microsoft Quick User**.
3. Choose the relevant site.
4. On the **Microsoft Quick User** page:
   - Mandatory. At **Username**, select the user to populate fields on the page.

     Note: This workflow is intended for Microsoft-only users. When choosing a hybrid user with Cisco-Microsoft services, you'll need to work with this user via the Hybrid multi vendor actions. The **Hybrid Status Message** field displays the user's hybrid status. See *Hybrid Cisco-Microsoft management*

   - To include users higher in the hierarchy in the **Username** drop-down, select **Include users at higher hierarchy**.
   - To send a user a welcome email once they're set up, select **Send welcome email**.

     Note:

     – You must have a SMTP server set up to send emails.

     – The read-only **User status** field displays the user's current status; that is, whether they are online, in staging, or not yet provisioned.

     – The value in the read-only **Feature type** field defines whether this Microsoft user has MS Teams with or without the voice service. The user has MS Teams and voice service when feature type displays both *Teams* and *PhoneSystem*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Mandatory. From the **Quick Add Group** drop-down, select the relevant Quick Add Group (QAG) (licenses the user and applies settings defined in the QAG).

  The list of available Quick Add Groups are filtered by vendor (see *Quick Add Groups and vendor filtering*), and are restricted to those available at a selected hierarchy, based on the option selected for **Quick Add Group & User Profile lookup level** in the General Settings of the Global Settings. See *Global settings*.

  Quick Add Groups support group licensing for MS 365 groups, so that users can be licensed according to group membership. Refer to:

  – *Microsoft Licenses* in the Core Feature Guide

  – *Quick Add Groups*

  Note:

  – If **Enable Microsoft User License Enforcement** has been set to **Yes** in the **Global Settings**, a user can only be added if the license allocation limit for the user's hierarchy is not exceeded. For details, see *Microsoft license management and alerting* in the Core Feature Guide.

  – If an existing user is holding a particular license is assigned a Quick Add Group where the group license provides additional services (for example, from existing IM services only to Voice services), the user license is updated as follows:

    * The user is either placed in the staging queue until the license update is synced and then provisioned with services; or

    * The user is provisioned without a staging process

    The tenant staging schedule sync for Microsoft Teams is disabled by default on install. You can enable the sync schedule and update its execution schedule.

  – If **Tenant dial plan**, **Calling line identity** and **Online voice routing policy** values are set, these will be used.

- From the **Line URI** drop-down, choose a number; alternatively, select **Use next available line** to automatically populate the **Line URI** field with the next available line.

  Note:

  – If filtering is enabled at the current hierarchy you can select a line filter, then select a line from the filtered subset of lines returned by the filter. For details, see *Manage number filters*.

  – The **Line URI** and **Use next available line** fields display *only* when **Feature Type** is *PhoneSystem*, or **Manage Licenses** is enabled (via the **MS Teams** tab in the site default docs).

  – The **Line URI** drop-down displays available lines (staged lines and lines reserved for other users are excluded), with the vendor and line type shown in brackets, for example, *Microsoft - CallingPlan*. Lines types may be: Direct Routing, Calling Plan, or Operator Connect

  – When choosing a line, the INI will eventually update to this number.

  – By default, **Use next available line** is disabled. When enabled, the system prioritizes local numbers, numbers available at the current site, before checking for available numbers from higher levels in the hierarchy. Additionally,

    * When used with a filter, the system selects the first available line returned from the filter.

Copyright © 2025 VisionOSS Limited. All rights reserved.

    * A user without a line is assigned the next available line.
    * If the user has an existing line, this line is replaced by the next available line.
    * Staged numbers are considered unavailable and won't be used.
    * Reserved numbers are excluded (numbers reserved for the user you're working with and numbers reserved for other users). See *Reserve numbers for a user*

  – **Enterprise Voice Enabled** is deprecated since PowerShell V4.0.0, so setting a value for this option is no longer required. Thus, to enable a licensed user for Enterprise Voice in Quick Add User, assign a line (choose a number from **Line URI**) and ensure that the **Feature Type** field displays value `Teams, PhoneSystem`. Alternatively, choose a Quick Add Group that has a configuration template set up to enable Enterprise Voice for licensed users, regardless of whether a line is assigned.

    To disable Enterprise Voice for this user (or to enable it again in future), this is done via the user's account settings (`relation/MicrosoftSubscriber`). See *Microsoft users*

- If a **Quick Add Group** is selected and related values are set, the **Tenant dial plan**, **Calling line identity** and **Online voice routing policy** fields, will take those values, else values from the site defaults (SDD).

  Choosing different values will overwrite QAG or site defaults (SDD) values.

- From **Calling Line Identity**, assign a calling line identity for this user, or use the value that comes from the QAG.
- Click **Save**.

5. Go to **User Staging** to view the user in the staging queue.

Note: The user is placed in the staging queue (with all configuration applied) while waiting for the cloud to sync in. Once the licensed user appears in the Microsoft Teams portal, a second, targeted sync is triggered (if the schedule is enabled), which searches only for staged users (not all users from the tenant). Once the sync completes, the user becomes fully provisioned and the number is flagged as used.

The user receives a welcome email (if you've chosen this option and you have a SMTP server configured).

You can also immediately un-stage a user waiting in the staging queue. This executes a direct sync to the Microsoft cloud to determine whether the user has appeared in MS Teams after their licensing update.

6. Verify that the user is configured and licensed:
   - Go to **Users**.

     Note: The **Located At** column on the Users list displays the hierarchy location of each user added to the system, for example, customer or site.

   - Click on the user to view their settings.
   - On the **MS Licenses** tab, view the user's license details.
   - On the **MS Teams** tab, verify the following:
     – The user's number is allocated

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Policies are assigned

Related topics

- Microsoft users in the Core Feature Guide
- Sync to customer then to site in the Core Feature Guide
- Flow through provisioning in the Core Feature Guide
- User staging in the Core Feature Guide
- *Microsoft licenses* in the Core Feature Guide
- *User voice mail settings*
- *Reserve numbers for a user*
- *Introduction to Microsoft Teams policies* in the Core Feature Guide
- *Manage number filters*

Move user & services

Tip: *Use the Action search to navigate Automate*

Overview

Use the **Move User & Services** page where there are existing Cisco UCM users at various sites, and then syncing in the Microsoft users at customer level. A check for mapping matches is carried out at site level to move the corresponding MS users down.

Important: Webex users and their services cannot be moved. A banner on the **Move User & Services** page informs you that options for moving a user are hidden if you select a user enabled for Webex.

Prerequisites

- Enable the **Enable Cisco** / **Microsoft Hybrid** Global Setting so that the **Hybrid Cisco-Microsoft Management** menu is available. See: **Enabled Services** at *Global settings*.

Move scenarios

All of the Cisco move functionality is available, as well as extra workflows for the hybrid moves.

The following scenarios are supported:

- Scenario 1
  - Move MS Teams, MS 0365
  - Set tenantDialplan (optional), onlineVoiceRoutingPolicy (optional)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Move INI and E164 association (if it is in a 1-to-1 association) and create at new site with new country if different
  - Delete SNR at home site and Add SNR at new site
  - Set the INI at new site according to Service Type
- Scenario 2
  - Move MS Teams, MS 0365
  - Set tenantDialplan (optional), onlineVoiceRoutingPolicy (optional)
  - Move INI
  - Delete SNR at home site and Add SNR at new site
  - Set the INI at new site according to Service Type
- Scenario 3
  - Move MS Teams, MS 0365
  - Set tenantDialplan (optional), onlineVoiceRoutingPolicy (optional)
  - new INI at new site
  - Delete SNR at home site and Add SNR at new site
  - Set the INI at new site according to Service Type
- Scenario 4
  - Move MS Teams, MS 0365
  - Set tenantDialplan (optional), onlineVoiceRoutingPolicy (optional)
  - new INI/E164 association at new site
  - Delete SNR at home site and Add SNR at new site
  - Set the INI at new site according to Service Type
- Scenario 5
  - Move MS Teams, MS 0365
  - Set tenantDialplan (optional), onlineVoiceRoutingPolicy (optional)
  - *Do nothing* with lines, do not select anything in **Lines** tab - the assumption is that there was a bulk pre-move of lines to the new site: INI and/or INI/E164 numbers.
  - Delete SNR at home site and Add SNR at new site
  - Set the INI at new site according to Service Type
- Scenario 6
  - If INI is associated to a range of E164s and there is an attempted move line, then this fails with workflow validation.

Note:

- From release 24.1, the **Line Template** drop-down under **Line Configuration** is not used by this feature. Any customizations (for example Field Display Policies) that referenced this field, should be updated to remove references to it.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- If the user has any other Cisco services that were not added by the hybrid feature, such as Phone, EM, RDP, VM etc., these will be moved by the Cisco user move workflows during the Hybrid-Multivendor-Move calls.
- In **Multi Vendor Service User Configuration**, the **New Role** list of available roles will include those where the **Hierarchies Allowed** list of the role contains the target hierarchy selected in the **Move To Hierarchy** list. See: *Role Management*.
- When moving a user that has Microsoft services, and the destination (move to) hierarchy has MS Teams site defaults (SDD) values set up for *Online Voice Routing Policy* or *Tenant Dial Plan*, these values are populated from the site defaults provided you're not setting different values for *Online Voice Routing Policy* or *Tenant Dial Plan* in the *Move user* GUI. Values you set for these items in the *Move user* GUI thus take precedence over values set up in the site defaults when moving a user.

Related topics

- *Global settings*
- *Hybrid Cisco-Microsoft management*
- *Hybrid service definitions*
- *User profiles*
- the Cisco - Microsoft Hybrid Number Inventory topic under Number Management

Microsoft - Move user & services

Tip: *Use the Action search to navigate Automate*

Overview

Automate allows you to move a non-hybrid, Microsoft-only user from one site to another site, with their services and a new line assigned.

You can do this in two ways:

- Use the **Move User & Services** page in the Admin Portal
- Use *Flow through provisioning (FTP)* along with a manual or scheduled sync to update a user in Automate that has been updated on the Microsoft cloud.

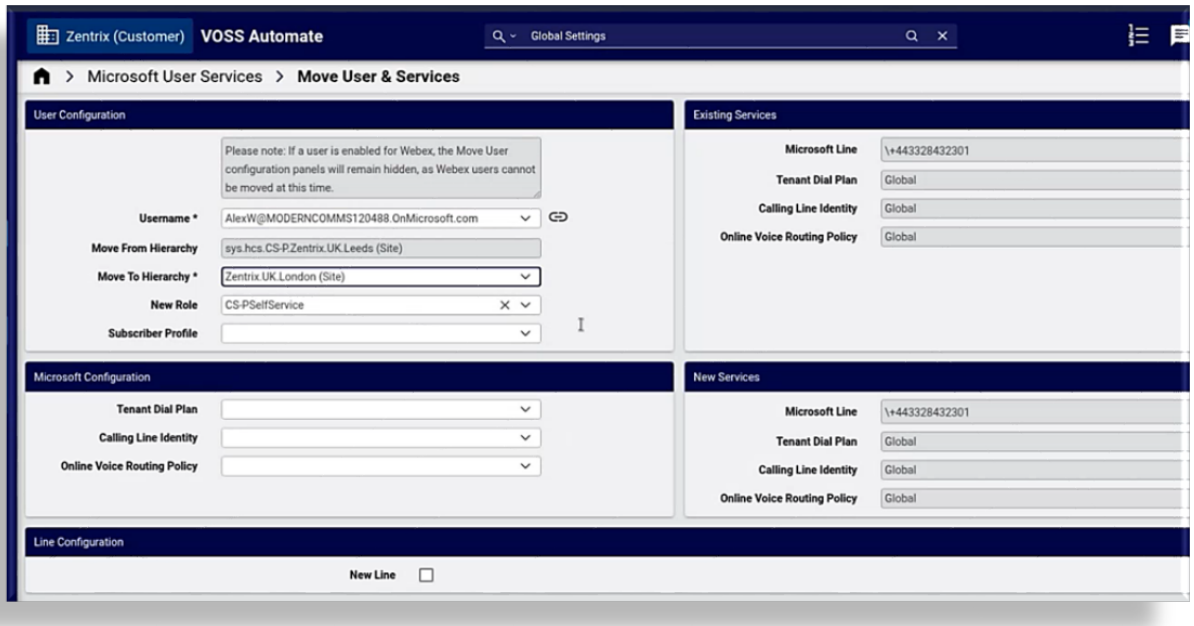
Number types supported for moving a Microsoft-only user site-to-site:

- Direct routing
- Operator Connect
- Calling plan
- Teams Phone Mobile

The table describes how Automate processes various workflow elements in Microsoft-only user move:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Element	Description
Lines	The line can be moved along with the user, or assign a new line. If the number is shared, the “shared line policy” is removed prior to the move and re-assigned after the move.
Policies	Any policies previously assigned to the user that are not overwritten by the new site, remain unchanged.
Licensing	Licensing and usage location remain unchanged. If the user licenses don’t match the supported new number type, a system message warns you that the user can’t be moved.
Enterprise Voice	If Enterprise Voice is enabled at the source site and the target site is non-Enterprise Voice enabled, then Enterprise Voice is also disabled for the moved user at the target site.
Failure handling	If the target site does not support the move, the transaction fails with a descriptive error message.



Related topics

- *Move a Microsoft user between sites using offboard and onboard*
- *Flow through provisioning (FTP)*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manually move a Microsoft user

This procedure manually moves a Microsoft user from one site to another site, with their existing or new services, and a new line.

Prerequisites:

- Ensure you have available lines at the target site. In this case, available lines for Microsoft users.
- To apply settings for the target site via a user profile, ensure the user profile is correctly configured for the services the user requires at the target site.

Move the user:

1. In the Admin Portal, go to **Move User & Services**.
2. Select a username to populate the page with the user's details and existing services.
3. Select an option at **Move to Hierarchy**. Existing services populate on the page.
4. Optionally, select a user profile. The read-only **New Services** fields update with the services assigned via the user profile.

   Note: Values you select in the fields on the **Move User & Services** page override any settings updated by the user profile settings (if you selected a user profile).

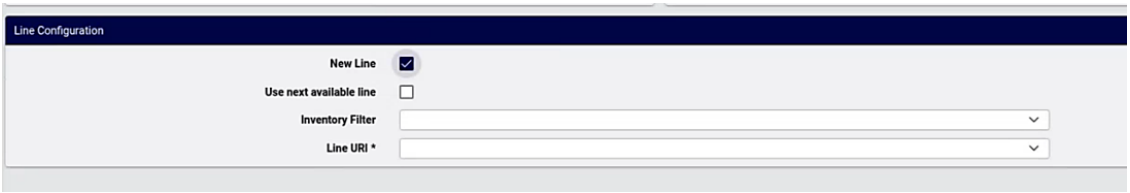
   Using a user profile to move the user allows you to apply the relevant Quick Add Group, policies, and configuration templates to update the user at their new location.

   If you don't select a user profile, the user moves with their current settings, except for the line, since Automate either assigns the next available line at the new site, or you can choose a new line for the target site.

5. Optionally (valid for direct routing only), select a tenant dial plan, calling line identity, and an online voice routing policy.

   Note: Values you select for these fields override values from the user profile for the new services.

6. At **Line Configuration**:
   - Select **New Line** to create a new line at the target hierarchy, or leave the checkbox clear to use the existing line.



   - To have the system find the next available line, select **Use next available line**, and optionally, select **Inventory Filter** so that the system can choose a line from a predefined pool of filtered numbers to be assigned, for example, only unused numbers with associated E164s, or unused numbers at the site only.

     Note: By default, Automate selects the next line available at the current site (checks locally first). If no lines are available at the current site, the system looks up the hierarchy to the customer level

Copyright © 2025 VisionOSS Limited. All rights reserved.

and if an available line is found, the read-only **Microsoft Line** field populates with the selected line.

- Alternatively, manually select a line from the **Line URI** field, with or without a line inventory filter applied.

Note: The **Line URI** drop-down displays available lines for Microsoft users. No additional filtering is applied. The line you choose populates the **New Line** field at **New Services**.

7. Save your changes to move the user with their new services and line.

Related topics

- *User profiles*

Move Microsoft user using flow-through provisioning

This procedure automatically moves an existing and already provisioned Microsoft user from one site to another site (the target site), with their existing or updated services (based on the user profile), and including a new number (line) at their new location.

Note: This scenario assumes the user's location (for example, their city or other geographic location) has been updated on the Microsoft Cloud portal (Microsoft 365 admin center) and you want to sync in this user to Automate and automatically update their location and services for the site they're moving to.

1. Configure model filter criteria for the Msoluser (Microsoft online user) for the target geographic location move.
2. Configure the site defaults.

   Go to **Defaults** for the site. Verify the required model filter criteria is selected in the **Move Filter Criteria** pane (at the **MS 365 User Model Filter Criteria** drop-down).
3. Configure Global Settings.
   - Go to **Global Settings**, and select the **Flow Through Provisioning** tab/panel.
   - Set **Enable Move & Provisioning after Update Sync** to *Yes* (enabled) to allow the user to be provisioned and moved following a data sync.
   - Optionally, select an option at **Flow Through Provisioning Criteria** for the flow through provisioning criteria set up to move the user/users to their new location.
4. Sync in the user:
   - Execute manual sync:

     In the Automate Admin Portal, go to the **Microsoft Tenant** list view, and open the configuration page for the relevant tenant. From the overflow menu, select **Sync New Users**.
   - Wait for scheduled sync:

     You can sync in and move the user via the automatic, scheduled sync (and not manually via **Sync New Users** in the tenant settings).

Copyright © 2025 VisionOSS Limited. All rights reserved.

When the sync runs (manual or scheduled sync), Automate syncs in the user, moves that user to the target site with their new services (line, policies) from the user profile. If the user profile is set up to send the user a welcome email, the user receives an email with their new location and service details.

Related topics

- *User profiles*
- *Model filter criteria*
- *Site defaults*
- *Global settings*

User calling settings

Tip: *Use the Action search to navigate Automate*

Overview

Microsoft

Automate supports configuration of calling (voice) settings for Microsoft users with enabled accounts, from within the VOSS Automate Admin Portal. Configurable settings include call settings and dial out policy, such as call forward and delegation.

Important:

- If you're upgrading to Automate 21.4 from an earlier version, you may need to run an import to ensure all user call settings are imported and are in sync with the settings for this functionality in the Microsoft Teams cloud portal.
- User calling settings display and are configurable *only* for Microsoft users with enabled accounts that can have user calling settings. For example, resource accounts do not have calling settings.

Note: Call delegation allows you to assign another user to make or receive calls on your behalf, for example, when you're out of office or otherwise unable to make or receive calls from your device. In this case, VOSS Automate allows you to define user calling settings that assign the person authorized to make or receive calls on your behalf, including whether this user may change your call settings.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

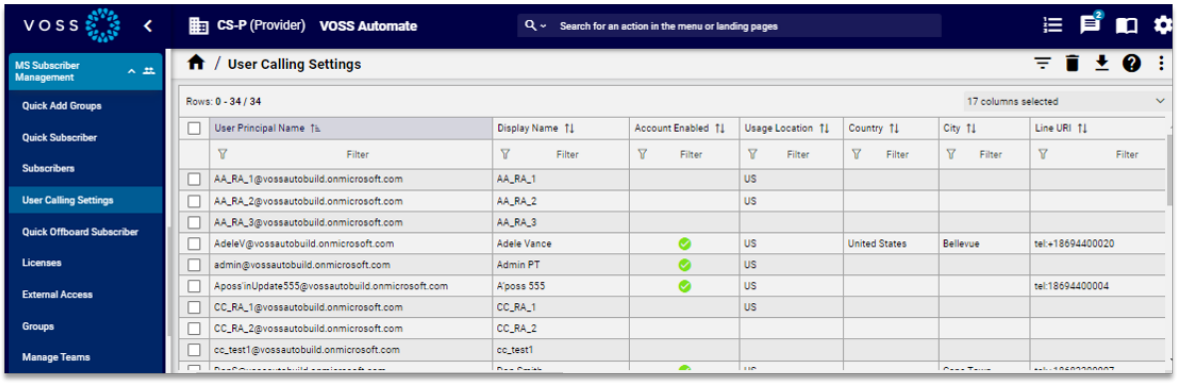
- *Multi vendor users*

Manage user calling settings

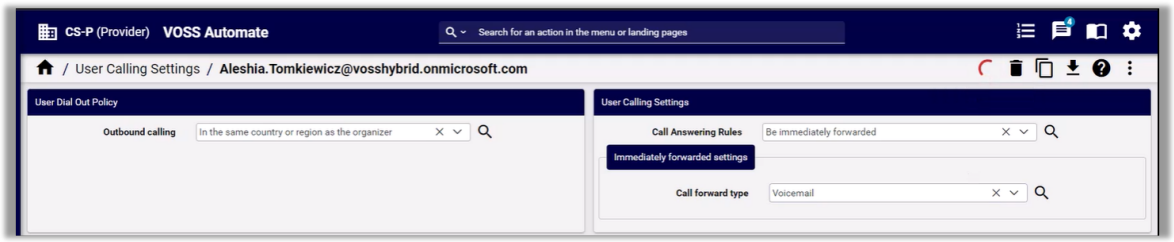
This procedure adds and updates user calling settings.

1. Go to **Call Forward & Delegation**.

   The list view displays configured user calling settings, with a default sort by user principal name.



2. Click on a user in the list view that has the **Account Enabled** column set to True (green check icon), to open their calling settings configuration page.



3. At **User Dial Out Policy**, select an outbound calling setting from the drop-down. Options are:
   - Any destination
   - In the same country or region as the organizer
   - Don't allow
4. At **User Calling Settings**, configure call answering options for this user:

   Note: User calling settings display and can be configured only for Microsoft users with enabled accounts, that can have user calling settings (for example, resource accounts do not have user calling settings).

   The table describes configurable options, which depend on the call answering rule you choose:

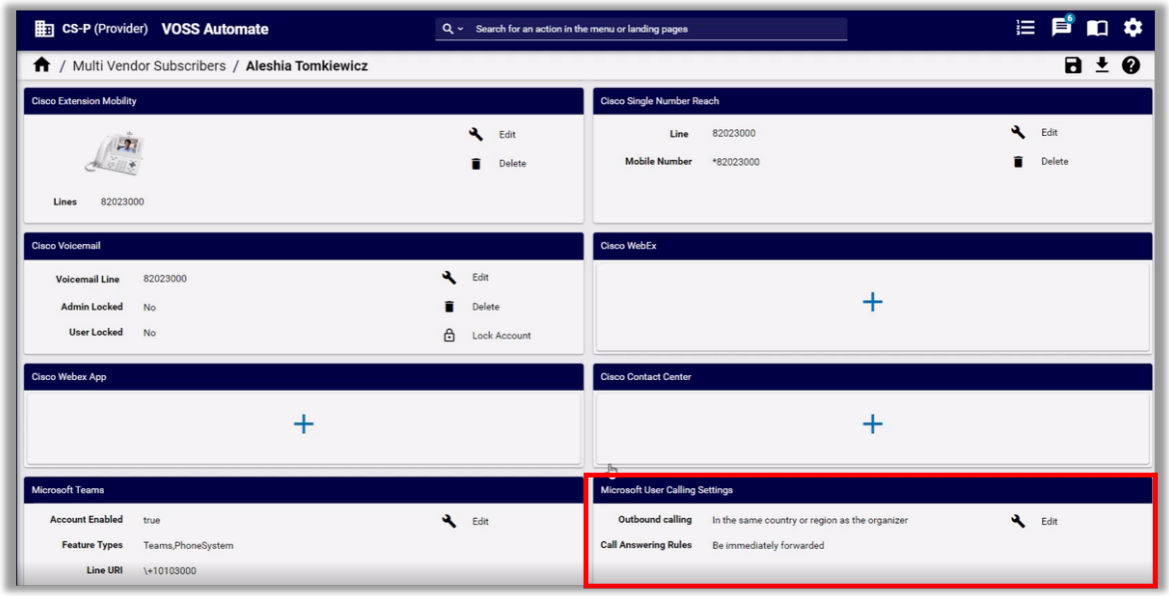
Copyright © 2025 VisionOSS Limited. All rights reserved.

Call Answering Rule	Description
Ring devices	When call answering rule is *Ring devices*, choose one of the following **Ring device settings** for these **Also allow** options: • Simultaneous ring a user Select a person, and choose settings in case the call is unanswered, for example, send to voicemail, forward to another person or to another number, allow group call pickup, set up call delegation, or do nothing. You can also define the number of seconds to wait before the call is redirected. • Simultaneous ring a number Specify another number to ring at the same time, and define rules if the call is not answered. • Call delegation Set up call delegation (choose the user, set up permissions, and define whether the delegated user may change call settings). • Group call pickup Define how the call is redirected if no user answers the call, for example, send to voicemail, forward to a specified person or number, set up call delegation, or do nothing. Also define how many seconds to allow the device to ring before redirecting. • None If **Also allow** is set to *None*, define ring settings if the call is not answered, including the number of seconds to wait before redirecting the call.
Be immediately forwarded	When your call answering rule is to immediately forward the call, at **Call forward type**, choose one of the following options, and configure forwarding settings: • Voicemail The call is forwarded to your voicemail. • Forward to a person Choose the relevant alternative user to forward the call to. • Another number Specify the alternative number to forward the call to. • Delegate Set up call delegation, and define rules for how the call is handled if the call is not answered by the delegated user. • Group call pickup

5. Save your changes.

   You can also view and edit a multi vendor, enabled, Microsoft user's calling settings via **Manage Users**.

Copyright © 2025 VisionOSS Limited. All rights reserved.



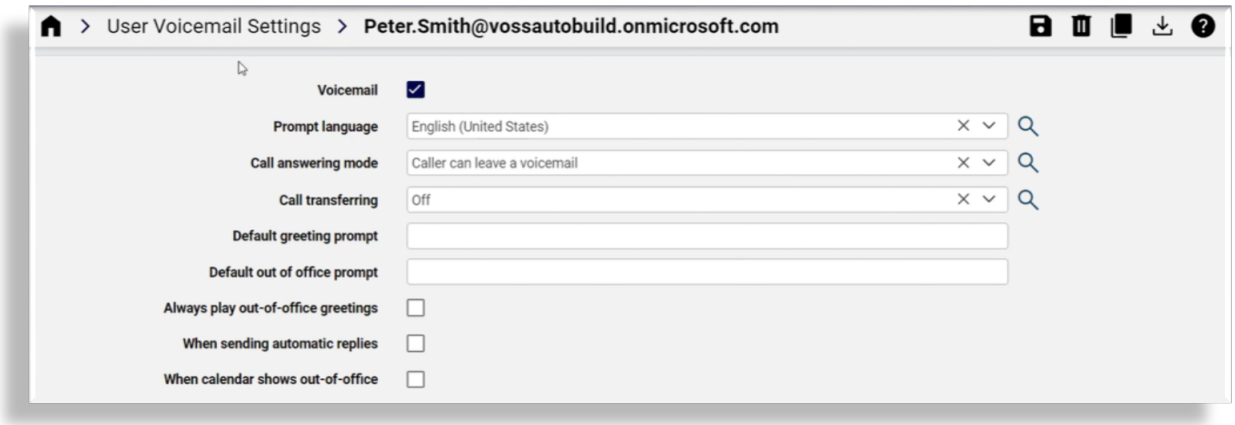
User voice mail settings

Tip: *Use the Action search to navigate Automate*

Overview

Microsoft

Automate supports syncing and management of Microsoft Teams user voice mail settings. Any changes you make for these settings in Automate or in the Microsoft Teams online portal are automatically and immediately synced between Automate and the Microsoft online portal.



Note:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **User Voicemail Settings** page is associated with model `device/msteamsonline/CsOnlineUser` with the `CsOnlineUser_VoicemailSettings_FDP` applied.
- The Microsoft user voice mail service can also be applied via Microsoft Quick User and a Quick Add Group (QAG) that includes the voice mail settings.

Related topics

- *Multi vendor users*
- *Microsoft Quick User*
- *Microsoft Quick User*

Configure voice mail

This procedure configures voice mail settings for a Microsoft user in Automate.

Note: You can also configure these settings on the Microsoft Teams online portal. Automate fetches any updates when you load the **Voicemail Settings** page.

1. Log in to the Admin Portal, then go to **User Voicemail Settings** to display the list view of Microsoft users with voice mail settings.
2. Click on the relevant user in the list to open their voice mail settings management page.
3. Update voice mail settings for this user, any of the following:
   - Enable/disable voice mail
   - Select the prompt language.
   - Select the call answering mode, either of the following:
     - Caller can leave a voice mail
     - Play an outgoing message to the caller
     - Service declines the call with no message
   - Enable/disable call transferring.
   - Optionally, fill out a default greeting prompt and a default out-of-office prompt.
   - Fill out a default out-of-office prompt.
   - Define whether to always play out-of-office greetings.
   - Define when to apply the voice mail settings, either when sending automatic replies and/or when the calendar shows out-of-office.
4. Click **Save**. Your changes are immediately and automatically updated for this user in the Microsoft Teams online portal.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Microsoft Teams CSOL users

This page lists Microsoft Teams users synced in from Microsoft tenants, allowing Automate to stay in sync with users on the Microsoft Teams portal.

You can click on a user in the list to view further details, including their assigned line.

Onboard user (Microsoft)

Microsoft

Overview

Onboarding a Microsoft user involves adding or syncing in users to Automate from the Microsoft portal (Microsoft Entra) with the correct licenses, moving users to the correct site, and provisioning them with the correct services.

Related topics

- *Microsoft Quick Start Guide for Automate*
- *Offboarding (Microsoft)*
- *Microsoft license management and alerting* in the Core Feature Guide
- *Prevent duplicate numbers*
- *Move a Microsoft user between sites using offboard and onboard*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Onboarding elements

The table describes the elements relevant for onboarding Microsoft users:

Element	Description
M365 User (Msoluser)	The base anchor for the user, and typically the first element pulled into Automate for a Microsoft user. Limited update options are available for this user. Automate can update usage location and licenses, depending on how the system is set up.
Usage location	Usage location is updated completely independent from licensing, provided a value for usage location is included in a configuration template (CFT) via Quick Add Group, Subscriber from Profile, or a field display policy (FDP). If usage location updates aren't required (either you're not using it or the permissions don't allow it), then exclude it from the CFT. The *LicenseAssignment* permission allows usage location update. Note that the Microsoft API sets the same usage location; it says it's updating usage location even if permissions don't exist.
Licenses	For onboarding, Quick User, Onboard user, or the field display policy (FDP) honors settings in the Quick Add Group configuration template (CFT) for the M365 user. Direct licenses are applied if they're included. If the CFT does not include any licenses, it won't try to apply licenses. Regardless of the license settings in the CFT, usage location can still be set. If using group licenses, this overrides any direct licenses configured in the onboarding CFTs.

Msoluser onboarding scenarios

The table describes Automate's behavior for the M365 user (`Msoluser`) during onboarding, depending on whether templates exist in your Quick Add Group:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Scenario	Description
No M365 template in your Quick Add Group	Used when the *LicenseAssignment* permission is not assigned to the application. In this case: • *Msoluser* is left untouched - usage location and license is not updated.
M365 user template exists in your Quick Add Group	• Usage location entry: – Automate updates the usage location according to definition in the CFT • License data (*LicenseAssignment* permission required): – Automate adds any license/s defined in the CFT (direct license assignment to the user) – Any existing licenses the user has (direct) are replaced with what was configured in the template
MS Group Add template exists in your Quick Add Group	Used to add group memberships to the user/s (for licensing or other purposes). The user is assigned to the group/s in the CFT, in addition to any existing group memberships the user has.

Common onboarding scenarios and setup

The table describes example common onboarding scenarios and the setup required, whether using Quick User, Onboard user, or a field display policy (FDPs):

Example onboard scenario	Setup
No update to Msoluser at all (usage location and/or licenses)	Do NOT include a *M365* template in the Quick Add Group.
Update usage location, no license update	• Include a *M365* CFT in your QAG. The CFT must include the usage location logic you require (for example, macro from site default, etc). • Leave the license fields blank in the CFT.
Update usage location, and update license (direct licensing)	Include a *M365* CFT in your Quick Add Group that includes the usage location logic and licenses you require (e.g. macro from site default, etc).
Update usage location and group assignment (for license or other purposes)	• Include a *M365* CFT in your Quick Add Group that includes the usage location logic you require (e.g. macro from site default, etc.) • Include a *Add Group* CFT in your Quick Add Group that includes the groups you wish to add to the user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Syncing in and onboarding Microsoft users

Automate provides two onboarding sync options for Microsoft users:

Sync users to customer level, and then to sites	*Configure Automate for Microsoft services* This option starts with an initial import of dial plans, policies, licenses, and Microsoft users, to the customer level (sync all to the tenant). Then you will need to set up the configuration and user move criteria before moving users to the sites (set up model filter criteria, site defaults, quick add groups, user profiles, and number inventory). Finally, you have two options to move users to the sites as fully provisioned users: • Run the overbuild to move multiple users to your sites at once. • Update single users via Microsoft Quick User When moving users to site, the Automate automated workflow applies the required configuration, services, lines, policies, and licenses.
Sync users directly to sites	*Sync to site with flow through provisioning* In this option, you run the initial sync together with flow through provisioning. In this case, you start by setting up the configuration and user move criteria before running the initial sync. That is, to set up the model filter criteria, site defaults, quick add groups, and user profiles. In addition, you will need to: • Configure flow through provisioning criteria • Enable flow through in the Global Settings Once changes are synced in from the Microsoft Cloud, Automate automated workflows move the tenant dial plan, policies, and licenses to the customer level, and moves users directly to the appropriate sites as fully provisioned users.

Note:

- Automate v21.2 introduced sync with flow through provisioning for Microsoft users. In 21.3, this feature extends the functionality to users synced in from LDAP and Cisco UCM.
- Only *Add* is supported for syncs with flow through provisioning. Update and delete are not supported since the requirements may differ depending on the customer scenario.
- For details on the generic flow through provisioning feature (which includes Microsoft, LDAP, or Cisco UCM users), see *Flow through provisioning (FTP)*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Prevent duplicate numbers*

Offboarding (Microsoft)

Tip: *Use the Action search to navigate Automate*

Overview

Offboarding Microsoft users in Automate is the process whereby the user is de-provisioned (their services are removed), and they're moved from the site (default) back to the tenant level in the hierarchy, typically, customer.

Note: By default, *Offboard user* moves the user from the site. However, you can change the **Retain User at Site after MS Offboard User** global setting to *Yes* (default is *No*) so that the user won't be moved. See *Global settings*.

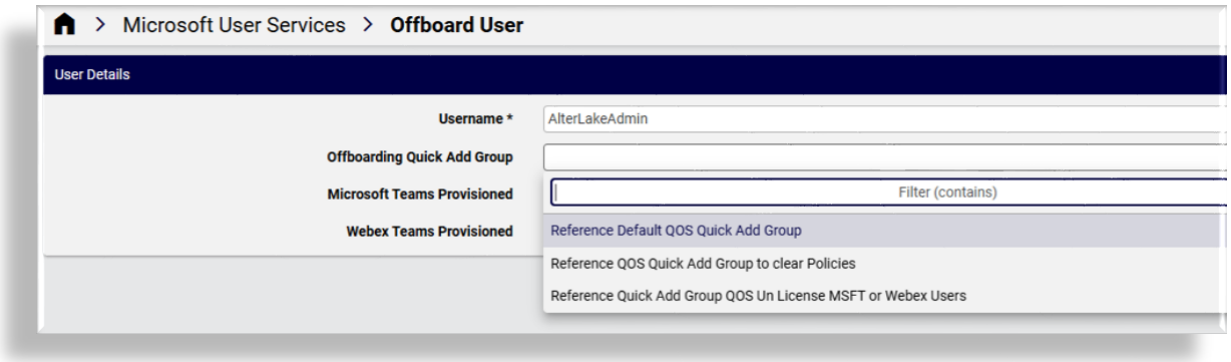
If a user is moved from the site during offboarding and they had a Self-service role at the site, their Self-service role is retained when they move to the customer level and if you later move this user to another site.

When offboarding, the user's *Usage Location* remains unchanged. Since Automate doesn't automatically manage user licenses (you'll need to grant Automate permissions to do this for Microsoft user licensing), the users licenses remain in place when offboarded unless Automate has license management permissions.

When running *Offboard User* for Microsoft you can choose from a filtered list of Quick Add Groups (QAGs) flagged for offboarding. These designated QAGs contain configuration templates (CFTs) that define how the user should be offboarded and de-provisioned. For example, via the CFTs in the QAG you can choose to:

- Leave the usage location and licenses in place
- Remove licenses (system default behavior)
- Remove licenses via removal of groups

Automate ships with default *offboard* Quick Add Groups (QAGs). You can use the defaults or clone and customize a QAG to use for offboarding via *Quick Add Groups*. QAGs flagged for offboarding display in the **Offboarding Quick Add Group** drop-down on the **Offboard User** page.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Onboard user (Microsoft)*
- *Quick Add Groups*
- *Reserve numbers for a user*
- *Offboard user (Webex or Microsoft)*
- *Move a Microsoft user between sites using offboard and onboard*

Configure a CFT for offboard user (Microsoft)

The configuration template (CFT) to be included in a Quick Add Group flagged for user offboarding may be customized via referenced variables to define how a user should be offboarded and de-provisioned.

In the Quick Add Group, you choose the CFT to use and select the *Subscriber Offboarding* checkbox. The CFT is customized to run the offboarding workflow. When running user offboard for Microsoft you can choose a Quick Add Group flagged for offboarding, and the CFT referenced in this Quick Add Group runs the offboarding workflow.

Note: A MSOL CFT removes licenses. A CSOL CFT only removes voice services (disables enterprise voice and removes the line). The CSOL CFT clears or changes values and should contain `fn.unset` for any fields that need to be cleared, such as *LineURI* and *enterpriseVoiceEnabled*. See the `System Microsoft Teams Online User Template Un License User` CFT for an example of the minimum configuration required.

If you don't select an offboarding Quick Add Group, the system default offboarding behavior applies.

Workflow when offboarding a Microsoft user

The offboard user workflow for a Microsoft user is as follows:

- The number assigned to the user in Microsoft Teams is removed and Enterprise Voice is disabled.

  Any other setting defined in the Teams configuration template (CFT) in the Quick Add Group, such as policies, are applied.
- The number is released in the Automate number inventory, and is either made available or placed into cooling, depending on your setup.
- M365 user (`Msoluser`) is updated based on configuration:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Licenses	– (Default) Remove licenses The default behavior is that all licenses are removed from the user. The `LicenseAssignment` permission is required in the system. If this permission is unavailable, the transaction ignores the error from Microsoft and continues to execute but leaves the licenses unchanged. – (Recommended) Leave licenses as is You'll need to configure Automate to leave the licenses unchanged if you don't wish to manage licenses. See the note below. It is recommended that you configure this behavior rather than relying on the default behavior (Remove licenses).
Remove from group(s)	This behavior is based on the *Remove Groups* configuration template included in the Quick Add Group.

- Move the user and related Microsoft service records (Msoluser, Csonlineuser, Exchange, etc.) back to the tenant level in the hierarchy (typically, customer).

  The user's role is also updated to a Self-service role at that level in the hierarchy. The user is then ready for onboarding again if needed (for example, in another site).

Common offboarding scenarios and setup for a Microsoft user

The table describes example common offboarding scenarios and the setup required when using *Offboard user (Webex or Microsoft)* for a Microsoft user:

Example onboard scenario	Setup
No update to *Msoluser* at all (usage location and/or licenses)	To set this up, see the section headed *Configuration to not remove licenses*
Remove licenses (direct licensing)	System default behavior; no additional configuration required.

Allow a Microsoft user to retain their licenses during user offboarding

This procedure configures Automate to leave a Microsoft user's licenses in place when running *offboard user*.

In this case, the default *ProviderAdmin* role (or any cloned role with similar access) will need to clone the `MicrosoftSubscriberMsolUser_Update` CFT to the customer hierarchy, and without making any changes to this CFT, just click **Save**.

Note: By default, for customers using Automate for license management and assigning license directly to

Copyright © 2025 VisionOSS Limited. All rights reserved.

users, *offboard user* removes all of the user's licenses.

Configure the following in Automate:

- Use the `MicrosoftSubscriberMsolUser_Update` configuration template (CFT) to configure license handling.
- By default, Automate attempts to remove all licenses assigned to the user. To change this behavior, clone the `MicrosoftSubscriberMsolUser_Update` CFT to a lower level in the hierarchy (the hierarchy where you want to change the default behavior). For example:
- Clone the CFT to *Provider* level if you want to apply it everywhere
- Clone the CFT to a particular *Customer* level (if it's customer-specific)
- After cloning the CFT, the licenses array in the CFT should be blank. If it's not blank for some reason, clear the licenses array in the cloned CFT before saving it.
- To change back to the default behavior to clear the licenses, you can delete the cloned CFT to return to the sys level instance of the CFT.

Microsoft user updates when offboarding

With regard to user updates in terms of usage location and licenses when offboarding, similar to onboarding, the *LicenseAssignment* permission is required to update the Usage Location and License fields via the **Microsoft User Details** page.

If permissions aren't granted and you're using direct licenses, it is recommended that you adjust your field display policy (FDP) for `relation/MicrosoftSubscriber` to make the Usage Location and License fields read-only for clarity to administrators.

Note: If you follow the steps in Offboard User to retain licenses on the user, any changes to licenses via the user won't be applied. This is for the case where you won't be managing licenses from Automate.

Offboard user (Webex or Microsoft)

Tip: *Use the Action search to navigate Automate*

Offboard a Microsoft or Webex user

This procedure offboards a user provisioned with the Microsoft Teams or Webex service and moves the user from the site to the customer level.

Note: The form displays read-only fields to indicate the user's provisioned services, Microsoft or Webex. The **Hybrid Status Message** field displays the user's hybrid status (for a user with Cisco-Microsoft services). See *Hybrid Cisco-Microsoft management*.

Custom strings may also exist on the form. These are configured via the field display policy for the model, `view/SubscriberQos`.

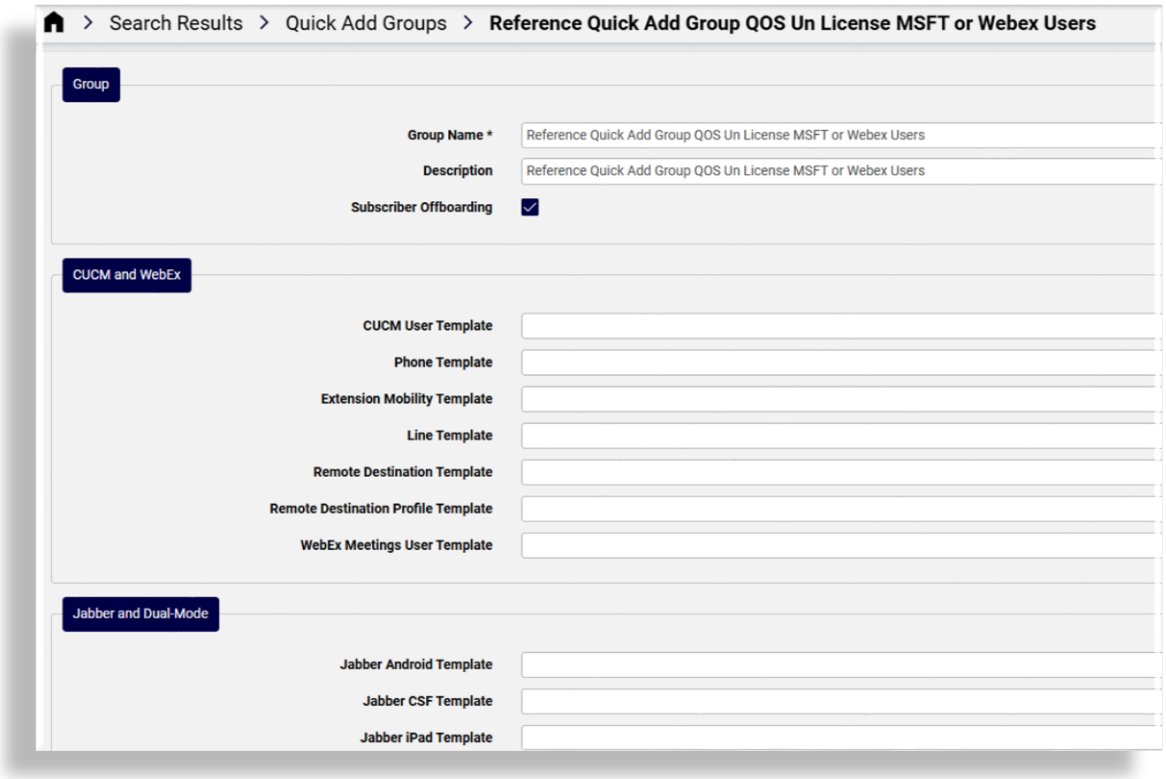
Copyright © 2025 VisionOSS Limited. All rights reserved.

1. In the Admin Portal, go to **Webex User Services** or **Microsoft User Services**.
2. Click **Offboard User**.
3. Select the username.
4. Optionally, at **Offboarding Quick Add Group**, select a Quick Add Group, or leave the field blank to apply the system default behavior.

Note: Quick add groups in the drop-down are enabled for user offboarding.

If you don't see the **Offboarding Quick Add Group** drop-down on this form, it's hidden via the field display policy (FDP), which means that the system default behavior applies when offboarding users. The system default for offboarding is to remove the user's licenses and services.

If you wish to customize how and whether licenses, and/or lines, and/or or services are removed when offboarding, you can set up this behavior in a custom configuration template (CFT), and associate it to a Quick Add Group used for offboarding to define how users are to be offboarded and de-provisioned.



---

5. Optionally, if the user has the read-only **Webex Teams Provisioned** checkbox enabled (indicating the user has Webex services), you can choose to select **Remove Webex User if permitted** to remove the user during offboarding.
6. Click **Save**.

   The user is moved to the sync source hierarchy, (typically, customer). For a Webex user, this includes moving the Contact Center and or Wholesale user (if these exist). If you've chosen to remove the Webex user, the user is removed from the system.
7. Verify that the user is de-provisioned and offboarded as defined via the configuration template in the Quick Add Group you chose, either a customized offboarding Quick Add Group, or the system default

Copyright © 2025 VisionOSS Limited. All rights reserved.

behavior.

The system default behavior for user offboarding removes the user's licenses and services:

Important: The offboard user transaction for a Microsoft user requires a sync with the Microsoft Cloud and relies on waiting for incoming new data from Microsoft. For this reason, you may expect some delay (between 30 and 60 seconds), before the user's new status (unlicensed and/or services removed) displays in Automate. For example, the user may still appear as licensed in Automate, and values such as *PhoneSystem* may still display as an assigned service in the Automate cache, even though the user is unlicensed and services are removed.

Related topics

- *Quick Add Groups*
- *Offboarding (Microsoft)*

Expose custom string fields on Offboard User

This procedure exposes custom string fields on the **Offboard User** page (*view/SubscriberQos*), providing flexibility for adding additional details for a user, if required to set specific values that for can example trigger workflows during off-boarding.

Note: The **Offboard User** page allows for the exposure of up to ten custom string fields and up to 10 custom boolean fields to the field display policy (FDP) you apply to the **Offboard User** page (*view/SubscriberQos*). Values are:

- **Custom String 1** (`customString1`) to **Custom String 10** (`customString10`)
- **Custom Boolean 1** (`customBoolean1`) to **Custom Boolean 10** (`customBoolean10`)

1. Log in to the Admin Portal as Provider admin or higher.
2. Create or update the Customers data model field display policy:
   - Go to **Field Display Policies**, and locate the entry for target model type *view/SubscriberQos*.
   - Click on the default field display policy (FDP) for the model (the FDP named *default*).
   - Clone (copy) the default FDP for the model, and give the clone a new name.

     Note: You can't modify default FDPs that ship with the system. This allows you to refer to or revert to a system default at any time, if required.

   - Modify the new FDP (the clone).

     Note: You can add a new group of fields containing only the new custom fields, or add fields to existing field groups.

   - Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Update the dashboard (*Introduction to Automate dashboards*) or menu layout (*Menu layouts*) to apply the FDP, and save your changes.
4. Log out, then log in again as Provider admin.

   Role-based access profile changes refresh so that you can view the updated menu layouts and FDPs you applied, including new custom fields.

Microsoft users

Tip: *Use the Action search to navigate Automate*

Overview

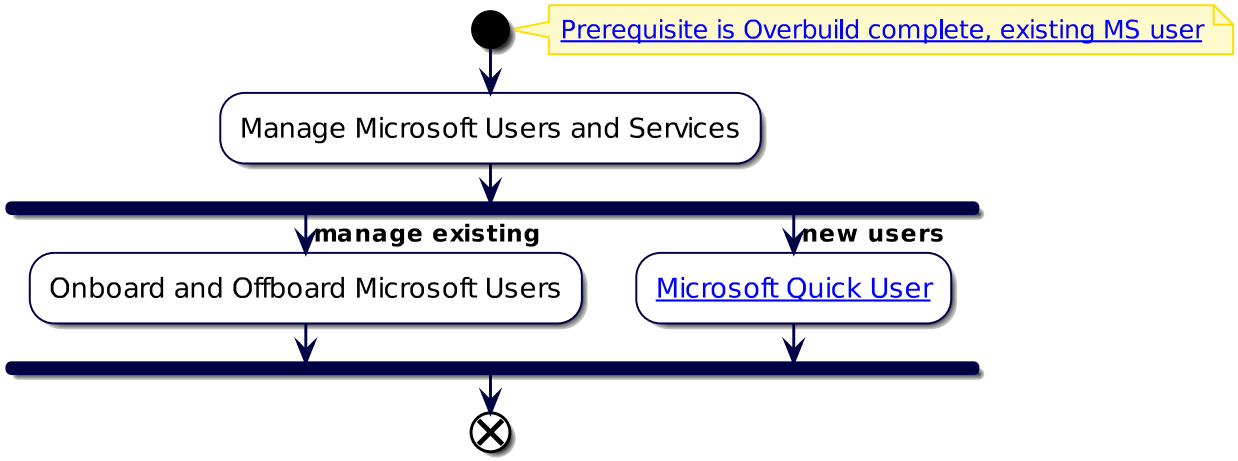
You will need to onboard Microsoft users in Automate.

Onboarding a Microsoft user involves importing users and related data to the customer level from the Microsoft Cloud service, and then moving users to the correct sites as fully provisioned users.

Automated workflows configure imported objects once changes are synced in, and apply the required configuration, policies, and licenses. This means administrators won't need to continually monitor the sync, or to perform additional steps to complete the process.

Once synced in (at the customer or site level), administrators can manage Microsoft users via a single interface and login, from within the Automate Admin Portal. To maintain data integrity, to manage licenses, and to automate number auditing for synced in users, regular, targeted backend syncs poll for changes made at the device model layer.

Note: If **Enable Microsoft User License Enforcement** is set to **Yes** in the **Global Settings**, a user can only be added if the license allocation limit for the user's hierarchy is not exceeded. For details, see *Microsoft License Management and Alerting* in the Core Feature Guide.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Microsoft Overview in the Core Feature Guide
- Automate Configuration and Sync for Microsoft Services in the Core Feature Guide
- Sync to Site with Flow Through in the Core Feature Guide
- Microsoft Exchange in the Core Feature Guide
- *Offboarding (Microsoft)*
- *Microsoft Quick User*
- *Prevent duplicate numbers*
- *Onboard user (Microsoft)*

View and edit Microsoft users

View a summary list of all Microsoft users

This procedure displays a summary list of Microsoft users.

1. Log in to the Automate Admin Portal.
2. Choose the hierarchy.
3. Go to the **Microsoft User Details** page.
4. View a summary of Microsoft users at the current hierarchy.

   The list view for Microsoft users provides details for the following, for each user in the list:

   - User principal name, first name, and last name
   - Licenses
   - Department
   - City, country, phone number, location
   - Associated device

View and update a Microsoft user

This procedure displays and edits the details of a single Microsoft user.

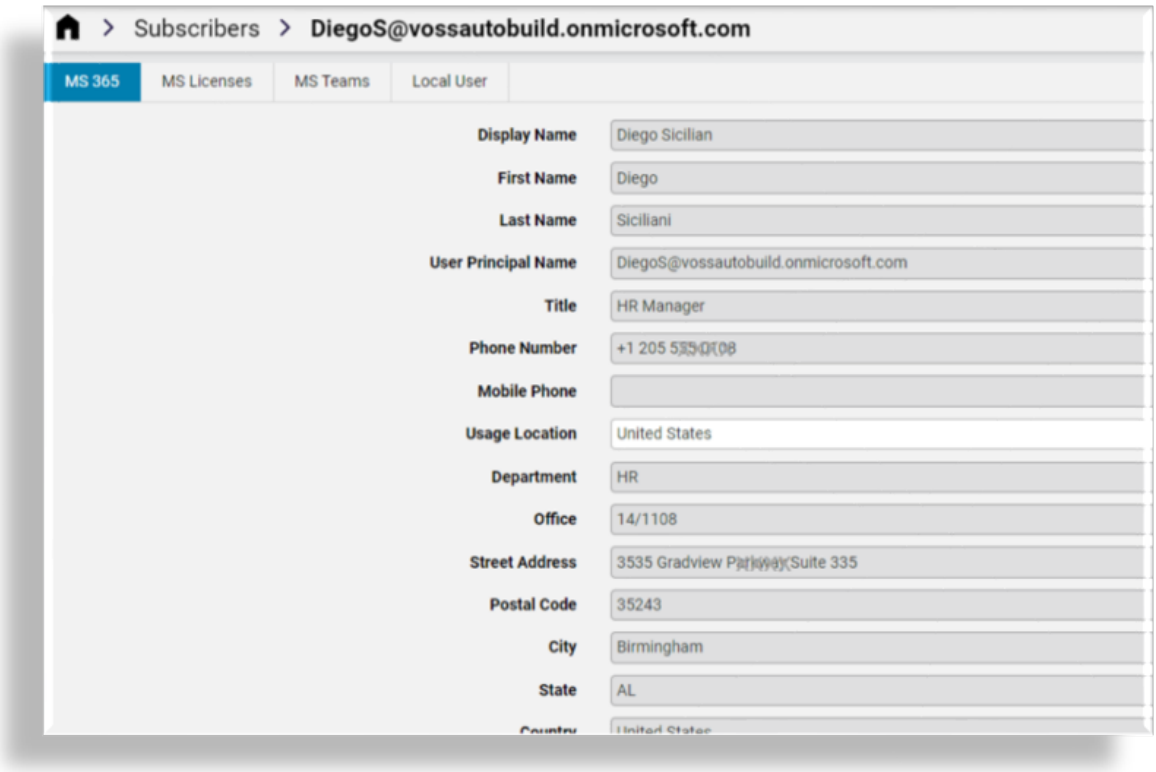
Note: This workflow is intended for Microsoft-only users. When choosing a hybrid user with Cisco-Microsoft services, you'll need to work with this user via the Hybrid multi vendor actions. The **Hybrid Status Message** field displays the user's hybrid status. See *Hybrid Cisco-Microsoft management*

---

1. Log in to the Automate Admin Portal.
2. Choose the hierarchy.
3. Go to the **Microsoft User Details** page.
4. View a summary of Microsoft users at the current hierarchy.
5. Click on a user in the list to open their settings.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Select a tab (or scroll to the relevant panel) to view and update settings:



Note: Automate allows you to toggle between a panel or tab layout via a toolbar button. The tabs/panels that display depend on enabled functionality.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Tab/Panel	Description
MS 365	Microsoft user details, such as their display name, first and last name, User Principal Name (UPN), title, contact details, usage location, department, employee ID, employee type, and groups.
Exchange Custom Attributes	Read-only. Displays on the user's form only when Microsoft Exchange is installed and enabled for the user (the user has a Microsoft Exchange license), and provided values are filled out for these fields on the user's Microsoft Exchange settings in Automate. These are fifteen additional fields that can be used for filtering from Microsoft Entra ID using model filter criteria, and to have the values available for flow through provisioning. The same fields are also available in the Microsoft Exchange settings (when installed) in Automate. The fields allow more flexibility when filtering users to be imported and then moved and, optionally, processed with flow through provisioning in Automate.
MS Licenses	View and update the user's Microsoft license details, including their type (Group or Direct), and their licenses. **Note:** When the license type is "Group", all license details (SKU and service plans) read-only.
MS Teams	The Microsoft user's MS Teams details. The fields below are read-only: • User status • Interpreted User Type • Country or Region • Feature Types • Line URI • Line Type On this tab you can also enable or disable Enterprise Voice for this user. • You can only enable Enterprise Voice for a user that has a PhoneSystem license. • You can only assign a number to a user that has a PhoneSystem license.
Local User	The user corresponding with this user.

7. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Model filter criteria*
- *Flow through provisioning (FTP)*

Manage a user's MS Teams policies

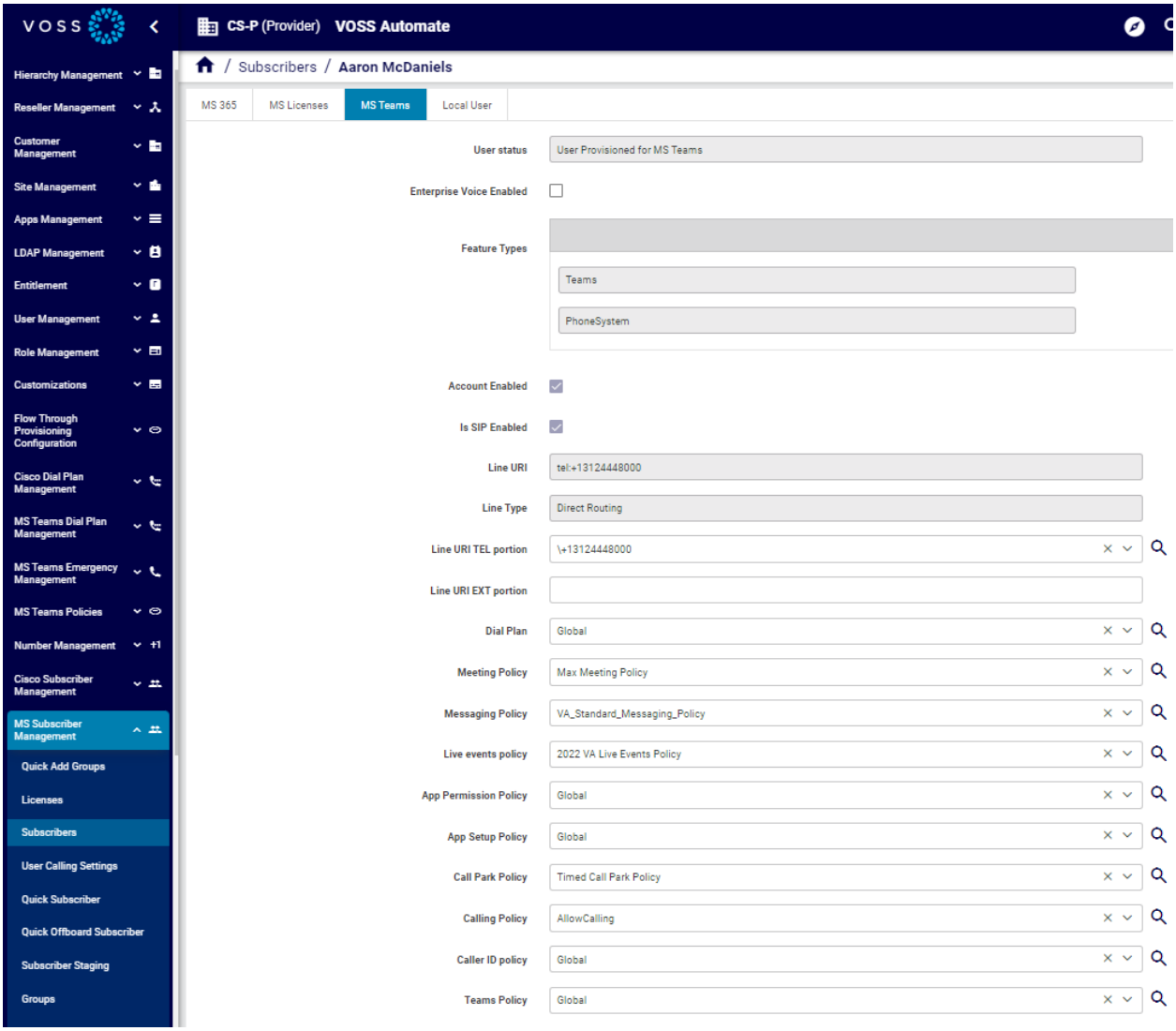
This procedure displays and updates the policies of individual users via the user edit functionality:

Note: Some policies support full CRUD (create, update, delete) operations within Automate.

Note: This workflow is intended for Microsoft-only users. When choosing a hybrid user with Cisco-Microsoft services, you'll need to work with this user via the Hybrid multi vendor actions. The **Hybrid Status Message** field displays the user's hybrid status. See *Hybrid Cisco-Microsoft management*

1. Go to the **Microsoft User Details** page.
2. Click on a user to open their settings.
3. Select the **MS Teams** tab.
4. View currently applied policies for the user.
5. To choose different policies, click the down-arrow at the relevant policy, and select an alternative from the drop-down.
6. Save your changes. Policy changes are synced back to the Microsoft cloud when performing an overbuild or a sync.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- *Introduction to Microsoft Teams policies* in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

User staging

Tip: *Use the Action search to navigate Automate*

Overview

When onboarding Microsoft users into Automate, unlicensed Microsoft 365 users are synced in to Automate from the Microsoft Teams cloud portal.

It is possible to license Microsoft users from within Automate. You could use Quick User to apply a user's MS Teams configuration and to license the user in a single operation. Since there is a dependency on the Microsoft cloud to sync the changes once the user is licensed, Automate places the user in a staging queue while it waits for the Microsoft cloud process to complete.

Related Topics

- Microsoft Users in the Core Feature Guide
- Microsoft Quick User in the Core Feature Guide
- Site Defaults in the Core Feature Guide

Scheduled staging sync

A scheduled staging sync and workflow can be enabled. This workflow removes the user from staging (unstage), re-runs the Microsoft Quick User workflow, updates the Microsoft Teams user with their correct provisioning details, provisions the user in Automate, and flags their number as used.

The staging schedule sync is disabled by default on install. When enabled, the default is for the staging schedule to run every 4 hours.

You can enable the staging schedule sync (`ScheduleMSTeamsOnlineTargetUserSync`) in Automate via the **Sync Scheduling** page (select **Active**), where you can also change the execution schedule (default is every 4 hours).

Unstage MS users

If the Microsoft Teams cloud portal takes too long to create the Microsoft Teams user and you don't want to wait for the scheduled workflow to execute (if its enabled), you can perform an unstage action on one or more selected users on the **User Staging** page to immediately execute the workflow for the selected users.

Copyright © 2025 VisionOSS Limited. All rights reserved.

To unstage one or more MS users

1. In the Admin Portal, use the **Action** search to go to the **Microsoft Users in Staging** page.
2. Select one or more users to remove from staging.
3. Click **Unstage immediate**.

8.1.3. General Exchange Functions

Microsoft Exchange

Tip: *Use the Action search to navigate Automate*

Overview

This feature allows you to manage Microsoft Exchange Online mailboxes and calendars from within Automate, including assigning access and calendar permissions to users and team members licensed for Microsoft Office.

Using automation, it is possible to model the end-state of a user's mailbox configuration during their on-boarding or offboarding workflow. For example, it is possible to have the correct retention policy or archiving status set when a user's mailbox is being on-boarded. Or automatically have email forwarding and automated replies set when the user's mailbox is being offboarded.

Note: Any admin role (Provider, Customer, Site) can access and work with Microsoft Exchange mailboxes, provided that Microsoft is enabled at the hierarchy.

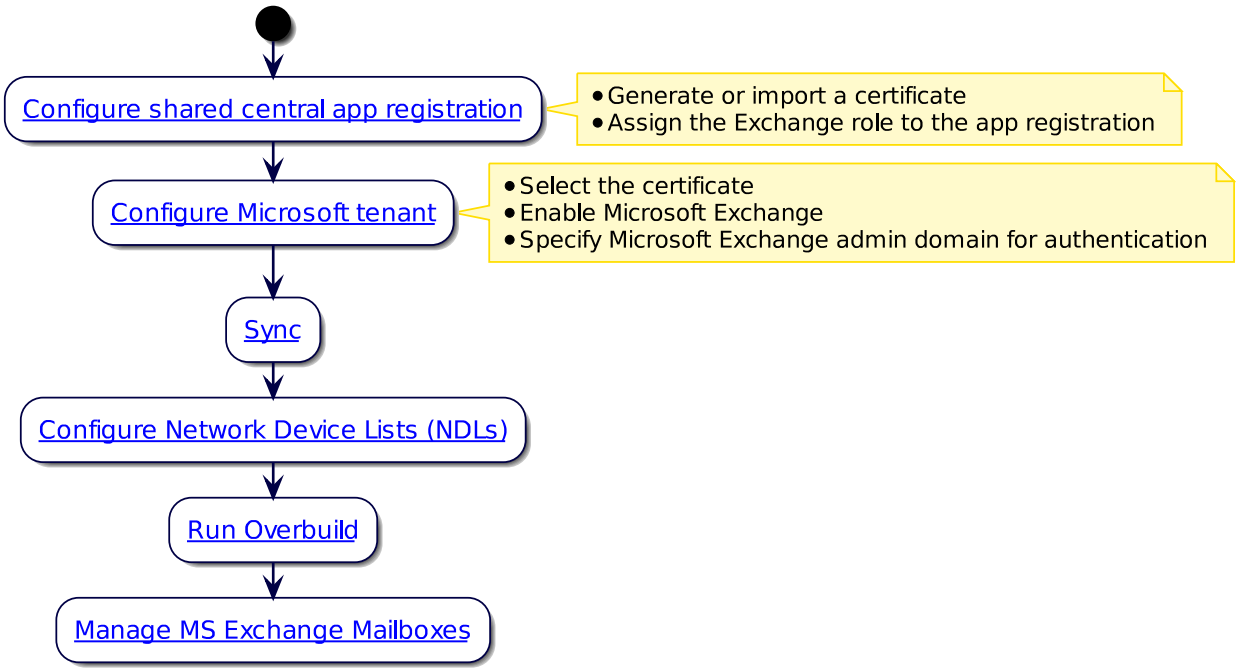
Related topics

- Microsoft tenant setup in the Core Feature Guide
- Overbuild for Microsoft in the Core Feature Guide

Microsoft Exchange Integration

The diagram displays the workflow steps for integrating Automate with Microsoft Exchange:

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes the steps in the Microsoft Exchange integration workflow diagram:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Integrate Microsoft Exchange	Description
1. Generate/import certificate in Automate, & enable Exchange	When adding the new Microsoft tenant and you're using Microsoft Exchange, you must either generate a certificate or import an existing certificate and have Automate manage it. Automate pushes the certificate to the PowerShell proxy.
2. Perform a sync	Once the Microsoft tenant is configured, perform a sync from the tenant configuration screen. This syncs in all Microsoft entities configured on the tenant, including Microsoft Exchange components.
3. Configure NDLs	To prepare for the overbuild that will move synced in Microsoft entities to the sites (including Microsoft Exchange components), add the Microsoft Exchange authentication credentials to the network device lists (NDLs) for sites with users requiring mailbox management in Automate.
4. Run overbuild	Microsoft users must be included in the overbuild settings. An overbuild moves Microsoft Office 365 users to the sites, based on the model filter criteria defined in the overbuild settings. Microsoft 365 users includes users enabled for Microsoft Teams and Microsoft Exchange on the Microsoft Cloud portal.
5. Manage mailboxes	Once you've set up Automate for integration with Microsoft Exchange Online, synced in mailboxes, and run the overbuild to move users and mailboxes to the sites, you can manage these mailboxes and calendars for users and users and teams from within Automate: • Assign access and calendar permissions for user mailboxes • Add, update, or delete shared mailboxes, including assigning or removing mailbox access and calendar permissions • Add or update the **Owners** field for Distribution Group mailboxes

Supported Microsoft Exchange mailboxes in Automate

Four types of Microsoft Exchange mailboxes are supported in Automate:

- User mailboxes
- Shared mailboxes
- Room mailboxes
- Distribution Groups

User mailboxes are created for individual Microsoft Office 365 users on the Microsoft Cloud portal, while shared mailboxes, room mailboxes, and distribution groups can be created on the Microsoft Office portal or in Automate.

Any changes made to the mailboxes and their associated calendars are synced between the Microsoft Cloud portal and Automate. This allows an Automate admin user to manage mailboxes from within Automate, and have these changes seamlessly update on the Microsoft Cloud.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The table describes the Microsoft Exchange mailboxes supported in Automate, and the ways in which you can work with these mailboxes:

Mailbox type	Description
User	User mailboxes are assigned to a single, licensed, Microsoft Office user. These mailboxes are created on Microsoft Exchange Online and synced in to Automate. The ability to manage access permissions on user mailboxes and calendars is useful where you need to allow other users to view, send, or receive emails on behalf of the mailbox owner. For example, to grant access to an executive assistant, or to monitor the mailbox of a user who is unable to attend to their emails or calendar items while out of office.
Shared	Shared mailboxes can be created on Microsoft Exchange and synced in to Automate, or they can be added, updated, or deleted on Automate, and any changes are then synced back to the Microsoft Cloud portal. Shared mailboxes are useful for groups of individual users or for teams. For example, a shared mailbox might be used for a support or sales team, with different members having the same or custom access and calender permissions on the shared mailbox. The owner, or user principal, of a shared mailbox is a 'dummy', unlicensed user on the Microsoft Cloud, and does not add to the Automate user count. The user principal name of a shared mailbox is auto-generated based on the display name you define.
Room	Room mailboxes can be created on Microsoft Exchange and synced in to Automate, or they can be added, updated, or deleted on Automate, and any changes are then synced back to the Microsoft Cloud portal. Rooms are entities, typically an actual room at a physical location, that become a user for the purpose of creating the Microsoft Exchange mailbox. The entity name is the user principal name of the room mailbox.
Distribution Group	Distribution Groups can be created on Microsoft Exchange and synced to Automate, or they can be added, updated, or deleted on Automate, and any changes are then synced back to the Microsoft Cloud portal. A distribution group is typically used to send emails to a group of recipients. You can add owners (one or more), for a distribution group in Automate, as well as modify owners.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Mailbox access permissions and calendar permissions

Access permissions on Microsoft Exchange mailboxes define the ownership rights and mailbox access permissions of one or more users for the mailbox. When configuring access permissions on a mailbox, you select a user from a list of users at the same hierarchy level as the mailbox, and select their access role permissions, for example, `Read and Manage`, `Send As` or `Send on Behalf`.

Calendar permissions allow you to assign a combination of role access permissions, such as `Owner`, and individual permissions, such as `Delete All Items`, to one or more users, on the calendar associated with the mailbox.

You can assign or remove access permissions and calendar permissions on all mailbox types, for users that exist at the same site as the mailbox.

Manage Microsoft Exchange mailboxes in Automate

This procedure updates Microsoft Exchange user mailboxes, and adds, modifies, and deletes Microsoft Exchange shared mailboxes, room mailboxes, and distribution groups.

Note: You can only add or delete shared mailboxes, room mailboxes, and distribution groups in Automate. User mailboxes may be updated in Automate, but they can be added or deleted only on the Microsoft Cloud portal.

---

1. Log in to the Automate Admin Portal.
2. Go to the **Exchange** page.
3. Choose the menu for the relevant mailbox type, either **User Mailboxes**, **Shared Mailboxes**, **Room Mailboxes**, or **Distribution Groups**.
4. View the summary list view of the mailbox type you selected.

   Note:

   - The **Located At** column in the list view displays the hierarchy level of mailboxes. Some may be at the customer level, and some may have been moved to a site.

     Microsoft Exchange mailboxes are initially synced in at the customer level, and must be moved to the sites, either manually (via the list view or the mailbox management screens), or when running the overbuild.
   - Separate menu items are available for recipient types of mailboxes: **User Mailboxes** and **Shared Mailboxes**. If required when a user if off-boarded, the **User Mailboxes** entry can be converted to a **Shared Mailboxes** entry. Refer to the additional API operations available for the users's mailbox ArchiveStatus at *Microsoft users*.

   ---

5. **Do you want to** . . .
   - **Move one or more mailboxes to a different level of the hierarchy**? Select the relevant checkboxes, then click **Move**.
   - **Export the data of one or more mailboxes**? Select the relevant checkboxes, then click **Export**. Choose an export format, and click **Export**.
   - **Delete one or more mailboxes (shared or room mailboxes, or distribution groups only)**? Select the relevant checkboxes, then click **Delete**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Add a new mailbox (shared or room mailboxes, or distribution groups only)**?
  - Click the toolbar **Plus** icon.
  - Define a **Display Name** for the new mailbox. The **Mail Name** field automatically updates with an allowed string value of the **Display Name** (for example, no spaces).
  - Select a **Mail Domain**. The **Primary Email Address** using the specified domain is assigned to the new mailbox.
  - Save your changes. Go to step 6 to update mailbox permissions and settings.
- **View or update a mailbox**?
  - Click in the relevant row to open the mailbox management screen.
  - Go to step 6 to update mailbox permissions and settings.

6. Update mailbox settings:

For all mailbox types	You can: • Move the mailbox to another level in the hierarchy. • Update the mailbox display name. On the **Delegation** tab you can set permissions and calendar permissions. To do this, select a mailbox user and assign access rights.
For user mailboxes	• On the **User mailbox** tab you can modify the retention policy and the archive status. • On the **Email forwarding** tab you can choose an option for forwarding all emails to this mailbox. Options are: **None**, **Internal**, or **External** You can then add an internal or external email address, and choose whether to send email to this mailbox and forward to another mailbox (if you've chosen Internal or External). Configuration templates associated with the Quick Add Group allows you to set default values when adding or removing the user. See the following settings in Quick Add Groups: • MS Exchange Online User Mailbox Template • MS Exchange Online Convert Mailbox Template Available fields: • DisplayName: mailbox display name • Permissions • CalendarPermissions: users and their access rights can be managed. • ForwardingAddress: for the Internal forwarding mailbox address. • ForwardingSmtpAddress: for the External forwarding mailbox address. • DeliverToMailboxAndForward: additional setting for the Internal forwarding to deliver to both the user mailbox and the forwarding mailbox. • AutoReplyState: automatic replies are enabled or disabled. • InternalMessage: set internal autoreply message. • ExternalAudience: choose None, contact list, all senders • ExternalMessage: set external autoreply message. • RetentionPolicy: selected policy for mailboxes • ArchiveStatus - for enabling and disabling archiving (Automate contains API operations for mailbox conversion and archiving) • Custom attributes (1 to 15) - you can't update these values in Automate; MS Exchange updates will reflect on the user display form.

Copyright © 2025 VisionOSS Limited. All rights reserved.

For shared mailboxes	• The **Email forwarding** tab offers similar settings to the **User mailbox**, but applied to the shared mailbox. • The **Automatic replies** tab allows you to enable or disable this feature (scheduling not available yet), with options to specify reply messages and audience.
For room mailboxes	• Add or update the **Location** field to define the physical location of the room associated with this mailbox. • Add or update the **Room Capacity** field to define the number of people the room associated with this mailbox holds.
For a distribution group	You can: • Add or update owners • Add or update members (users with access permissions for sending emails as a selected user, or on behalf of a selected user).

Note: Delete is allowed only for shared mailboxes, room mailboxes, or distribution groups.

7. Assign or remove permissions:
   - To assign access or calendar permissions to a user:
     - Click the **Plus** icon at either **Permissions** or **Calendar Permissions** (as applicable).
     - Select the user, and select the relevant permissions.
     - Repeat this step to assign permissions to additional users.
   - To remove access or calendar permissions from a user:
     - Either uncheck permissions assigned to the user, or remove the user entry from the relevant permissions field (**Permissions** or **Calendar Permissions**).
     - Repeat this step to remove permissions from additional users.

Note: Calendar permissions are only relevant for user, shared, and room mailboxes. For distribution groups, only mailbox access permissions are relevant.

When deleting (removing) permissions, the Microsoft cloud portal may take a few minutes to process the update, which may cause a delay for the refreshed data to reflect in the Automate GUI.

8. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Quick Add Groups*

8.2. Webex User Services

8.2.1. User Quick Actions (Webex)

Webex Quick User

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes how to add a Webex App user via Webex Quick User (`view/WebexTeamsSubscriberQas`).

If the **Webex Control Hub Access** setting **Contact Center Customer** is enabled, you can also add a Webex Contact Center agent - see the topic: *Add Cisco Webex App user / Webex Contact Center agent via Quick User* below.

Related topics

- *Quick actions for multi vendor user*
- *Reserve numbers for a user*
- *Manage number filters*

Add Cisco Webex App user / Webex Contact Center agent via Quick User

This procedure adds a Webex Teams user via a standalone view called `view/WebexTeamsSubscriberQas`.

1. In the Admin Portal, go to **Webex Quick User**.

   Note: Some fields are read-only on the form if you're adding or updating a Webex Control Hub user.

2. At **Username**, select the relevant username (existing user) from the drop-down, or fill out a username (new user). To choose an existing user above the current site level, select **Include users at higher hierarchy**, then select a username.

   Note: In a non-directory synced scenario (non-LDAP customer), users with the administrator role are excluded from the **Username** drop-down.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. If you're adding a new user, fill out their first name, last name, email address, and other user details.

Note:

- For directory-synced Webex Control Hub - that is, where the associated Spark customer details have the **Directory Synchronized Enabled** checkbox is enabled:
  - You can't add a new user
  - You can only add an existing user - select the user's email address, then, for example, update the phone number or Quick Add Group
- **Display Name** auto-populates as a read-only value when selecting an existing user's email address that has a first name and last name; else, **Display Name** is optional and is not populated.

4. Choose a number, or select **Use next available line**.

Note:

- When using **Use next available line**, the system prioritizes local numbers (numbers available at the current site), before checking for available numbers from higher levels in the hierarchy.

  The line selected is the next available Webex number from the Webex Control Hub inventory, thus filtering by vendor (Webex Calling) for the Webex Calling user you're adding.

  If used with a line filter (provided filtering is enabled at the current hierarchy), available lines are a subset of lines returned from the line filter.See also *Manage number filters*.
- When **Use next available line** is disabled (checkbox is clear), you can still select a line filter (if enabled) and choose a line from the filtered choices.
- A Webex Calling License is required for phone number type. The Webex API (used for syncing with the Webex Control Hub) only supports add or update for phone number type *Work*.
- For LDAP-synced users, their updated phone number details are written back to the LDAP user.
- Reserved numbers are excluded (numbers reserved for the user you're working with and numbers reserved for other users). See *Reserve numbers for a user*

5. Mandatory. Select a **Quick Add Group**.

Note:

- Available Quick Add Groups are filtered by vendor (see *Quick Add Groups and vendor filtering*) and restricted according to the Global Settings (**General** tab, **Quick Add Group lookup level**, see *Global settings*).
- To add a *Webex Contact Center agent*, a default **Webex Contact Center and Calling Quick Add Group** is provided that can be used or modified to the agent and settings - associated with default configuration templates:
  - **Default Webex Teams User Template with Contact Centre**
  - **Default Webex Contact Centre Template**.

  It is required that the **Webex Control Hub Access** setting **Contact Center Customer** is enabled. See *Introduction to Webex Contact Center* in the Core Feature Guide.
- You can provide Cisco Webex settings via the Quick Add Group.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Cisco Quick User can be used for users with UCM calling or for Cisco UCM users with no UCM calling.

  Note: Cisco Quick User should *not* to be used for standalone Webex users. Use Webex Quick User for that purpose.

- Choosing a **Webex Calling** group allows a user to be assigned a *Webex Calling - Professional* license, enabling management of their calling settings.

  In this Quick Add Group, the configuration template selected in the **Default Webex App Calling Template** is "Default Webex Teams User Calling Template".

  If this Quick Add Group is available in a user profile, then the **Onboard User** (from profile) user management option also allows management of calling settings.

- A **Default Webex App Wholesale for wholesale user** configuration template (`default_webex_app_wholesale_template`) has been added to Quick Add Groups and should be configured in accordance with the required wholesale packages, for example webex_calling. This template must be set for Webex Wholesale customers.

6. If you have email configured you can choose to send a welcome email to the user you're adding. Select **Send welcome email**.
7. Save your changes.

Related topics

- *Manage number filters*

Onboard user (Cisco)

Cisco

Tip: *Use the Action search to navigate Automate*

This procedure adds a user from a profile to enable user onboarding via defined a pre-defined profile determining services and service settings.

1. In the Admin Portal, set the hierarchy to the relevant site.
2. Go to **Onboard User**.

   Note: This page has two tabs/panels:

   - Details
   - Existing Services - read-only, and displays and populates only once you select a username.

   Click the toolbar **Switch to Tab/Panel** icon to toggle between a tab or panel layout.

3. On the **Details** tab/panel, configure the following:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Mandatory. Select the username (mandatory).

  Fields on the **Existing Services** tab/panel display and update to provide a read-only view of the selected user's existing services. If the user has existing dual mode devices, this includes the name and destination for mobile identity, remote destination, and CTIRD remote destination.

  Fields on the **Details** tab/panel updates with the user's details, including name and contact details, and current settings.

- Select the profile for configuring and provisioning the user.

  Note: Profiles are set up at the Provider or Reseller level and vendor-related services in the profile are enabled for each customer in the Global Settings at the customer level.

  The drop-down displays profiles relevant to services enabled by vendor for the customer in the Global Settings. For example, a customer enabled only for Webex services will only have profiles available in this drop-down for Webex services, while a customer enabled for both Cisco and Microsoft services will have profiles that include both Cisco and Microsoft services.

  Services are assigned via the profile and display as read-only details once you save.

- Fill out the user's details. You can update their first name, last name, email address, mobile number.

  Note: A value for **Last Name** is mandatory only for CUCM users, and optional when provisioning Microsoft or Webex Calling services.

  Password and PIN fields become available once the profile is selected, as follows:

  – For an LDAP user: only the PIN field will be available
  – For a CUCM-LDAP user: only the PIN field will be available
  – For a Microsoft user: PIN and password fields will *not* be available
  – For a Webex user: PIN and password fields will be available
  – For a Local/CUCM-local/None-existing user: PIN and password fields will be available

  Note:

  – The corresponding CUCM, CUC, and Webex user password will be set with this password.
  – The corresponding CUCM and CUC user PIN will be set with this PIN.

- At **Use generated phone name**, if the selected profile has voice service enabled, define whether to have the system generate a random phone name.
- At **Line filter**, select a number inventory filter, if available. If you're not selecting **Use next available line**, you can choose a number from the subset of lines returned by the line filter.

  Note: You can only choose an inventory filter if filtering is enabled at the site. Either custom filters or shipped filters, or all enabled filters may be available, depending on the filter group enabled at the hierarchy. See *Manage number filters*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- At **Use next available line**, define whether to use the next available line from the inventory or from an inventory filter you choose.

  Note:

  - When using **Use next available line** functionality, the system prioritizes local numbers (numbers available at the current site) before checking for available numbers from higher levels in the hierarchy. If the user has *reserved numbers*, these are excluded and won't be applied as the *next available line*.
  - When using inventory filters with **Use next available line**, the system selects the first available number in the subset of filtered available numbers from the filter. If you've chosen a line filter to display only *used* lines, the system won't find a next available line since only used lines are returned for your chosen filter you've chosen. In this case, the transaction will fail with "no available lines".
  - Numbers reserved for other users won't be available, regardless of their status (available or used, reserved, etc). If an inventory filter is applied to display only numbers reserved for or belonging to the user you're working with, only those numbers display.

9. Save your changes.

Related Topics

- *User profiles*
- *Multi vendor users*
- *Reserve numbers for a user*
- *Manage number filters*

8.2.2. Device Quick Actions

Replace device

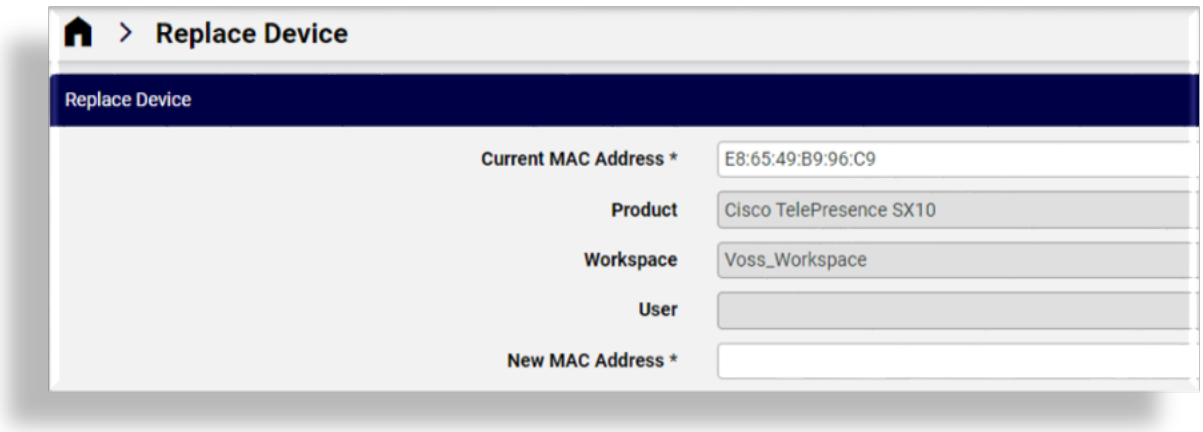
Tip: *Use the Action search to navigate Automate*

On the **Replace Device** page you assign a new MAC address to an existing Cisco Webex ATA, MPP, or Wi_Fi device, and to copy the configuration of the existing device (including user or workspace assignment) to a replacement device.

This allows you to easily replace a faulty or failed device without having to manually complete all of the configuration settings for a replacement device.

Select the current MAC address to auto-populate the form, then fill out the new MAC address, and save.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related Topics

- *Quick Add Webex Device*
- *Webex devices*
- *Webex Workspaces*

Reset devices to baseline

Tip: *Use the Action search to navigate Automate*

Overview

Webex meeting room device users may regularly change device settings throughout the day, for example, to change the volume, or camera settings. Since custom settings could impact future meetings, it may be considered good practice to regularly reset and clear device settings to their baseline configuration (standard settings).

In the Admin Portal you can set up a regular schedule for resetting Webex-registered meeting room devices, which will typically execute daily (before the start of the working day), or reset one or more devices manually, as required.

Reset schedules are configured via the **RoomOS Reset Schedule** page.

Alternatively, you can manually reset active devices, via the **Reset Devices to Baseline** page.

You can view all registered (active) devices via the **Devices** page for Webex App. You can add devices when adding a new workspace or when updating an existing workspace.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manually reset a RoomOS device

1. In the Admin Portal, go to **Reset Devices to Baseline**.
2. Choose the device scope (refresh action). The table describes the available options:

Refresh Single Device	Choose one active device from the list that displays when you select this option.
Refresh Multiple Devices	Choose from the list of active devices that display when you select this option.
Refresh All Devices	Resets all active devices.

3. Choose a device configuration profile for resetting the device.
4. Fill out your username and password.
5. Click **Save**.

   The device configuration profile resets the selected active devices (one, more, or all, depending on the option you selected for device scope).

Schedule RoomOS device reset

This procedure requires:

- Customization: the cloning to a required hierarchy and modifying of the **Reset Device Schedule Configuration Template**
- The setup of the **Webex Schedule**.

Reset device schedule configuration template

The **Reset Device Schedule Configuration Template** page lists a default instance of `WebexDeviceRefreshSchedule_CFT` that is to be cloned to the required hierarchy and modified:

- Device scope
- Devices
- Device profile
- Any associated usernames and passwords for devices

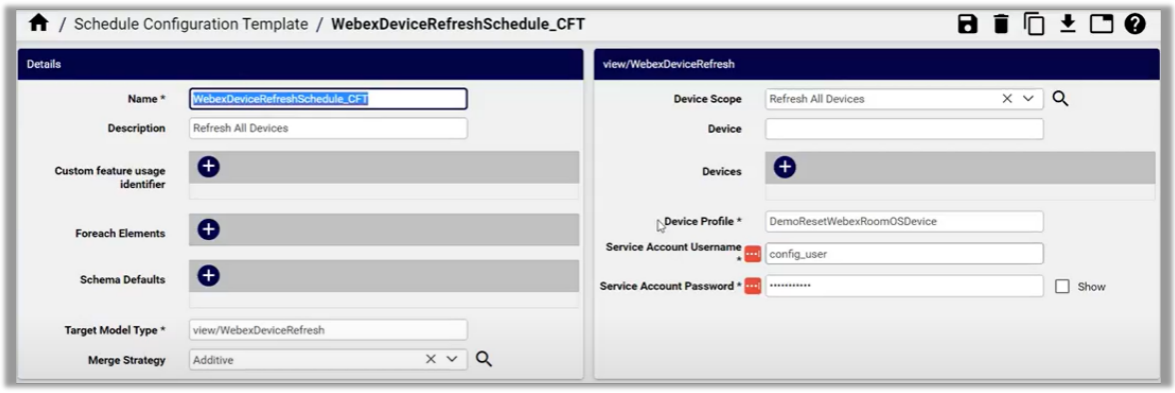
1. In the Admin Portal, go to **Reset Device Schedule Configuration Template** list view.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Click on the schedule you want to use.

   The schedule configuration template contains a workflow that is executed by the reset schedule. The default schedule configuration template name is `WebexDeviceRefreshSchedule_CFT`.

3. On the schedule configuration page, choose the device scope, and the device configuration profile to use.

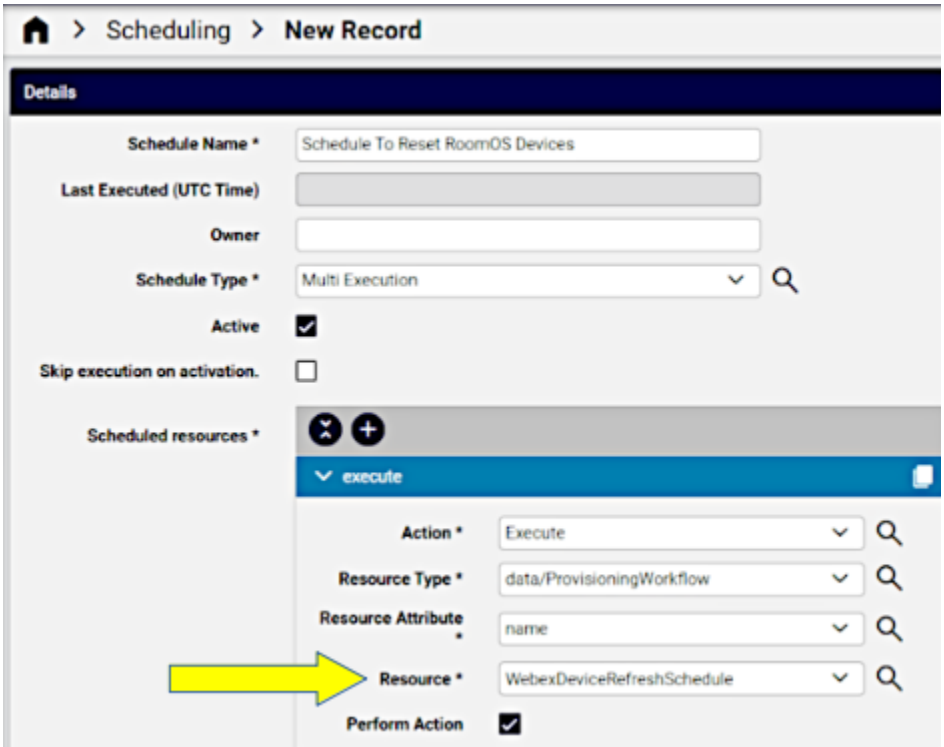


4. Fill out the username and password that has access to the devices.
5. Save your changes.

Webex schedule

When setting up the schedule, the **Resource** field is specified as `WebexDeviceRefreshSchedule`, which will reference the configured instance of `WebexDeviceRefreshSchedule_CFT`.

Copyright © 2025 VisionOSS Limited. All rights reserved.



1. Go to **Webex Schedule**.
2. On the schedule form, create the schedule, and at **Scheduled resources**, at the **Resource** drop-down, choose the schedule (`WebexDeviceRefreshSchedule`).
3. Save your changes.

Devices will be refreshed according to the schedule and the workflow defined in the schedule configuration template.

Quick Add Webex Device

Overview

You can add Webex App ATA, MPP, and Wi-Fi devices using **Quick Add Webex Device**. This tool uses a configuration template with pre-configured settings to add these devices and associate them with users and existing or new workspaces.

Note: For the selected **Person** on the GUI, only users with numbers and pre-provisioned with a Webex Pro license are available.

Quick Add Webex Device can also be used to replace an existing device.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Webex devices*
- *Webex Workspaces*
- *Replace device*
- *Configuration templates*

8.3. Cisco User Services

8.3.1. User Quick Actions (Cisco)

Cisco Quick User

Tip: *Use the Action search to navigate Automate*

Overview

Cisco Quick User provides a single page where you can add a Cisco UCM user with a line, a voicemail, and a Webex account, and provision the user with services such as voice, extension mobility, single number reach (SNR), and conferencing and collaboration services.

Important: Cisco Quick User is a simple, generic method for provisioning users that applies single values from configuration templates (via Quick Add Groups), and the site defaults.

For more complex provisioning requirements, such as adding route partitions or multiple values for other service fields (such as two or more lines), use Automate's advanced user management functionality (**Cisco Advanced User**), or bulk loaders. For example, you could use Cisco Quick User to add users with only the first line on phones, then use advanced user management to add the second line to the phone.

For details around how Quick Add User handles the application of a Line configuration template associated with a selected Quick Add Group (QAG) when adding or updating a user, see *Shared lines*.

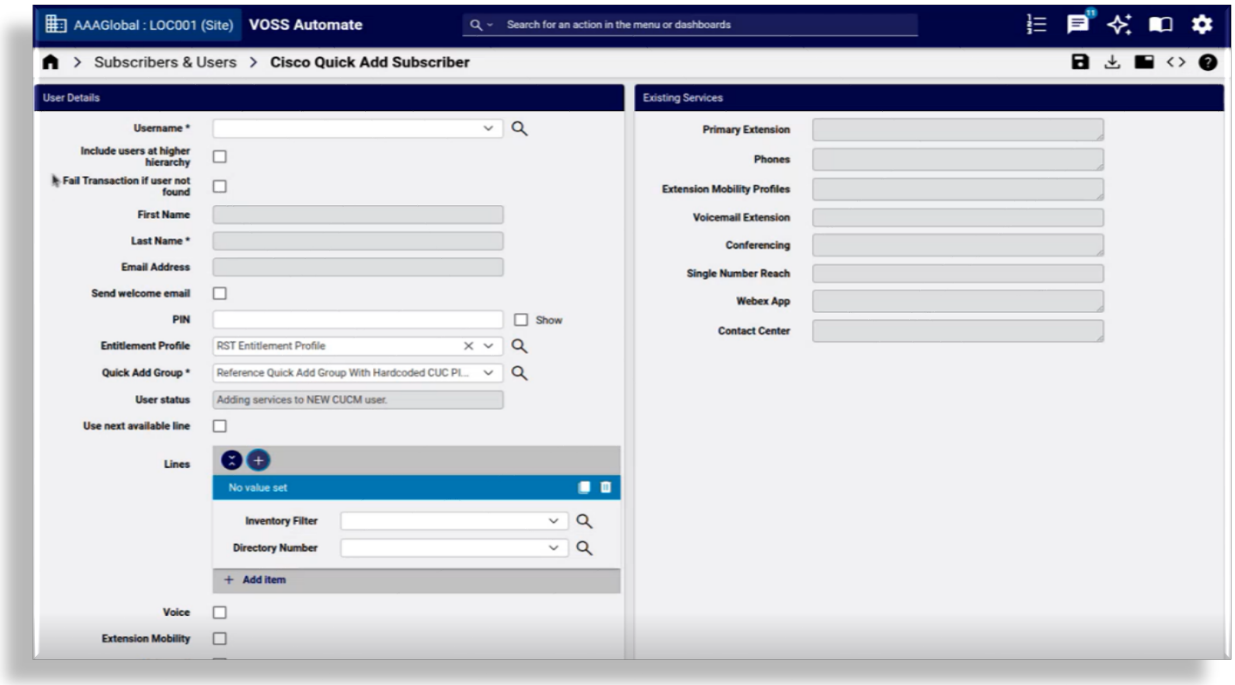
Supported User Types

Quick Add User for UCM users supports several user types, including:

- LDAP users
- UCM-integrated users
- LDAP-integrated users on UCM
- Manually created users

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: If the default Self-service Language is set on the site default docs (SDD), users are assigned the corresponding Self-service language.



Related topics

- *Provisioning users with Cisco Webex*
- *Cisco Quick User Class of Service*
- *Provision the Voice Service*
- *Quick Add Groups, default model*
- *Configuration templates*
- *Expose device pools and Class of Service in Cisco Quick User*
- *Add Webex App service using Quick Add User*
- *Provision the extension mobility service*
- *Provision the Pexip Conference service*
- *Provision the Jabber or dual mode device service*
- *Provision a Contact Center agent*
- *Enable self-provisioning*
- *Reserve numbers for a user*
- *Manage number filters*
- Global Settings in the Core Feature Guide.
- Introduction to Entitlement in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure Cisco Quick User

To create or configure users, to enable users with services, or to associate users with devices, configure the following items on the system:

Configuration	Description
1. Configure servers	Configure the following servers in Automate: • Cisco Unified Communications Manager (UCM) server Adding a UCM server allows the following: – Syncing of manually provisioned users or LDAP-integrated users in UCM to Automate – Syncing in of users phones, directory numbers, extension mobility profiles in UCM to Automate – Creation of users (push users to UCM) – Pushing of users' associated phones, directory numbers, and extension mobility profiles, to UCM. • LDAP server Required only if you want to configure LDAP-synced users in Automate, else, optional. • Cisco Unity Connection (CUC) server Required only if you want to add CUC voicemail users that are configured in Automate.
2. Configure dial plans	Provider deployment only. Configure a dial plan at both the customer and site hierarchies.
3. Configure voicemail service	Deploy voicemail service with a pilot number created and associated to a site in Automate (via the **Voicemail** page). This step is required to create a "Default CUC User Template" (via the **Site Defaults** page for CUC. The template is required to create CUC voicemail users.
4. Configure Webex service	Configure a Webex Server in Automate to deploy any Webex users provisioned through Quick Add User. Set a password for Webex users in the Site Defaults.

Add a user via Cisco Quick User

This procedure adds a UCM user via Cisco Quick User.

Prerequisites:

- Configure **Phones** settings in the Global Settings to select phones by their description or description and line.
- Default user template (`voicemailusertemplate`) must exist on UCM. You can update the default by editing the default CUC User Template value in the SDD.
- Configure Quick Add Groups. See *Quick Add Groups*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: For details around how Quick Add User handles the application of a Line configuration template associated with a selected Quick Add Group (QAG) when adding or updating a user, see *Shared lines*.

- If required, expose device pools and Class of Service (CoS) in Quick Add User. See *Expose device pools and Class of Service in Cisco Quick User*
- Ensure site defaults are correctly configured.
- Enable filtering at the hierarchy to use inventory filters. See *Enable/disable filtering*.

Add user via Quick Add User

1. In the Admin Portal, go to **Cisco Quick Add User**.

   Note:

   - You can switch between a tab or panel layout on this form.
   - The **Existing Services** tab/panel displays devices and services associated with the user you choose. If the user has existing dual mode devices, the **Phones** field includes details for mobile identity, remote destination, and CTIRD remote destination. Existing services are associated with services enabled/disabled at the customer level via the Global Settings.

2. Configure user details on the **User Details** tab/panel:

   Note: LDAP-synced or LDAP-integrated at UCM user fields are read-only.

   - Mandatory. Select the username.
   - If the username you require doesn't exist at the current site, select **Include users at higher hierarchy** to add users above the current site.

     Note:

     – You can only edit existing UCM users via Quick Add User if these users exist at site level.

     – The field associated with this checkbox (`lookUpForUser`), is hidden by default. You can expose it via a custom field display policy. This setting is also available for bulk load sheets and API calls.

   - To prevent adding users that don't exist on UCM, select **Fail Transaction if user not found**.

     Note: The field associated with this checkbox (`failIfNotFound`) is hidden by default. You can expose it via a custom field display policy.

     By default, the transaction won't fail. This option is used when users have not been synced from LDAP to UCM. This setting is also available for bulk load sheets and API calls.

   - Mandatory. Fill out a first name and a last name.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: First name is mandatory only if you're provisioning the user with a Webex account. You can set only one Webex account per user. The first name and last name is auto-populated as a display name on the Webex user record. The display name is used when making Webex calls.

- Optionally, fill out an email address. If you wish to send the user a welcome email, select **Send welcome email**.

  Note: *Send welcome email* displays only once you add an email address, provided you have the following enabled and configured:

  – SMTP server must be set up (*Add a SMTP Server*)

  – In the Global Settings (Email tab), enable (for the relevant hierarchy) **Allow email to be sent to user after Quick Add User**. See *Global settings*

  A welcome email is sent to the user email address using the configured "Quick Add User" HTML email template that applies to the hierarchy. See *Email*.

- Fill out a PIN.
- Choose an entitlement profile, if one exists, to associate with the user you're adding.
- Choose a Quick Add Group (QAG), or select the default.

  Note: Quick Add Groups are filtered by vendor (see *Quick Add Groups and vendor filtering*), and are restricted to those available at a selected hierarchy, based on the option selected for **Quick Add Group & Subscriber Profile lookup level** in the *Global settings* (**General Settings**).

- Choose a device pool.
- At **Use next available line**, if you want to enable this functionality (disabled by default), select the checkbox.

  When enabled:

  – The system prioritizes local numbers (numbers available at the current site) before checking for available numbers from higher levels in the hierarchy.

  – Reserved numbers are excluded (numbers reserved for the user you're working with and numbers reserved for other users).

  – If filtering is also enabled at the hierarchy, select an inventory filter to have the system choose the first available line it finds from the filtered list of numbers. If filtering is disabled, the system automatically selects the next available line.

  When disabled:

  – If filtering is enabled at the hierarchy, select the inventory filter, then select the line from the **Directory Number** drop-down.

  – If filtering is disabled, select a number from the **Directory Number** drop-down.

  For details around how *Use next available* lines integrates with inventory filters, see *Inventory filters and "Use next available line"*.

  Note: You can create directory numbers in UCM in two ways:

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Create a voice mail line in Quick Add User
  - Create a line in Quick Add User

  When creating a voicemail or voicemail line using Quick Add User, the **Directory Number Used** field is set to “true” in the **Number Inventory**. A directory number created without any device associations (for example, a voice mail line), is tagged in the user **Lines** page as *DN created without device from QAS*’.

- Select services:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Service	Description
Voice	Provisions the voice service. Since you can create multiple devices for a user, this checkbox is always available. Selecting the Voice service displays these additional fields: – **Phone Type** (Lists phone types allowed by the entitlement profile, if one exists, else, phone type is retrieved from the QAG) – **Phone Protocol** – **Phone Button Template** (You can override the default phone button template value by entering a custom value in this field. However, the new value is only applied on the UCM if allowed for the phone type.) – **Phone Security Profile** – **Phones** Add one or more phones. You can associate a line with multiple phones, and you can associate a phone with multiple lines. The **Phone Name** drop-down lists available phones at the user's site, based on the phone type specified in the SDD for this site, in the associated QAG at the customer level, or synced from UCM. To add a new phone, you can enter a valid name in the **Phone Name** field. The phone name must consist of a prefix, for instance *SEP*, followed by a MAC address (12 hexadecimal characters). The transaction will fail if you enter the phone name incorrectly (for example, too few or too many characters). Choosing alternative options in these fields overrides values set up in the Quick Add Group (QAG), configuration template (CFT), site defaults document (SDD), or any other backend (read-only) CFTs. If the QAG does not specify a phone template, or if the specified phone template has blank values for the phone fields, the phone field values are pulled from the SDD. To avoid conflicting Quick Add User settings, it is recommended that you configure settings on the Quick Add User page in the following order: 1. Entitlement Profile (only if these exist on the deployment, and are associated with the user) 2. Quick Add Group 3. Voice (then choose phone type, phone protocol, phone button template, and phone security profile)
Extension Mobility	Provisions extension mobility. Only one extension mobility profile per user, so the checkbox displays only until you create an extension mobility profile.
Voicemail	Provisions voicemail service.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Service	Description
Single Number Reach	Provisions single number reach (SNR) service, and allows you to specify the SNR mobile number. If a mobile number is already configured for a user, it is used to pre-populate the Mobile Number field when adding SNR for that user. You can enter a different mobile number for SNR, if required. SNR mobile numbers are formatted with a Plus (+) and the number, for example *+99218732876*. SNR mobile numbers cannot include include spaces, dashes, or other special characters. The SNR mobile number can be the same as the user's number that displays on the **Users** page.
Jabber / Dual-Mode Device	Provisions Jabber / Dual-mode device service, and allows you to add Jabber and Dual-Mode devices. You can associate multiple Jabber and Dual Mode devices to a user. Jabber and Dual Mode devices get the first line assigned to them (specified in Quick Add User).
Enable self-provisioning	Defines whether to enable self-provisioning for this user, and allows you to choose the relevant self-provisioning user profile. When enabled, phone lines are added using the Universal Line Template (ULT) referenced in the selected self-provisioning user profile. When adding a user with lines but no devices, or when adding a user with devices and lines, enabling self-provisioning here automatically sets the *UCM User Primary Extension* to the Quick Add User line pattern and ULT route partition. Existing self-provisioning user profiles display on the **User Profile** page, (and can be seen in the site's Site Defaults). You can change this default, if required.

3. Save your changes. The user is added.
   - If you've provisioned SNR (single number reach), verify, on the **Existing Services** tab/panel, that the **Single Number Reach** field displays the SNR profile name, which is the user name, followed by *"-RDP"*. For example: *jsmith-RDP*.
   - If you wish to update a user or their associated services (after adding the user via Quick User), this is done from the relevant service menu items.
   - For self-provisioned phones to show as being associated with a user, perform a UCM data sync after setting up a self-provisioned phone.

Related Topics

- *Reserve numbers for a user*
- *Global settings*
- *Manage number filters*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Enable services in Cisco Quick User

When adding a user via Cisco Quick User, you can enable user services, such as voicemail, extension mobility, single number reach, conferencing (meetings), and collaboration (messaging) services (such as Webex App).

The Quick Add User page displays services included in a selected entitlement profile (if entitlement profiles are used). For example, if the entitlement profile excludes voice services, the checkboxes for Voice, Jabber, and Self Service ID won't appear on the page. The selected entitlement profile also filters options available in the **Phone Type** drop-down (showing only devices enabled in the entitlement profile).

Note: It is possible to use Cisco Quick User to add a user without an entitlement profile. For example, entitlement profiles may not exist on the deployment, or they may not be associated with the user. In this case, a phone type, for example, may still be associated with the user via the Quick Add Group (QAG).

For the Voicemail service:

- Configuration settings are only available if the site's SDD has a default value on the CUC Defaults tab for the Default CUC User Template.

  The default value (`voicemailusertemplate`) should already exist on the UCM and is automatically populated on an HCS system when a voicemail pilot is created.
- A CUC device must be configured at the related Network Device List (NDL), at site level.
- If the selected QAG specifies any CFT entries for UserPin or UserPassword, these are applied. Otherwise, the values from the User Template defined on CUC apply. For default CFTs, see: *Quick Add Groups, default model*.

While the Admin Portal hides configuration settings for unavailable services, API and bulk load operations have provisioning workflow checks that check for the presence of the Default CUC User Template in the SDD and a configured Webex server in the NDL, before the selected services can be added.

A UCM (call manager) must be configured at the user's hierarchy. If this does not exist, the Quick Add User bulk load transactions and API calls display the following warning: *No Call Manager has been configured*

Add Webex App service using Quick Add User

Note: When using Quick Add User to provision WebexApp services, the SiteDefaultsDoc - **User Defaults** tab values should be set to either:

- **Webex App - Use Organization's Domain** = True

or

- **Webex App - UC Manager Profile** = <Selected UC Profile>

Selecting the **Webex App** checkbox on the Quick Add User page displays the **Webex Teams User Template** drop-down, where you can select a **Webex Teams User Template** to apply to the user.

- Choosing a template from the drop-down overrides the default user template referenced in the Quick Add User Group (QAG) associated with the user.
- If you don't select a **Webex Teams User Template** from the drop-down, the **Webex App User Template** referenced in the associated QAG is applied.

Copyright © 2025 VisionOSS Limited. All rights reserved.

If you want customized values, clone the **Webex Teams User Template** (**Customizations > Configuration Templates**) and edit as required. The Webex Teams User Template for UCM Calling provides for a **Settings** group of controls for the specification of Calling Behavior and provisioning of Jabber devices if relevant to the calling behavior.

Add a Contact Center agent using Quick Add User

- *Contact Center*

You can use Quick Add User to create a Contact Center (UCCX) agent.

The **Contact Center Agent** checkbox displays if:

- The associated Entitlement Profile has Contact Center enabled
- A Contact Center Server is available at the hierarchy.

  See *Configure UCCX server* in the Core Feature Guide.
- The selected user is not already associated with an Agent

If the checkbox is selected:

- A **Contact Center Agent Profile** drop-down list is available to select an agent profile.

  Note: The **Contact Center Agent Profile** needs to be created before adding the Contact Center Agent from the Quick Add User feature.

  The agent profile will determine the team, resource group and skills assigned to the newly created agent. See *Agent Profiles*.
- The **Agent Extension** can be selected.

  The extension will be a list of specified Lines, in other words, the administrator must specify the Line to be created or reused before selecting the **Contact Center** check box.
- The **Agent Device Type** can be selected: either Extension Mobility or Phone:
  - If Extension Mobility is selected, the **Extension Mobility** check box is automatically enabled.
  - If Phone is selected, the administrator must first enable **Voice** and specify a Phone to be created or reused before selecting the **Contact Center** check box.

An IPCC extension is automatically managed for the UCM user associated with the Contact Center agent.

Quick Add User device pool

When adding a user via Cisco Quick User, you can associate a device pool to the user's newly associated devices or services (other than the device pool provided in the Site Defaults Doc or referenced configuration template in the Quick Add Group).

A device pool contains system, device, and location-related information, and is mandatory when adding a user using Cisco Quick User.

A device pool can be referenced by:

- Site Defaults Doc (SDD)
- Reference Configuration Template (CFT) referenced in the Quick Add User Group (QAG)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Admin Portal (if exposed)

Device pool and Site Defaults Doc

The device pool referenced in the SDD ensures that a user's devices are always associated to a device pool. If there is no device pool referenced in either the QAG or Admin Portal drop-down (see below) the value defaults to the SDD.

Device pool and Quick Add Group

The device pool referenced by a Configuration Template (CFT) in the QAG takes precedence over the device pool referenced in either the SDD or the Admin Portal drop-down (if exposed). See Quick Add Groups for details.

Device pool and Admin Portal

An administrator can expose a **Device Pool** drop-down on the Quick Add User page on the Admin Portal by editing or cloning the Field Display Policy. See *Expose device pools and Class of Service in Cisco Quick User*. The **Device Pool** drop-down allows an administrator to overwrite the value in the SDD by selecting a custom device pool from the drop-down list. The options available in the list are the site-level device pools if they are available, otherwise it displays all device pools available at customer level (NDLR aware).

Note:

- Where multiple device pools are available at a site, a load balance check is available on the number of phones using the Device Pools in order to assign the phone to the least used device pool. Contact VOSS if this load balance check is required.
- When exposing the **Device Pool** drop-down, the administrator **must** remove the value in the **Device Pool** field of the CFT referenced in the QAG, that is, the field must be blank. This is done to ensure that the value in the CFT does not overwrite the custom value in the drop-down.

  The CFTs and their target models for which the device pool name can be made blank to allow the Portal to drive the device pool selection include:

  - Phone templates (device/cucm/Phone)
  - Jabber device templates (device/cucm/Phone)
  - Remote Destination Profile templates (device/cucm/RemoteDestinationProfile)

Cisco Quick User Class of Service

With Cisco Quick User you can associate Calling Search Space (CSS) values to a user's newly associated lines, devices, or services (other than the CSS's provided in the Site Defaults Doc or referenced configuration template in the Quick Add Group), by selecting a Class of Service (CoS).

A Class of Service (CoS) allows you to specify a Calling Search Space (CSS) for devices and lines. A CSS is mandatory for lines and devices when adding a user using Quick Add User.

A CSS can be referenced by:

- Site Defaults Doc (SDD)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Reference Configuration Template (CFT) referenced in the Quick Add Group (QAG)
- Admin Portal, via the Class of Service field (if exposed)

Class of Service and Site Defaults Doc

The Calling Search Space values referenced in the SDD ensure that a user's lines and devices always have a Calling Search Space associated to it. If there are no Calling Search Space values referenced in either the Quick Add Group or via the Class of Service field in the Admin Portal drop-down (see below) the value defaults to the SDD.

Class of Service and Quick Add Group

The Calling Search Space values referenced by a Configuration Template (CFT) in the Quick Add Group take precedence over the Calling Search Space values referenced in either the SDD or the Class of Service via the Admin Portal drop-down (if exposed). See Quick Add Groups for details.

Class of Service and Admin Portal

An administrator can expose a **Class of Service** drop-down on the Quick Add User page on the Admin Portal by editing or cloning the Field Display Policy. See *Expose device pools and Class of Service in Cisco Quick User*. The **Class of Service** drop-down allows an administrator to overwrite the Calling Search Space values in the SDD by selecting a custom Class of Service from the drop-down list. The Class of Service, in turn, contains a custom Calling Search Space for lines and devices, respectively. The options available in the list are the customer-level Class of Service instances, as created by the relevant administrator.

Note: When exposing the **Class of Service** drop-down, the administrator **must** remove the values in the Calling Search Space fields of the CFT's referenced in the QAG, that is, the field must be blank. This ensures that the value in the CFT does not overwrite the custom Calling Search Space value as defined in the selected Class of Service.

The CFTs and their target models for which the Calling Search Space name can be made blank to allow the Portal to drive the Calling Search Space values include:

- Line templates (device/cucm/Line)
- Phone templates (device/cucm/Phone)
- Jabber device templates (device/cucm/Phone)
- Remote Destination Profile templates (device/cucm/RemoteDestinationProfile)

Expose device pools and Class of Service in Cisco Quick User

This procedure exposes the **Device Pools** field and **Class of Service (CoS)** field on the Cisco Quick User form, at a specified hierarchy.

Pre-requisites:

- You must be logged on as an administrator with access to Field Display Policies (FDP)

Perform these steps:

1. In the Admin Portal, go to **Field Display Policies**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Filter the **Target Model Type** on `view/QuickSubscriber`.
3. Choose an option, depending on the hierarchy where the **Device Pools** or **Class of Service** fields should be exposed in Cisco Quick User:
   - **The FDP exists at the correct hierarchy**? Click on the FDP to open it.
   - **The FDP does not exist at the required hierarchy**? Clone one of the FDPs at a hierarchy above the required hierarchy.
4. Open the FDP to edit it, and go to the first group's **Available** list in the **Fields** block.
5. Select **device_pool** or **class_of_service**, then click the **Move** icon to move the **device_pool** or **class_of_service** from the **Available** list to the **Selected** list.
6. Use the **Move up** and **Move down** icons to move the label to the desired position relative the the other field labels.
7. Ensure that the cloned FDP name is "default", then click **Save**.
8. If you're at the hierarchy where the cloned FDP is created or at a lower hierarchy, go to **Cisco Quick User**, where you will see the relevant field exposed (either **Device Pools** or **Class of Service**).

Provision the Voice Service

This procedure provisions a voice service to a subscriber.

1. Go to **Subscriber Management > Quick Add Subscriber**.
2. Select a user from the **Username** drop-down; then, select the **Voice** checkbox.
3. Optionally, select phone details in these fields:
   - Phone Type
   - Phone Protocol
   - Phone Button Template
   - Phone Security Profile

   Note:

   - To prevent conflicting QAS settings, fill out the optional fields in the order displayed on the form.
   - Default values depend on the selected Quick Add Group (QAG). New values you define for the optional fields override existing values in QAG, CFT (configuration template), and in any other backend (non-editable) CFTs. The system populates any fields left blank with values from QAG, CFT, SDD (Site Defaults Document), or other backend CFTs.
   - The template you select (for example, 'Phone Type'), must exist in the QAG and must be allowed by the entitlement profile, which filters the **Phone Type** drop-down to display only devices enabled by this profile.
   - If a phone button template is not specified in QAG, or if the specified phone button template has blank values for the phone fields, the phone field values are pulled from the SDD.

     To override the default phone button template, enter a new value in the **Phone Button Template** field. The new value is applied on Unified CM, if it allows the phone type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. Required. In the **Lines** section, select a line from the **Directory Number** drop-down.

   Note: The line must be one of the directory numbers in **Subscriber Management > Directory Number Inventory**.

5. Required. In the **Phones** section, select a phone from the **Phone Name** drop-down.

   Important:

   - Phones available in this drop-down are:
     - In the assigned Quick Add Subscriber Group, which have possibly synced from Unified CM
     - Available at the specific site
     - Not currently owned by any other user

       Note that the ability to associate an existing, un-associated phone to a subscriber using Quick Add Subscriber (QAS) depends on the Global Settings setup for Phones.
   - If you wish to add a new phone, enter a valid name in the **Phone Name** field. Ensure you enter the phone name correctly (including the correct number of characters).

     The phone name must have:
     - A prefix (such as SEP)
     - A MAC address (12 hexadecimal characters)

   To add more phones, repeat this step until you have all the phones you need.

6. Click **Save**.

See also:

- *Global settings*

Provision the extension mobility service

Tip: *Use the Action search to navigate Automate*

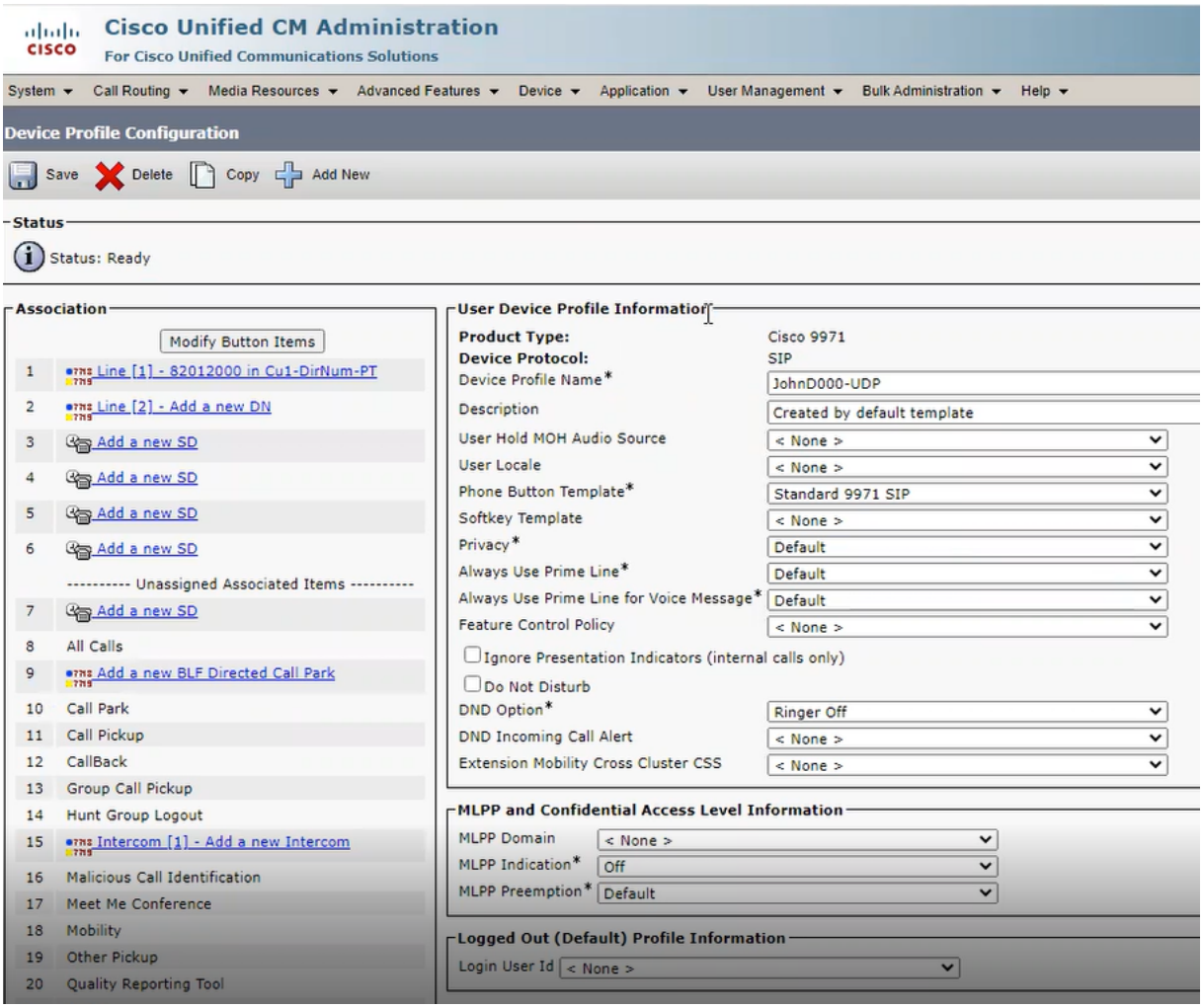
Overview

In Automate, enabling extension mobility via Quick Add Subscriber (QAS) creates a device profile for the user on CallManager (the call processing component of CUCM).

A CUCM user device profile may be considered a dummy phone with lines. When the user logs in to a physical phone associated with the CallManager and enters their username and pin, CallManager applies their device profile to the phone (with their line, settings, and extension number), effectively assigning ownership of the phone to the user for the period they're logged in.

Provided a user is logged in to a physical phone via their device profile username and pin, they're always reachable via the extension number assigned to their device profile, regardless of the physical device they're using. The user's extension number is associated with their device profile and not to a physical device and is thus always 'mobile'.

Copyright © 2025 VisionOSS Limited. All rights reserved.



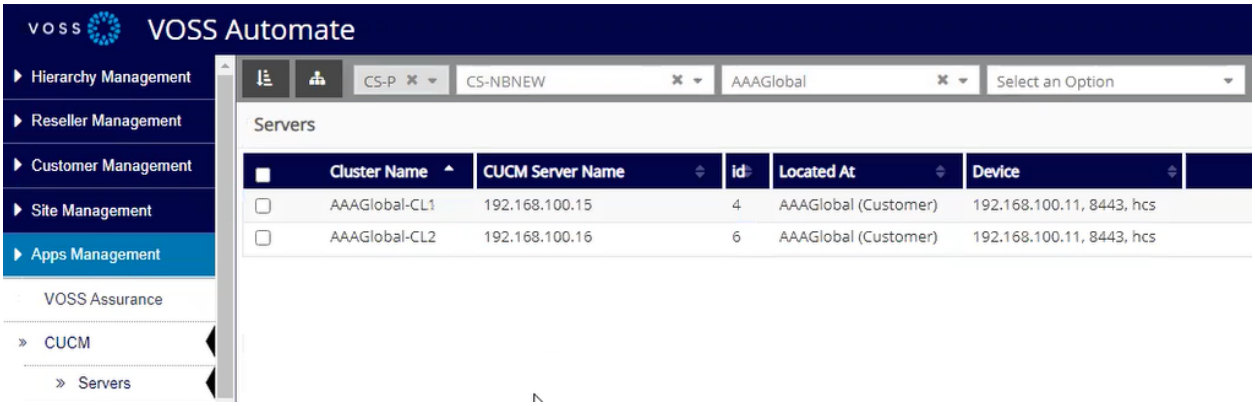
Related Topics

- Introduction to EMCC in the Core Feature Guide
- Configuration Templates in the Core Feature Guide
- Extension mobility in the Core Feature Guide

EMCC and Multi-Cluster CallManager

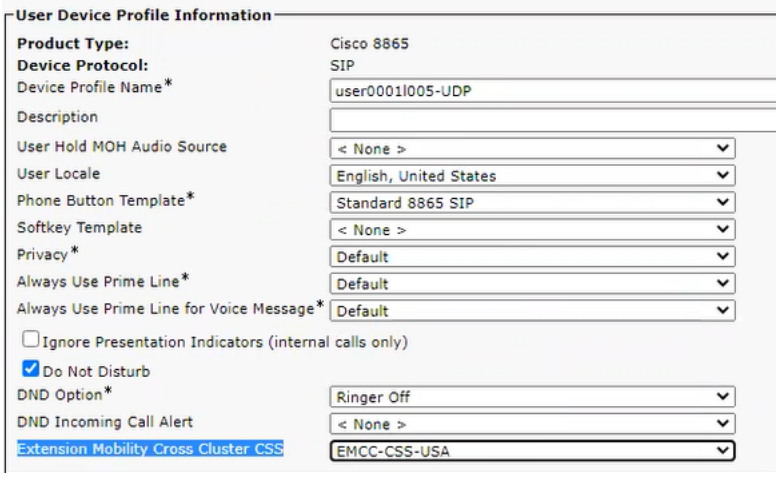
A large organization (set up at the Automate Customer hierarchy) may have multiple CallManager clusters (separate CallManager servers in a multi-cluster setup). For example, a CallManager cluster located in London (providing phones and services to the London office), and a CallManager cluster located in New York (providing phones and services to the New York office). In this scenario, CallManager allows inter-cluster calls between these locations; each CallManager has a different IP address, and each has different data (the phones, users, and services, for either London or New York, in this case).

Copyright © 2025 VisionOSS Limited. All rights reserved.



A CUCM administrator configures cross-cluster via the CUCM Extension Mobility Cross Cluster (EMCC) feature settings on CUCM, and in Automate (via the **EMCC** page).

Once configured on CUCM, EMCC may be enabled per user in CUCM, and a EMCC calling search space (CSS) is chosen for the user device profile.



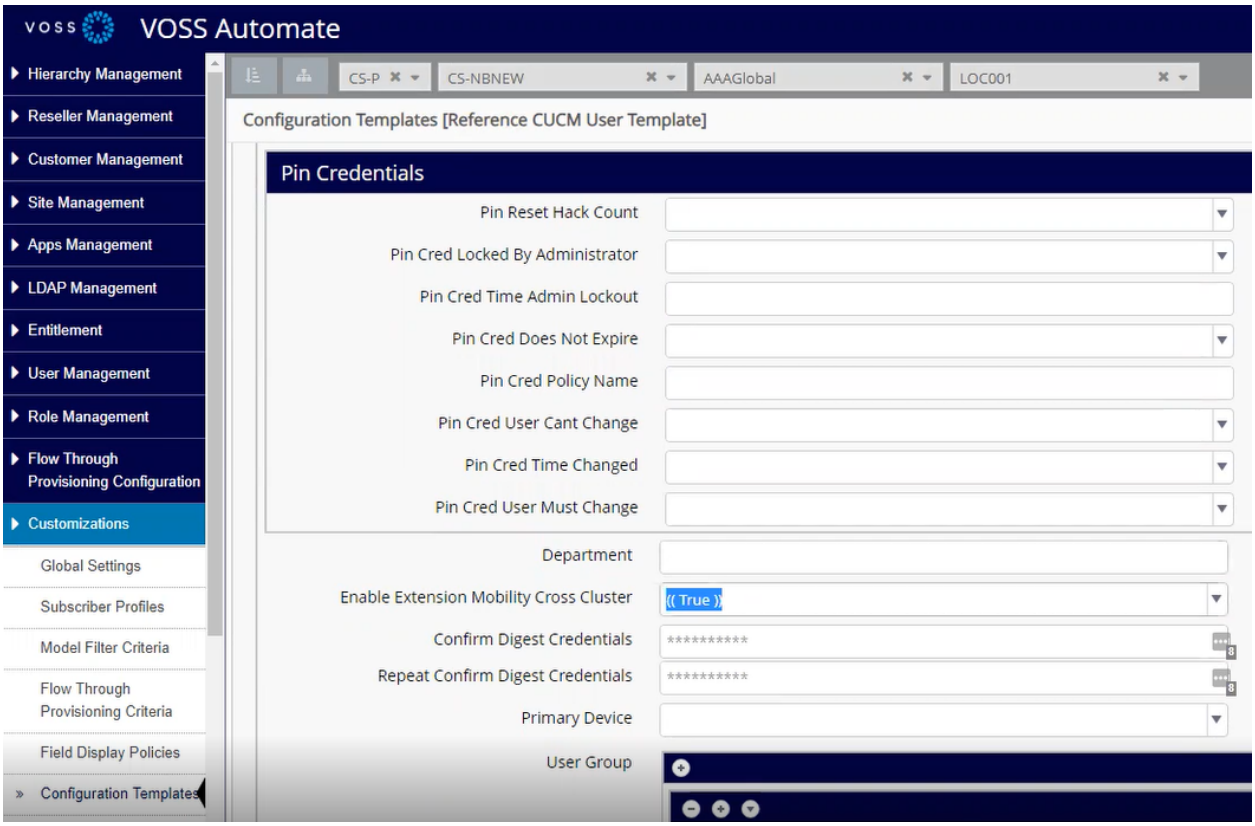
Note: In Automate, EMCC groups define the clusters and countries to be used together for extension mobility. When saving an EMCC group, Automate creates the relevant route partitions, device pools, and the CSS related to the countries selected for the EMCC group.

A user enabled for EMCC can use their extension at another location that is part of the cluster. For example, a user can log in to a desk phone in London in the morning, travel to New York, and log in to a desk phone at the New York office when they arrive. Regardless of their physical location, the user remains reachable via the same extension number, provided they're logged in to a physical phone in a connected cluster, using their home cluster device profile username and pin.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick Add Subscriber and Configuration Templates

QAS references a selected QAG, which contains a number of configuration templates that define values for various settings. For example, the CUCM user template, or the extension mobility template (which defines the user device profile settings). For example, you can assign to the QAG, a CUCM user template that has **Enable Extension Mobility Cross Cluster** set to *True*, so that all subscribers added via QAS with this QAG are automatically enabled for EMCC.



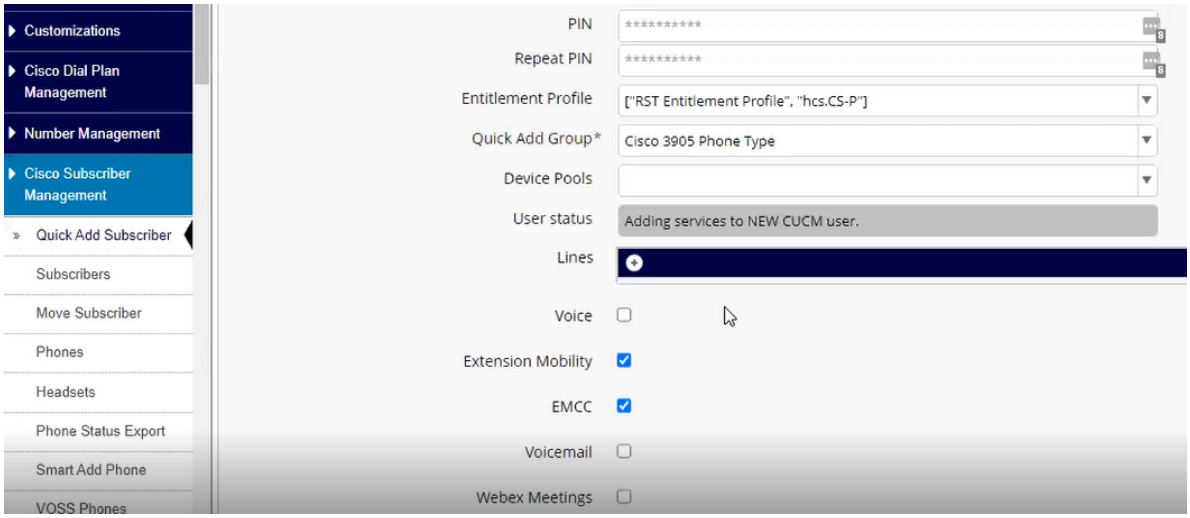
Device Profiles and Extension Mobility Profiles

A CallManager device profile is called an extension mobility profile in Automate. Device profiles are configured in Automate via device profile configuration templates. EMCC CSS may be automatically assigned via device profile configuration template.

Assigning extension mobility via QAS

1. Go to **Quick Add User**, and choose a user from the **Username** drop-down list.
2. Select **Extension Mobility**.

Copyright © 2025 VisionOSS Limited. All rights reserved.



3. To enable EMCC, select **EMCC**.

Note: The **EMCC** checkbox displays only if you've selected the **Extension Mobility** checkbox.

---

4. Click **Save**.
   - The CUCM user is added on CUCM.
   - The CUCM device profile user is added on CUCM, based on settings in the device profile configuration template in the QAG.
   - The device profile is associated with the CUCM user.
   - If you've enabled EMCC:
     - EMCC is enabled for the device profile on CUCM.
     - The EMCC calling search space (CSS) is set for the device profile. The CSS name is based on the country associated with the site, for example, `EMCC-CSS-USA`
     - The device profile is subscribed to the `EMCC Login/Logout` phone service on CUCM (which will allow the user to log in and log out of a physical device to use their extension remotely). Automate requires this service to exist on CUCM, or the provisioning will fail.
5. Verify that the extension mobility profile name appears in the **Extension Mobility Profiles** field on the **Existing Services** tab.

Note: Extension mobility can also be enabled and inspected via the **Subscriber Management** list view (click on the subscriber and check the settings on the following tabs:

- User
- Extension Mobility

Copyright © 2025 VisionOSS Limited. All rights reserved.

Provision the Jabber or dual mode device service

Tip: *Use the Action search to navigate Automate*

This procedure provisions a user with the Jabber or dual mode device service, using Quick Add User.

1. Go to **Quick Add User**.
2. From the **Username** drop-down, choose a user.
3. Select the **Jabber/Dual-Mode Device** checkbox. The **Jabber and Dual-Mode Devices** field appears.
4. Click the Plus icon (+) at **Jabber and Dual-Mode Devices** to expose the **Jabber/Dual Mode Agent** drop-down and **Device Name** field.
5. At **Jabber/Dual Mode Agent**, choose a device type. The **Device Name** field is automatically generated as follows:
   a. If no device name exists in the format *<device type prefix><username>*, then in this format:

      <device type prefix><username>

   b. If device name exists in the format *<device type prefix><username>* or *<device type prefix><username><number>*, then in the format:

      <device type prefix><username><random number>

      where *<random number>* is generated and unique.

   - <device type prefix> - always three characters, either BOT, CSF, TAB, TCT, CIM, or CTI.
   - <username> - 8 characters maximum. If a username contains '_' and '.' characters, these characters are removed from the automatically generated username. Automatically generated usernames can be edited if required.
   - <random number> - dependent on length of username, to make up a total of 11 characters along with the username.

   See examples in table below.

   Example Device Type and Device Name Combinations

For this type of device	Device Name (automatically generated) Format (regex): "[a-zA-Z0-9]{1,15}"
Android (Cisco Dual Mode for Android)	For example: BOTJOHND003938
CSF (Cisco Unified Client Services Framework)	For example: CSFROBWOR77891
iPad (Cisco Jabber for Tablet)	For example: TABRQUENT18947
iPhone (Cisco Dual Mode for iPhone)	For example: TCTPDEVILLI156
Carrier Integrated Mobile	For example: CIMJOHNSMI
CTI Remote Device	For example: CTIJOHNSMI

   For the following Agents, also select the **Mobile Identity** checkbox to enable Mobile Identity if required:

   - Android

Copyright © 2025 VisionOSS Limited. All rights reserved.

- iPhone
- Carrier Integrated Mobile

6. Click **Save**.
7. Go to **Quick Add User**.
8. From the **Username** list, choose the same user.
9. On the **Existing Services** tab, ensure that the **Phones** field displays the Jabber device.

For each device type, a Configuration Template that is associated with the user's Quick Add Group is used to provision the device. For defaults, see: *Quick Add Groups, default model*.

Note: If a CSF Jabber device type is selected, all lines are associated to the CSF Jabber device by default.

Enable self-provisioning

This procedure enables self-provisioning for a subscriber using Quick user (QAS).

Tip: *Use the Action search to navigate Automate*

1. Go to **Quick user**, then, from the **Username** drop-down, select a user.
2. Select the **Enable Self Provisioning** checkbox. The **Self Provisioning User Profile** drop-down appears.
3. From the **Self Provisioning User Profile** drop-down, choose a Self Provisioning User Profile. These were previously created under **User Profile**.
4. In the **Lines** field, click the Plus icon (+) to display the **Directory Number** drop-down.
5. Choose a line from the **Directory Number** drop-down.
6. Click **Save**.
7. Go to **Subscribers** and choose the same user from the **Subscribers** list view.
8. Verify that the **Self-service** and **User Profile** fields display the same settings as those set in Quick user.

Move user

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

A Customer administrator (or higher) can move a user from:

- Provider level to a Site (if you're logged in as a Provider administrator)
- Customer level to a Site
- One Site to a another Site, under the same Customer
- One Site to another Site, for example, on a different Cisco UCM cluster and CUCxn cluster.

When moving a user:

- The user, phones, device profiles, SNR, voicemail, and Automate data are processed in the move.
- The user is updated with a new primary extension, where appropriate.
- The following existing services (associated with this user) are moved along with this user:
  - Phones (and associated lines)
  - Devices
  - Device profiles
  - Single number reach
  - Voicemail
  - Webex
  - Webex App
  - Contact center
- When moving between sites on the same Cisco UCM cluster, user data is moved to the new hierarchy and updated as described above. It is assumed that the CUCxn, if used will remain.
- When moving between different UCM clusters, the move data is re-provisioned on the new cluster and deleted on the original cluster, except for the UCM user. When the UCM user is local, the old user is removed.

  Important: When moving a user across clusters, while the user retains their remote destination information, their time of day information (ToD) and related time schedules and time periods data associated with the remote destination profile must be recreated at the target hierarchy.

- For an LDAP user, the Automate user is purged.

  The user is removed from the `device/cucm/User` model of the source UCM in Automate.

  The home cluster flag is maintained such that it is only set to True on the UCM cluster hosting the user, even if the user exists on other UCM clusters.
- When moving between clusters, the CUCxn server can be retained. In this case, the model instances are moved.

  If the CUCxn server changes, a new CUCxn user is created against a chosen user template. This will not copy custom settings for the CUCxn user or any recorded prompts and messages.
- The first line on all devices must be common prior to the move. Replacing lines creates the same line layout on all devices.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- When moving cross cluster, the UCM cluster is changed. The CUCxn cluster may be retained or changed, based on the new site NDL. If the CUCxn cluster is changed, only basic voicemail is created - user customized configuration, as well as prompts and messages are not moved to the new CUCxn cluster.
- CUCxn cluster moves are only supported where the UCM cluster changes.

Related topics

- *Reserve numbers for a user*
- *Microsoft - Move user & services*

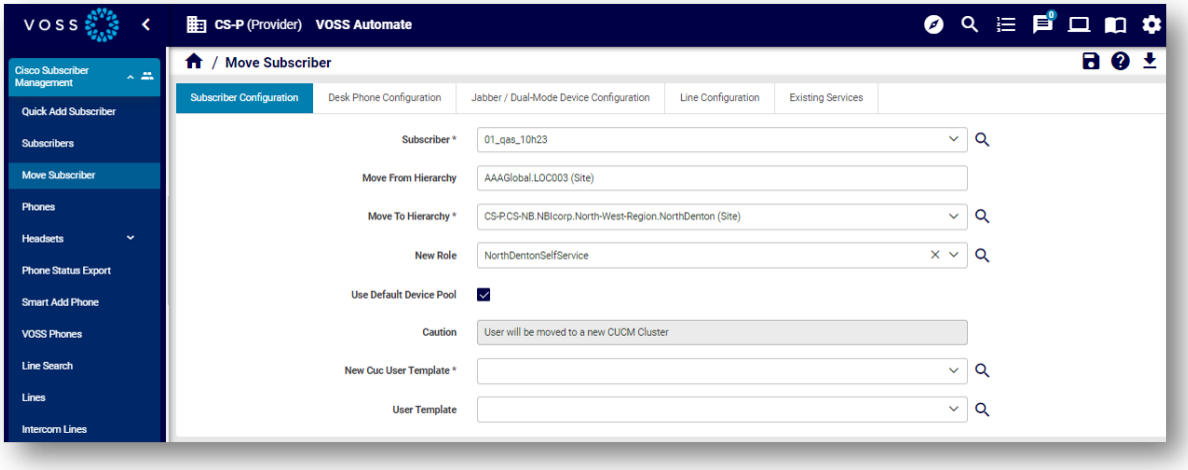
Move user configuration

You can move users via the **Move user** page, then configure options on the following tabs:

- *User Configuration Tab*
- *Desk Phone Configuration Tab*
- *Jabber/Dual-Mode Device Configuration Tab*
- *Line Configuration Tab*
- *Existing Services Tab*

User Configuration Tab

On this tab you choose the user you're moving and their target hierarchy.



The table describes configuration options on the User Configuration tab:

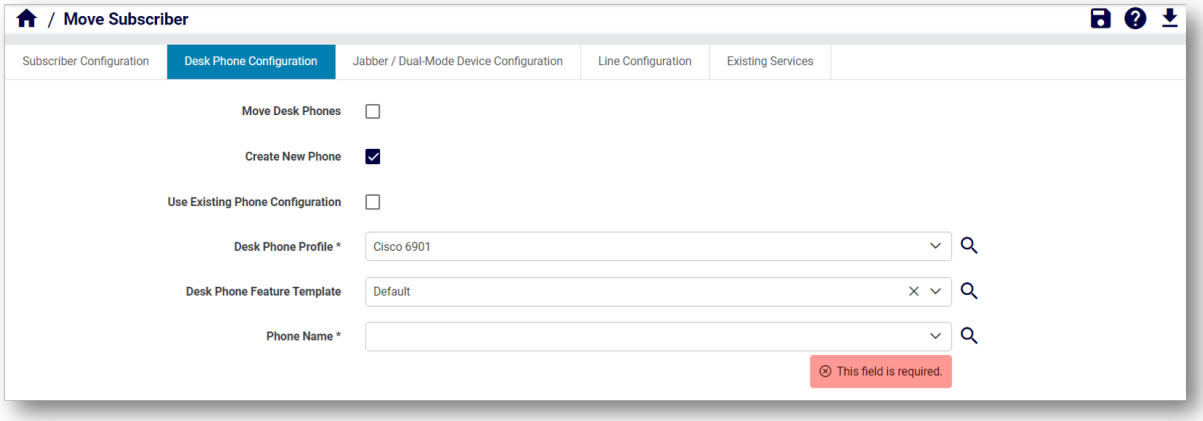
Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Username	The user you're moving.
Move from Hierarchy	Auto-populated, based on the user you choose. The hierarchy the user is moving from.
Move to Hierarchy	Mandatory. Choose a target hierarchy for the move.
New Role	Optional. Choose the user's role at the target hierarchy. The list of available roles will include those where the **Hierarchies Allowed** list of the role contains the target hierarchy selected in the **New Role** list.[1]
Use Default Device Pool	Choose whether to use the default device pool (the site default at the target hierarchy).
Device Pool	Displays only when **Use Default Device Pool** is not selected. Allows you to choose a device pool at the target hierarchy, if you're not using the default.
Caution	Read only warning field, for example, to alert you when you're moving a user to a new Cisco UCM cluster.
New CUC User Template	Mandatory when moving a user to a different Cisco UCM cluster.
User Template	Optional template (`MoveUpdateUserCustom_CFT`) for custom user updates on Cisco UCM. You can clone and customize this template, if required. Available user templates are listed on the **Configuration Templates** page.

Desk Phone Configuration Tab

This tab configures the desk phones of the user you're moving.

Note: By default, existing desk phones are moved with the user. However, desk phones can either remain at the old site or move with the user. Existing softphone devices, such as Jabber or Dual Mode devices, are always moved.



[1] See: *Role Management*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The table describes configuration options on the Desk Phone Configuration tab:

Field	Description
Move Desk Phones	Enabled by default. Defines whether to move the user's (SEP prefix) desk phones to the target hierarchy. Phones that aren't moved remain at the origin hierarchy. When unchecked (disabled), the moved user is disassociated from their existing desk phones. Existing (non-SEP prefix) softphone devices (such as Jabber or Dual Mode devices) are always moved, but can be configured via the Jabber/Dual Mode configuration templates. See *Jabber/Dual-Mode Device Configuration*.
Create New Phone	Choose this option to create new phones for the user at the target hierarchy. When enabled, configure the following fields on this tab: • Use existing phone configuration (yes/no) • Desk phone profile • Desk phone feature template • Phone name
Use Existing Phone Configuration	Displays when **Create New Phone** is enabled. Defines whether to use the existing phone configuration as a template to create the new phone. When enabled, configure the following fields on the tab: • Phone configuration source • Phone name Profile settings can be updated on the new phone.
Phone Configuration Source	Displays only when **Use Existing Phone Configuration** is enabled. Choose from a list of the user's existing phones to create the new phone using the configuration of the existing phone.
Desk Phone Profile	Displays when **Create New Phone** is enabled and **Use Existing Phone Configuration** is disabled. From the drop-down, choose the profile for the new phone (and its associated configuration, which is based on the phone configuration mapping at the target hierarchy). If you change the target hierarchy after selecting an option as the desk phone profile, you'll need to choose another option from the refreshed choices in this drop-down.
Desk Phone Feature Template	Displays when **Create New Phone** is enabled and **Use Existing Phone Configuration** is disabled. Optional configuration template. Choose a template from the the first Phone Mapping Configuration found up the hierarchy tree. The Move user process applies the newly created phone with the desk phone profile and then on top of it the details from the chosen desk phone feature template.
Phone Name	Displays when **Create New Phone** is enabled. Choose a phone name from the drop-down, which displays options from the **Phone Configuration Mapping** page (**Customizations > Phone Configuration Mapping**). Default phone configuration mappings are available per hierarchy and are used at the selected hierarchy and below. See "Configuration Mapping Files" in the Core Feature Guide for details.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Jabber/Dual-Mode Device Configuration Tab

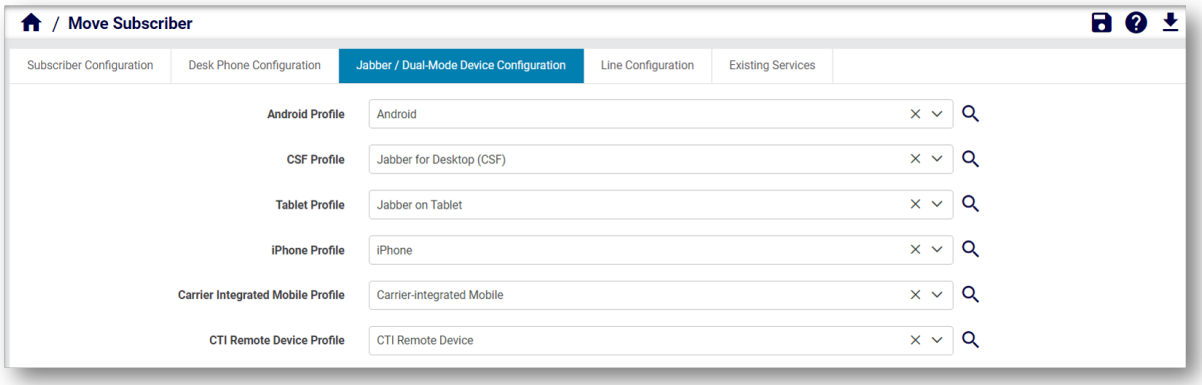
This tab configures Jabber and dual mode devices that are, by default, moved with the user.

The device configuration is derived from the device profile selected in the associated **Profile** drop-down (i.e. Android, CSF, Tablet, iPhone, Carrier Integrated Mobile and CTI Remote Device).

The default device profiles are found on the **Phone Mapping [Default]** page.

You can clone and save a profile if required, and customize the relevant settings, for example, **Basic Phone CFT**, in order to apply different settings to the device.

See “Configuration Mapping Files” in the Core Feature Guide for more details.



Line Configuration Tab

This tab configures options for moving lines and/or creating lines when moving a user.

Note: You can use inventory filters to filter the lines available to choose from, if number inventory filtering is enabled at the current hierarchy. See *Manage number filters*.

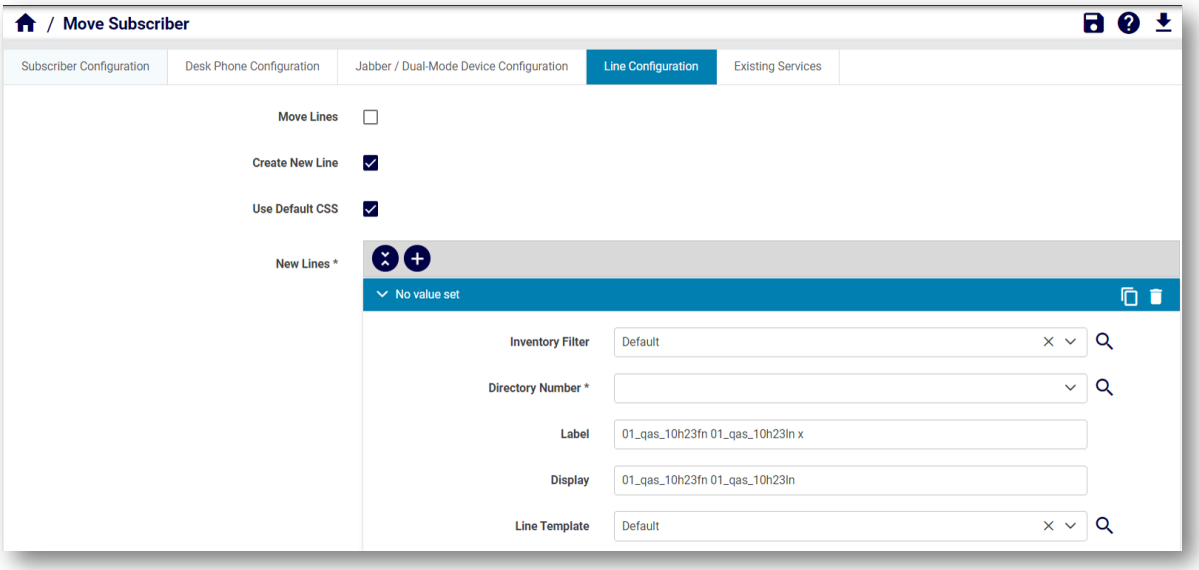
When moving a user, the system performs a validation check to ensure that the first line across all devices is common.

All new lines created (or existing lines moved) in the move, are assigned to SNR. For example, if a user with three lines and a Phone, SoftPhone, DeviceProfile, and SNR is moved, all these services will be associated with the three lines. The only exception to this is for Voicemail, where the first line is always selected as the Voicemail line.

At the target hierarchy, the line label updates to FirstName, LastName, and extension.

Note: When moving a user with first name or last name containing non-ASCII characters, and the user has a phone, extension mobility (device profile), and remote destination profile, each with associated lines, Automate configuration templates (CFTs) convert the non-ASCII characters to ASCII. This allows the user to move with all services and lines re-associated as configured.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Creating Lines

When moving a user to another Cisco UCM cluster, you must create new lines (in this case, the option to move lines is hidden).

When creating a new line:

- Choose the default CSS (at the target hierarchy); else, select a line CSS and a Call Forward CSS for the new line. A configuration template `MoveUpdateLineCustom_CFT` is available to make custom line updates
- Choose a line template for the new line. One line template may apply to all lines.

Moving Lines

Important: Lines are exposed and supported by Automate (if the required conditions already specified in this doc are met).

- Lines can only be moved to the destination hierarchy if your system is using a type 4 dial plan, and only if the move is on the same cluster.

  To enable moving of lines to the destination hierarchy, the `UserMove_AllowLineMove_MCR` macro must be cloned to the applicable hierarchy level and the value set to `{{ fn.true }}`.

  Ensure that the customer dial plan supports moving of lines between sites before attempting to move the line.

- Lines can't be moved between sites if the customer dial plan at the target site uses SLC-based dial plans (types 1, 2, and 3).

  Note: To allow moving of a user with their device profile and line:

  – The customer dial plan of the target site must not be SLC-based; that is, the following setting must be disabled in the target site's customer dial plan: *Site-Location Code (SLC) based dial plan*

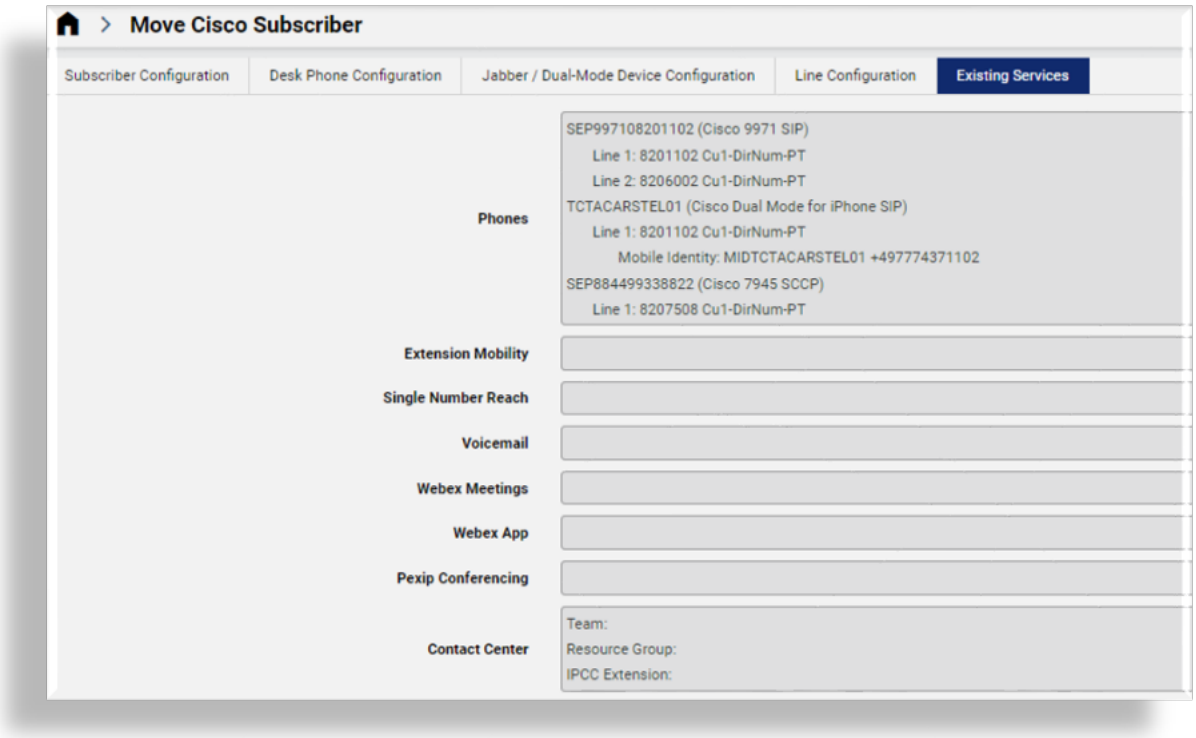
Copyright © 2025 VisionOSS Limited. All rights reserved.

You can view the customer dial plan configuration via the customer **Dial Plan** page.

Additionally, the global setting, *Enforce HCS Dialplan Rules*, must be disabled for the target site. You can view this setting via The Number Inventory tab in the **Global Settings**.

Existing Services Tab

This read-only tab displays the existing services of a user you're moving, including, for dual-mode devices, the name and destination for mobile identity, remote destination, and CTI remote device with remote destination.



Reassign user services

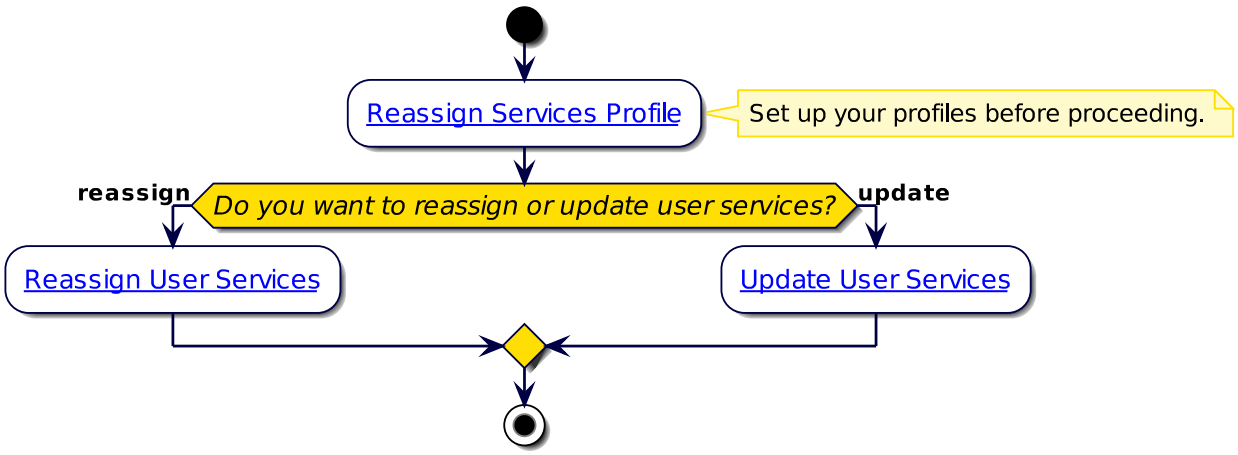
Tip: *Use the Action search to navigate Automate*

Overview

Reassign user services simplifies and automates the transfer of existing user services from a source user to a target user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Reassign services high level workflow



This utility is for example useful when an employee leaves an organization and a new employee starts the same role. Instead of removing the old user and configuring a new user with the same settings and standards, the services and settings can be moved from the old user to the new user.

These services can include:

- Fixed phones
- Device Profile(s)
- Remote Destination Profile(s). Remote destination needs to be set up for the target user separately
- Voicemail user with related services including alternate extension and message handle (action)

Note: Webex (Meetings and App) and CCX services are not currently supported by this feature.

Custom settings can be applied to these services during the reassignment. A **Reassign Services Profile** setting is available to choose the configuration templates that will be used to update services during reassignment. These allow you to customize most settings on any of the above devices, including Line Alerting Name, Line Label, DisplayASCII values, and so on.

Example templates are provided that contain macro variables for fields that are likely to differ between users. The field values then resolve with input from existing target user details. In this way the templates are not limited by for example a Site and Phone Model.

When reassigning services from existing source users to existing target users, the latter are moved to the *same site* as the source user, if these differ.

It is also possible to create a new target user as part of the “reassign services” process instead of selecting an existing user without services. This user will be created at the same site as the source user.

Other features included are:

- Change User Details (modified Reassign Services) that updates the services of an existing user using custom templates referenced in a Reassign Services Profile.

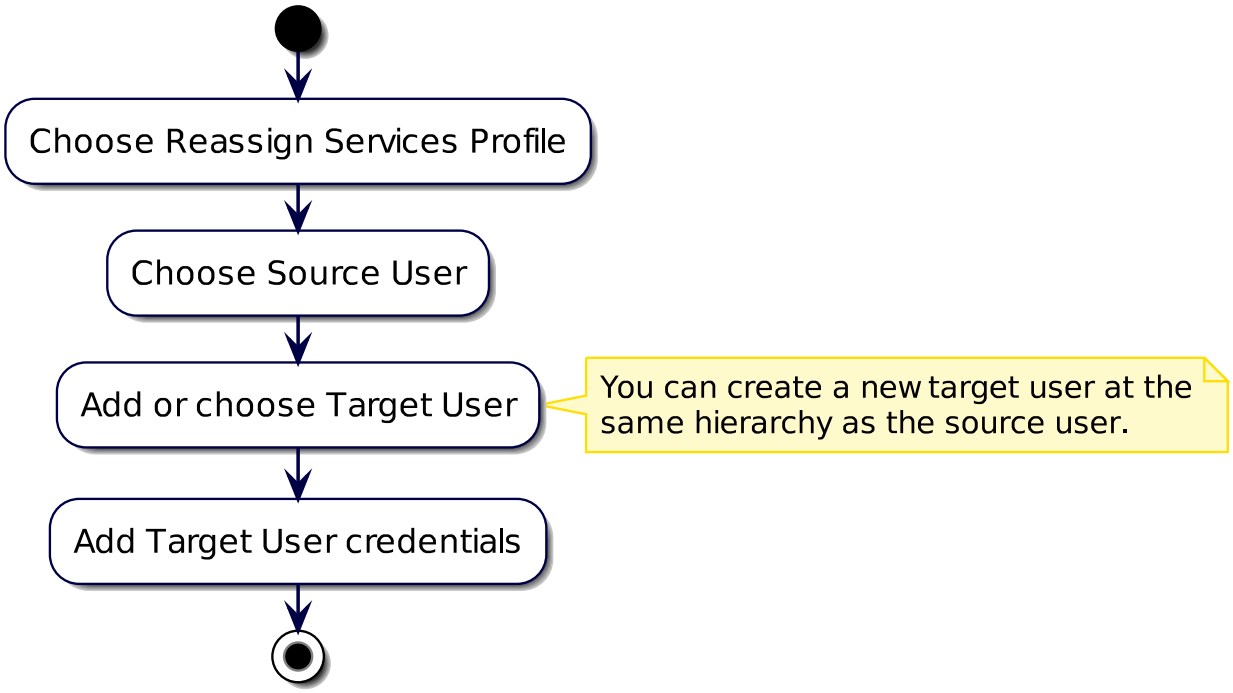
Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Reassign a user's service*
- *Update a user's service*
- *Reassign services profile*
- *Reserve numbers for a user*

Reassign a user's service

The Reassign Services functionality requires that you select a customer hierarchy (if you are not already there) since it supports target users that are on a different site to the source user.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Field Name	Comment
Reassign Service Profile	This field will pre-populate with the first profile. You can select a different profile if required. If no profile option is available, then a reassign service profile needs to be added in the system.
Source User	Choose the user to be reassigned. This provides a list of usernames of users in the system. It will list local or CUCM-LDAP Synced users only (not Automate-LDAP synced) Once a user is selected, the **Source User Services** tab is updated to show services currently assigned and that will be reassigned to the target user. This is a good way to validate that all the services are shown or that there are not services that you do not want reassigned.
Source User Hierarchy	Once a user is selected the **Source User Hierarchy** will be populated - this is a read-only informational field.
Add A New Target User	Select this option if you need to add a new local user to the system as the target user. Once selected, the form updates to reflect this choice.
Target User	To reassign to an existing user: select the username from the drop-down. This will show local or CUCM-LDAP synced users at the customer level or lower. Once a user is selected, the **Target User Services** tab is updated to reflect any services currently assigned to the user. If the user has any entries on this tab then the transaction will be blocked. So this provides an option to check before submitting. To create a new target user: enter the username for the new user to be created. The user will be added to the same hierarchy as the source user.
Target User Hierarchy	Shown only if add new target user is not selected - read-only informational field. Shows the hierarchy of the selected target user. Can be different to the source user and the feature will move the target user to the same hierarchy as the selected source user.
First Name	First Name of the Target user. Will be read only if the target user is a LDAP synced user.
Last Name	Last Name of the Target user. Will be read only if the target user is a LDAP synced user.
Email Address	Email Address of the Target user. Will be read only if the target user is a LDAP synced user.
Password	Visible if the target user is not a LDAP synced user. Enter the password for the target user.
Pin	Enter the PIN for the target user (used for device profile and voice-mail).

Notes:

- The feature requires that source user services should all be at the same site hierarchy.
- Target user and hierarchy:
  - New target user - will be added to the hierarchy of the source user.
  - Existing target user - If the target user is in a different hierarchy to the source user, the target user will be moved to the same hierarchy as the source user as part of the reassign of services.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: It is not possible to reassign services to a user who is on a different CUCM Cluster than the source user. The target user drop-down will currently not show users on a different cluster.

- The **Source User Services** tab will populate once a source user has been selected. This shows the services currently assigned to that user and the services that will be reassigned. This is a good way to validate the services that will be reassigned and to check if there are any services missing or that should not be reassigned. This can then be corrected as needed before reassigning the services.
- The **Target User Services** tabs will populate once a target user is populated. This is a good way to validate that the target user does not currently have any services assigned, as this will cause the transaction to fail with an error message indicating the target user has services. This can be resolved by choosing a different target user or by removing the services currently configured for the target user.
- Based on the setting in the reassign profile, the source user will either be left in the system (without any services) or removed from the system entirely.

Most of the services are updated to be associated to the target user and have settings updated according to the Configuration Templates (CFTs) in the reassign profiles.

There are some considerations:

- Single Number Reach (SNR) - Any existing remote destinations configured for the source user are deleted. The Remote Destination Profile (RDP) is then associated to the target user and updated per the CFT in the reassign services profile.
- Voicemail - the existing voicemail service for the source user is deleted to ensure a clean voicemail service. The voicemail service is then rebuilt for the target user based on the CFT in the reassign service profile. This means that any personalized settings, messages, greetings, and so on are cleared.
- Shared lines - Shared lines associated to the source user will only be updated if the shared line is the source user's primary extension.

The feature includes the optional ability to update shared line appearances of the source user's lines on other users' phones to reflect the destination user's details. For example:

- Bob.Smith has a phone with the following:
  - Line1: 55210 - Label: Bob Smith 55210
- Mary Smith has a phone with the following:
  - Line 1: 55220 - Label: Mary Smith 55220
  - Line 2: 55210 (shared line appear of Bob) - Label: Bob Smith 55210

In this case, when Bob's service is reassigned to a new user, Mary's Line 2 appearance will need to be updated to reflect the new user (e.g display name, label, etc.). This is supported for line appearances on Phones, Device Profiles, and Remote Destination Profiles. See the reassign services profiles section for more details on the controls.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Shared Lines in the Core Feature Guide.

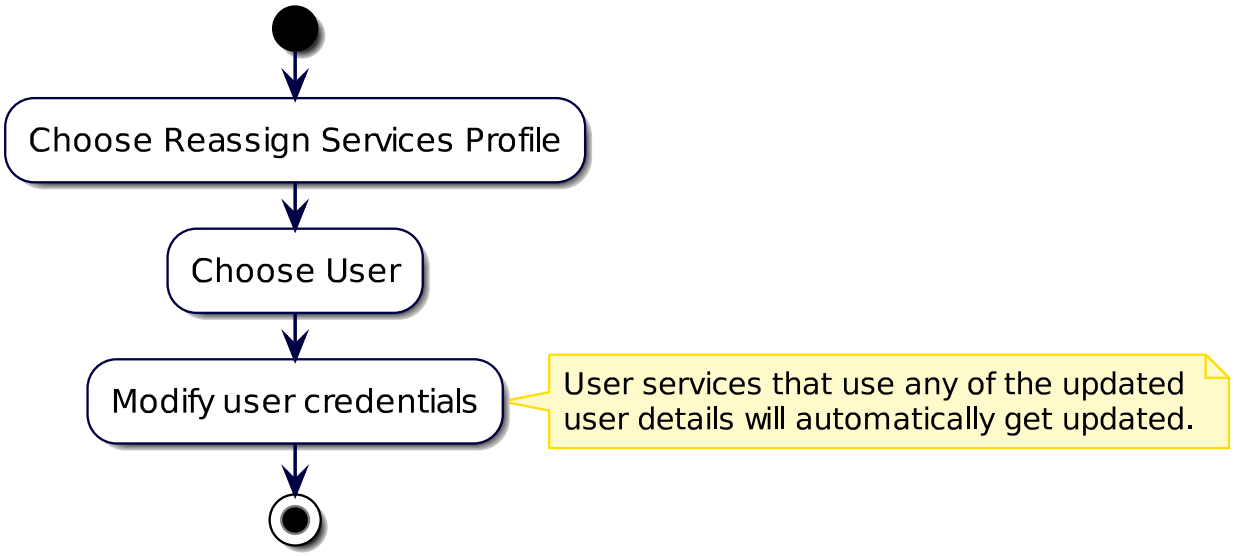
Update a user's service

The **Update User Services** tab/panel displays a simplified form of Reassign Services where only one source user is selected, and that user's services are updated using custom configuration templates referenced in a *reassign services* profile. The input fields allow for an easy update of basic details such as First Name, Last Name, Email, Password and PIN. User services that use any of the updated user details will automatically get updated.

The **Reassign Services Profile** drop-down list is available to select a profile to be used to also update the user's services details.

Similar to Reassign Services, selecting a Username auto-populates the Hierarchy of the selected user and the **Current User Services** tab/panel displays the services that will be updated.

Reassign User Services (Update user services workflow)



Reassign services profile

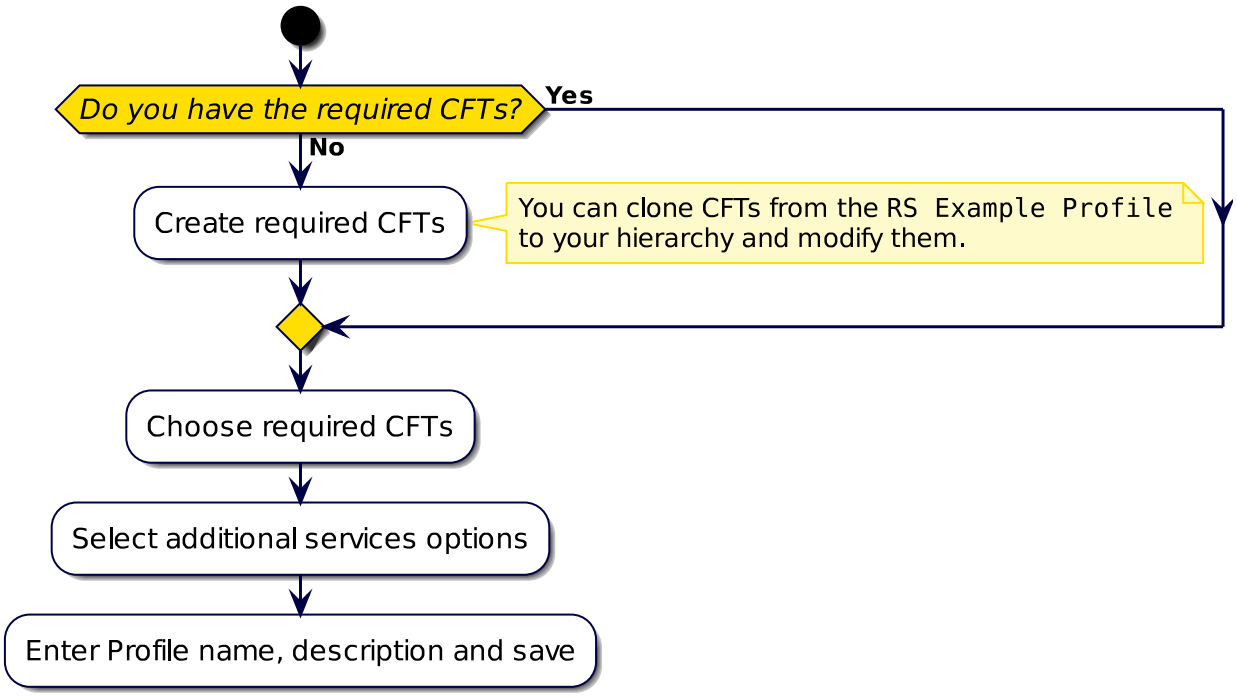
Tip: *Use the Action search to navigate Automate*

The **Reassign Services Profile** page allows for a set of configuration settings and additional settings to apply when using *reassign services* functionality.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Reassign services profile configuration workflow

The flowchart describes the configuration settings to apply. If no configuration template is defined for a service, it is still moved to the new user. However, existing settings are left in place.



Configuration templates and reassign services profile

Configuration templates (CFTs) selected in the profile determine how many of the detailed settings of the various services are updated as part of the reassign. This will allow you to re-align settings to your baseline service deployment logic and update any settings that incorporate the user's name - for example descriptions, alerting/display names, labels, and so on.

If no CFT is defined for a service, it is still moved to the new user. However, existing settings will be left in place. There are a few cases where the feature will make updates to specific service settings regardless of the CFT (i.e. when these settings are required to associate the user and service - owner of a phone, associated devices on the UCM user, etc). If the source user does not have a given service (e.g voicemail) then any CFT in the profile is ignored as the feature does not add new services that did not exist on the source user.

Automate ships with a collection of sample CFTs (prefixed `RS`), which provide examples of common settings and logic.

This profile and templates for configuration settings can be maintained per hierarchy as needed. The reassign services feature is similar to Quick Add User, allowing re-use of macros/logic from your Quick Add Group CFTs in the reassign services profiles. In many cases you could even use the same CFT to ease maintaining multiple sets of CFTs that define the baseline user and service configuration.

Note: At least one reassign services profile must be added to use the reassign user services functionality.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Reassign services profile settings

Go to **Reassign Services Profile**, then choose an existing profile to view its settings, or to add a new profile.

Field	Description
Profile Name	Name for the Profile - recommended to make it meaningful to the user's that will be using the feature if you need more than one profile.
Profile Description	Description for the profile
Remove Source User	If selected the feature will fully remove the source user after moving all the services. If not selected then the base user and user will be left when the feature completes however no services will be enabled.
User CFT	This CFT defines Automate user settings to apply to the target user - e.g. role
CUCM User CFT	This CFT defines the UCM User settings to apply for the target user - e.g Department, Service Profile, etc.
Line CFT	This CFT defines the UCM Line settings to apply for the target user - e.g. Description, Alerting Name, Pickup Group, Call Forwarding, etc
Phone CFT	This CFT defines the Phone settings to apply to the devices being moved - e.g. Line Label, display name, device pool, CSS, etc. This same CFT applies to all phones (hardphones, soft-clients, etc) so typically relate to line appearance settings or other non-phone type specific settings. ownerID, mobility user (for soft clients) as set via the workflow irrespective of the CFT.
Device Profile CFT	This CFT defines the Device Profile (extension mobility) service for the user - e.g Line label, display name, etc. As with the Phone this is typically for line appearance settings on the device profile.
Remote Destination Profile CFT	This CFT defines the Remote Destination Profile (Single Number Reach - SNR) settings to apply to the service being moved - e.g line label, display name, CSSs, etc. Again typically for updating line appearance settings but can also edit other base RDP settings.
CUC User CFT	This CFT defines the CUC User (Voicemail) settings to apply when setting up voicemail for the user.
Add CUC User Alternate Extension	This setting determines if the feature will add a voicemail alternate extension for the user if voicemail exists on the source user. This can be used to add a standard alternate extension (e.g short extension version of the user's number) if needed as part of your standard deployment.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
CUC Alternate Extension CFT	This setting is visible if the add alternate extension setting above is true. This CFT determines the settings for the alternate extension that will be added. This is where you would define the alternate extension to be added as standard.
Update CUC User Message Handler (Action)	This setting determines if the feature will configure the message handler settings for voicemail (form of single inbox).
CUC Message Handler (Action) CFT	This setting is visible if the message handler setting above is true. This CFT determines the settings that will be configured for the message handler. So this will need to include the email address for example of the user as well as the message actions.
Update shared lines (for unassociated Phones, Device profiles, RDP)	This setting determines if the feature will update line appearances of the source user's lines on other user's devices. This can be used to update the display names or labels for instance on those remote devices to reflect the new user's details. These CFTs only apply to line appearance settings on those devices (not general phone settings) and only for the line appearances that are shared with the source user. Other line appearances on the devices will not be updated. For example, the other user's phone had 3 lines, only 1 of which was shared with the source user. Only that 1 line appearance will be updated and the other 2 will be left untouched.
Shared Line (unassociated Phone) CFT	This setting is visible if the Update Shared Line setting is true. This CFT determines the settings on the other users' Phones that have the line appearance.
Shared Line (unassociated Profile) CFT	This setting is visible if the Update Shared Line setting is true. This CFT determines the settings on the other users' Device Profiles that have the line appearance.
Shared Line (unassociated RDP) CFT	This setting is visible if the Update Shared Line setting is true. This CFT determines the settings on the other users' RDP that have the line appearance.

Typically, configuration templates similar to your current Quick Add User templates can be used. Example configuration templates are also available for each drop-down, with naming convention `RS Example <service> CFT`. The templates shown on the **Configuration Templates** menu can be cloned, renamed and modified per hierarchy as required.

Configuration examples:

- Template Name: `RS Example CUCMPhone CFT`

  Field: **Line** > **Display Ascii**

  Value:

```
((input.firstName == fn.null ))
<{{input.lastName}}>
<{{input.firstName}} {{input.lastName}}>
```

- Template Name: `RS Example CUCMLine CFT`

  Field: **ASCII Alerting Name**

Copyright © 2025 VisionOSS Limited. All rights reserved.

Value:

```
{{fn.sub_string input.lastName, 0, 30}}
```

Additional optional settings available:

- **Add CUC User Alternate Extension**:

  If checked, a drop-down is enabled to select a template that updates the alternate extension.

  Example template: `RS Example CUCAlternateExtension CFT`

  Field: **DisplayName**

  Value:

```
{{ input.firstName }} {{ input.lastName }} Alt
```

- **Update CUC User Message Handler (Action)**:

  If checked, a drop-down is enabled to select a template that updates the email address for single inbox.

  Example template: `RS Example CUCMessageHandler CFT`

  Field: **RelayAddres**

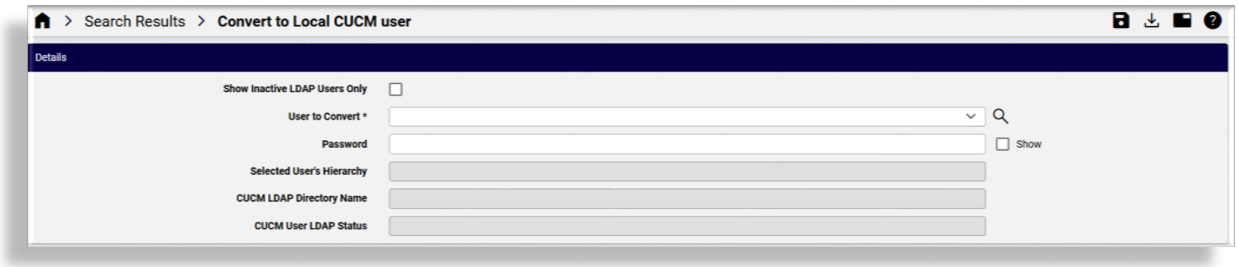
  Value: if no input email address is available, a dummy address is added

- **Update shared lines (for unassociated Phones, Device profiles, RDP)**:

  If checked, a drop-down is enabled to select a template so that for any shared line instances from the source user, line label details can optionally be updated with those of the target user. The **Line CFT** template updates do not apply to shared lines.

Convert user type CUCM-LDAP to CUCM Local

The **Convert to Local CUCM user** tool converts a CUCM-LDAP user account to a CUCM "Local" user. If the user exists on CUCxn Server then the user is also converted to a Local User, that is, the user on CUCxn is set to "Do not Integrate with LDAP Directory".



Tip: *Use the Action search to navigate Automate*

Converting a user from CUCM-LDAP to CUCM Local is typically required when:

- The user has been deleted from the LDAP server
- The CUCM has synced with the LDAP server
- The user has been set to "Inactive"

Copyright © 2025 VisionOSS Limited. All rights reserved.

In this scenario, the user would be deleted when the Garbage Collection process runs on CUCM.

Converting the user to a CUCM Local user prevents the user from being automatically deleted.

Note: You can also configure Automate to automatically convert inactive CUCM-LDAP users (users that would normally be deleted automatically by the CUCM in a data sync) to "Local" in a sync via the following setting, via the **Users** tab in the **Global Setting**: *Convert Inactive CUCM LDAP User to Local on Sync*.

The table describes **Convert to Local CUCM user** settings:

Field	Description
Show Inactive LDAP Users Only	Defines whether to display only inactive users, which have already been deleted from LDAP and are due to be permanently deleted from CUCM. An "inactive user" on CUCM is a user that was deleted from the LDAP Server, and CUCM synced with the LDAP server after the deletion took place. Inactive users are deleted from CUCM when the Garbage Collector next runs on CUCM.
User to Convert	Mandatory. By default, only users with CUCM-LDAP type display in this drop-down. When **Show Inactive LDAP Users Only** is enabled, the list of users is filtered to only show the "CUCM-LDAP" users with a status of "Inactive", that is with status value = 2. • Active (1): the user is still in LDAP since the last sync • Inactive (2): the user is not in LDAP since the last sync
Password	The password used to set the password for the user on CUCM and CUCxn.
Selected User's Hierarchy	Read only. The selected user's current hierarchy.
CUCM LDAP Directory Name	Read-only. The LDAP directory name.
CUCM User LDAP Status	Read-only. The selected user's current status

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Global Settings in the Core Feature Guide.

Cisco UCM users

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes the user management functionality for Cisco Unified Communication Management (Cisco UCM) users.

From 21.4-PB5, Automate ships with two management page layout options for Cisco users in the Automate Admin Portal, each with their own look and feel, and with different levels of detail included on the forms. These layouts are accessible via two *User* menus in the **Cisco User Management** menu group:

- *Cisco UCM Users menu*
- *Cisco Advanced User menu*

The table describes the models associated with each of these layouts:

Model	Menu	Description
`relation/CiscoSubscriber`	Cisco Advanced User	This page layout will be familiar to users of the Classic Admin GUI and who wish to retain the look and feel of a Cisco, single vendor view of the page when upgrading to Automate 24.1.
`relation/Subscriber`	Cisco UCM Users	Provides a user-friendly panel layout, with features such as quick actions, and graphical icons for phones and services.

Important: The two menu/layout option is available in the Automate Admin Portal. The Classic Admin GUI is deprecated from v24.1.

Customers upgrading to Automate 24.1 and who wish to retain the familiar look and feel of the Cisco User layout of the Classic Admin GUI may want to use the `relation/Subscriber` model for their Cisco users. See *Cisco Advanced User menu*.

You can view, add, update, or delete users via the list views and user management pages for either of these menus. It is recommended that you choose one or the other of these page layouts to use in your environment.

Copyright © 2025 VisionOSS Limited. All rights reserved.

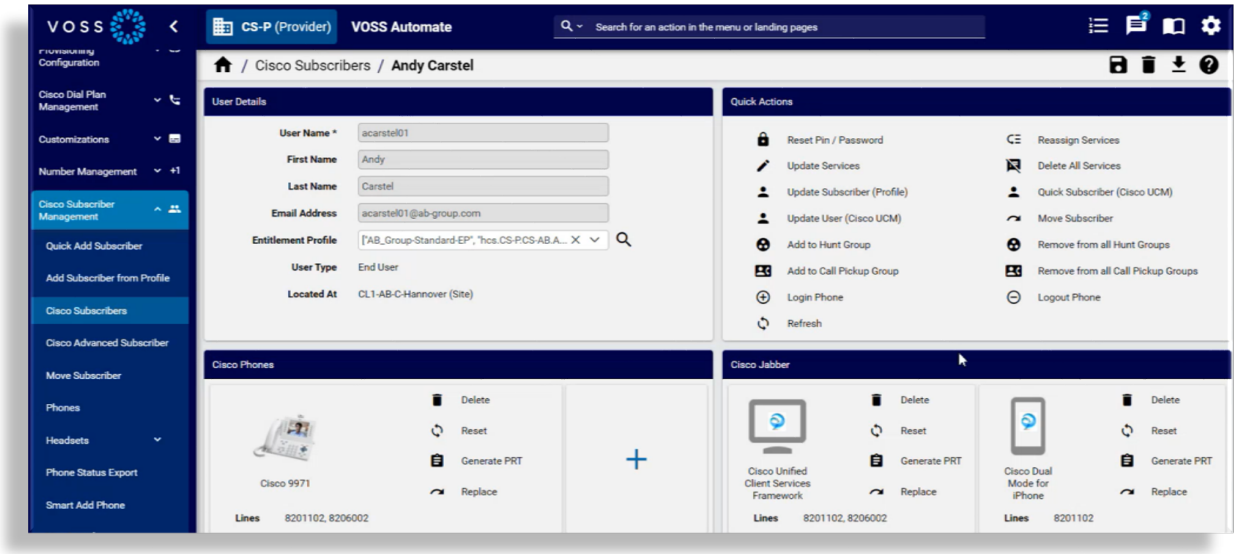
Related topics

- Multi vendor users in the Core Feature Guide
- *Conventions used in this guide*
- *Reserve numbers for a user*
- *Manage number filters*

Cisco UCM Users menu

The Cisco UCM Users menu uses the `relation/Subscribers` model in the Admin Portal, and uses a multi vendor user field display policy. Viewing a user via this model provides a user-friendly panel layout, and features such as quick actions, and graphical icons for phones and services.

The image shows the look and feel of the management page layout of a user accessed via Cisco UCM Users in the Admin Portal:



Cisco Advanced User menu

The Cisco Advanced User menu is associated with the `relation/CiscoSubscriber` model in the Admin Portal. Viewing a user via the list view for this menu provides a Cisco-centric user management page layout that may be preferred by users familiar with the older, Automate Classic Admin GUI in a Cisco-only (single vendor) environment.

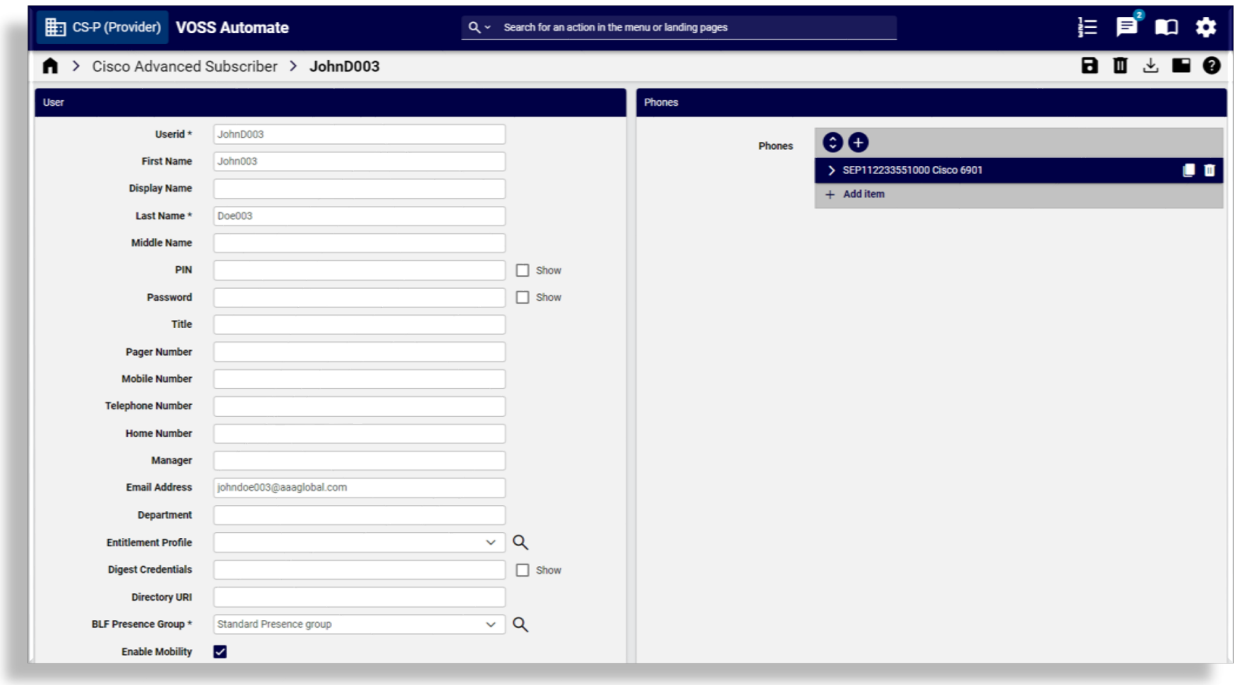
You can view this page as a tab or panel layout (and switch between these layouts via the **Switch to Panel/Tab Layout** toolbar icon).

This menu and model must be set up using a custom menu path associated with *relation/CiscoSubscriber*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

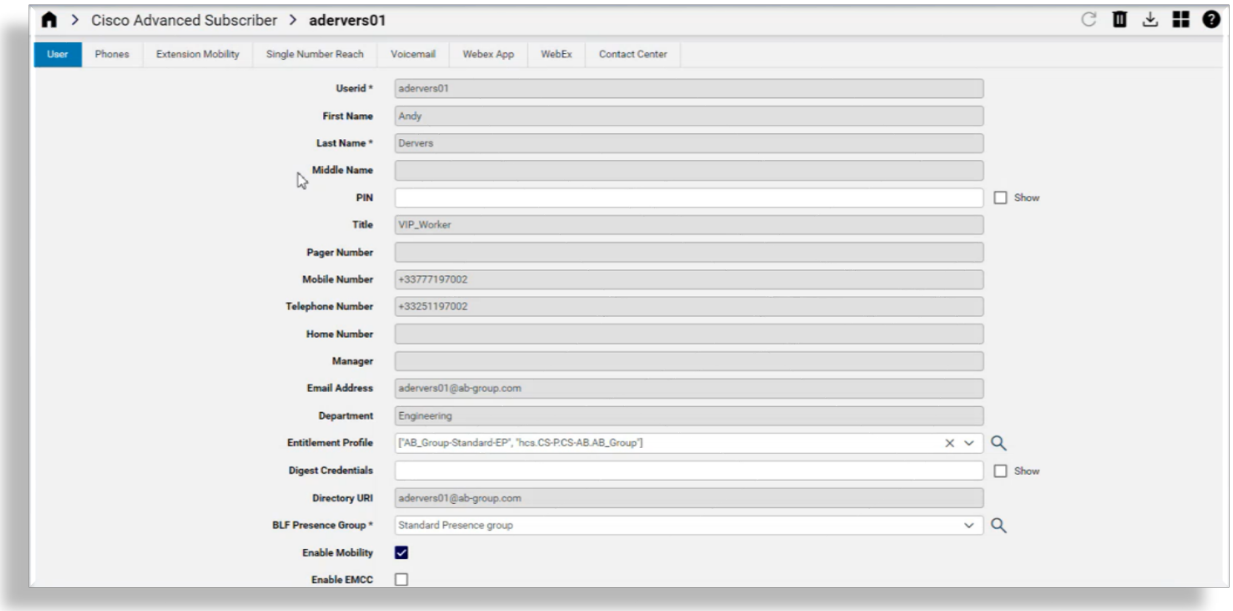
Cisco Advanced User panel layout

The image shows the look and feel of the management page layout of a user accessed via the Cisco Advanced User menu in the Admin Portal, using a panel layout:



Cisco Advanced user tab layout

The image shows the look and feel of the management page layout of a user accessed via Cisco Advanced Users in the Admin Portal, using a tab layout:



Copyright © 2025 VisionOSS Limited. All rights reserved.

Configuring Cisco user menu items

This procedure configures menu layouts and dashboards for the menus items **Cisco Users** and **Cisco Advanced User**.

Note: The Automate Admin Portal allows you to choose between `relation/CiscoSubscriber` and `relation/Subscriber`. It is recommended that you choose choose one or the other of these page layouts to use in your environment.

Users with an access profile with permissions on `relation/Subscribers` will automatically have the same permissions on the customized relation, `relation/CiscoSubscriber`.

---

1. Log in to the Automate Admin Portal as an admin with permissions to customize menu layouts, then go to **Menu Layouts**.
2. In the list view, click on a menu layout to edit it.

   Note: The menu items are accessible to reseller admin and operator, provider admin and operator, enhanced provider admin, multi vendor provider admin.

3. Go to **Cisco Users**.
4. Configure the **Cisco Users** menu item:
   - Model type is *relation/Subscriber*.
   - The default field display policy is *MultiVendorFDP*.
   - This menu item uses the *Subscriber_Menu_CFT* configuration template (one option only).
5. Configure the **Cisco Advanced User** menu item:
   - Choose `relation/CiscoSubscriber` (a customized relation specifically designed to provide the alternative layout).
   - The default field display policy is *SubscriberAdvancedDefault*.
   - Choose a configuration template.
6. Configure a dashboard for the admin you're working with.
   - Go to **Dashboards**.

     You can:

     – Add links for the dashboard, if required, to point to either `relation/Subscriber` or `relation/CiscoSubscriber`, depending on the menu you're using.

       Choose whether to set up the links you're configuring as the default model type (`relation/Subscriber` or `relation/CiscoSubscriber`)

       Note: When performing a global search for a user, or when opening a user via the line search, the page layout that opens is the one marked as the dashboard default.

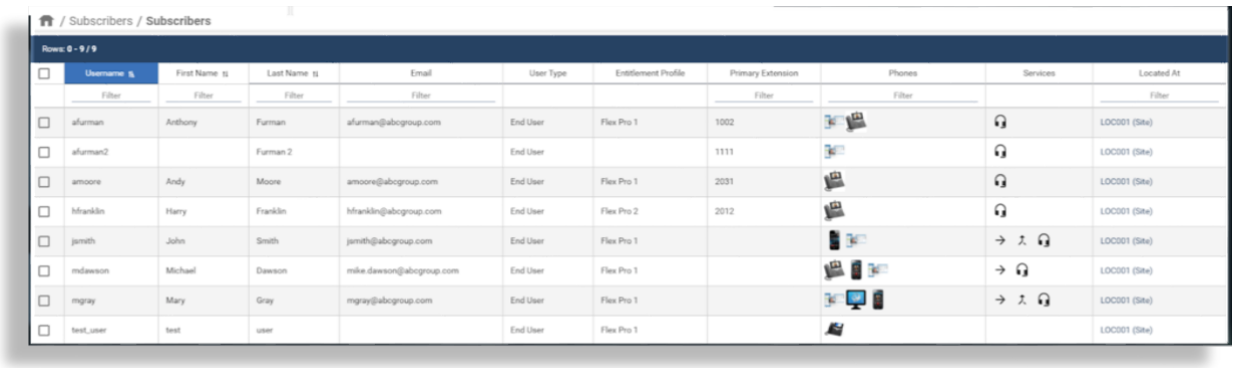
     – Add counters to the dashboard, if required. And if required, add filters to the counters.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: You can use a different FDP or configuration template for the counters on the dashboard.

View Cisco users

In the Admin Portal, you can view a summary list of Cisco users (at the current hierarchy and down), which includes details of each user's currently provisioned services, grouped by vendor.



To view the Cisco user list view in the Admin Portal, either of the following options, depending on your setup:

Environment	Steps
Single vendor environment (Cisco)	Either of the following: • Go to **Cisco Users**. • Go to **Cisco Advanced User**
Multi vendor environment (which includes includes Cisco users)	Go to **Multi Vendor Users**

The table describes columns in the Users summary list - you can click on a user in the list view to open its management page:

Note: The list view is the same for both the *Cisco Users* menu and the *Cisco Advanced Users* menu.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Username	The username associated with the user.
First Name / Last Name	First name and last name of the user.
Email	User's email address.
User Type	The type of user, either Admin, End User, or End User + Admin (associated with their user role.
Sync type	How the user is synced in to Automate, for example, UCM, LDAP, Local (the source application of user data. • Local - user was manually created in Automate (not synced from LDAP or UCM) • UCM - user exists on both Automate and Cisco UCM (not synced from LDAP); user may have been created first on Automate (top-down) or created on UCM and synced in to Automate (bottom-up). As for User[1]
Entitlement Profile	The name of the entitlement profile associated with the user.
Primary Extension	The user's primary extension number, as selected from the Pattern drop-down list when adding the user. For Multi Vendor only, the line extension used as the primary line (a pre-allocated administrator line, and associated E164 number).
Phones	Displays all phones associated with the user at the current hierarchy and below.
Services	Displays all services associated with the user, one or more of the following: • Extension Mobility - link to the user's extension mobility profiles on UCM (one or more) • Voicemail - link to voicemail number allocated to the user (in a multi vendor environment, the user's provisioned voicemail services are listed by vendor). • Single Number Reach - link to the remote destination number configured for the user • Voice - link (for multi vendor users only) to the user's provisioned phones • Conferencing - the user's conferencing services (for example, Webex App, MS Teams, Pexip, Zoom) • Headset - the user's headset, typically connected to a phone associated to a user.
Located At	Displays an abbreviated version of the hierarchy showing the lowest point in the hierarchy. The hierarchy type is shown in brackets. When filtering on this column, only use text outside of brackets in the criteria. For example, "SiteName (Site)", where (Site)= the hierarchy node type, only use the "SiteName" portion in the filter criteria.

Note: Other user details that may be available in the list view or when adding or viewing a user's:

- Role - user role, typically a Self-service user role

[1] **Sync Source**: see: *User sync source*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Auth Method - as for User[2]
- Collaboration - multi vendor users only; the user's messaging services, for example, WebEx, MS Teams, Zoom
- Webex App - whether the user is enabled for Webex App
- Contact Center - if enabled, the contact center agent's Team and extension, if the user is an agent
- Device - IP address or hostname

Add a user

This procedure adds a Cisco UCM user in Automate.

Note: If *Enable CSS filtering* is enabled at the customer dial plan, available calling search spaces includes only those marked as a Class of Service on the **Class of Service** page at the particular site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

If *Enable CSS filtering* is disabled, the list of available calling search spaces includes all CSSs that are configured on Automate.[3]

1. Log in to the Admin Portal as Customer admin or Site admin.

   Note: Only a subset of the fields described in this procedure are visible for Site admins.

2. Go to **Cisco Users** or **Cisco Advanced Users**.
3. If you're logged in as Customer admin, choose the site where you want to add the user.
4. On the **Users** list view, click the Plus (+) icon.
5. Configure user details on the form:
   - User
   - Phones
   - Extension Mobility
   - Single Number Reach
   - Voicemail
   - Webex
   - Webex App
   - Pexip Conference
   - Contact Center
6. Click **Save**.

   Repeat this procedure to add another user.

[2] **Auth Method**: see: *User authentication methods*.
[3] This only applies to the Automate *Provider* deployment.

Copyright © 2025 VisionOSS Limited. All rights reserved.

User settings

The **User** tab/panel defines the user details of an Automate user you're adding or updating.

Note the following:

- Only alphanumeric characters are allowed.
- For Cisco users, available entitlement profiles are imported from Cisco UCM.
- When choosing an existing device (phone) to associate with a user and then saving the form, the **Phones** component is populated with the phone details.
- When adding a LDAP user as a user, **Password** fields are hidden, and **Enable Mobility** is enabled by default, when any of the following is included or added:
  - A remote destination phone
  - Mobile identity for a phone
  - Remote destination profile (RDP)

  If user self-provisioning is set up (allowing users to add their own smart devices, such as company or personal phones), and **Enable Mobility** is disabled (checkbox cleared), then the setting is enabled when users add a company or personal phone via the Self-service interface.

  To enable Extend and Connect in Automate:

  1. On the **Users** tab/panel, select **Enable Mobility**.
  2. Add the following three groups of users:
     a. Standard CCM End Users
     b. Standard CTI Enabled
     c. Standard CCM Admin User
- For users entitled to Webex App, you can add a standalone Webex Apps user by completing the following minimum fields on the User component, then go directly to the Webex App component: **Userid**, **Last Name**, **Email Address**
- To provide access to EMCC (only customers configured for EMCC), select **Enable EMCC**.
- The group you choose in **BLF Presence Group** (configured in Cisco Unified Administration), specifies destinations the user can monitor.

  Note: BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. The **Busy Lamp Field** default is set according to the selected number and specifies the Standard Presence Group that is configured with installation.

- For Primary Extension, the pattern you choose specifies the lines available to the user. Your choice displays in the **Primary Line** column on the **Users** list view.
- User Language and Role is set up in the Site Defaults of the user's site hierarchy. If this is not specified, hierarchy defaults apply.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Phones settings

On the **Phones** tab/panel you can add or update a user's phone.

To add a phone:

1. On the **Phones** tab/panel, click **Add**.
2. Provide a device name, description, product type, device protocol, phone button template, and device security profile.

   Note: Values for the following fields are dynamic, and change based on options selected in associated fields.

   - Product Type
   - Device Protocol
   - Phone Button Template
   - Device Security Profile

   For example, when adding a device name with the product prefix and MAC address, a 79XX-type phone has device name 'SEP' prefixed, while ATA-type phones have 'ATA' prefixed to the MAC address. Field validation and tooltips provide guidance when you select the product type.

   Note that the device names for hard phones have prefix SEP or BAP, depending on device type.

   The phone type must support the protocol, or it defaults to the protocol option set up in the site defaults. Some phone types support multiple protocols (for example, Cisco 7960 with SCCP and SIP), and some phone types support only one protocol (for example, Cisco 9971 with only SIP). See *Site defaults*

3. Click **Save**.

Consider the following when adding a phone:

- You can override the **Phone Button Template** value. Either choose another option, or type in a custom value. The value is applied on Unified CM if the Unified CM allows it for the phone type.
- Modify phone-specific settings, such as **DND Option**, **Do Not Disturb**, and **Hot Line Device**.

  Note: Available phone settings depend on the selected product type (phone type), the device protocol (for example, SIP or SCCP), and the Field Display Policy (FDP) applied by the administrator.

- You can choose a Mobile User ID Name from the drop-down list when a Dual-Mode Phone for Android or iPhones is selected. This associates the selected user to the Mobile Identity feature on this phone and must match the Userid added on the **User** component.
- Advanced settings fields are updated automatically for the phone based on the phone type. The phone is automatically associated to the user and is then displayed as an associated device for the user after you save.

  When associating a phone that is also associated with another user, the Owner User ID defaults to the first user.
- Line assignments are added in the **Line** section:
  - The **Pattern** field only shows lines with status *Available* or *Used*.
  - Pattern options in **Route Partition Name** are based on the selected partition selected. You can type in a custom pattern value.

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Enduser** - identifies the user for Presence; you can add a new User ID

    Note: Automate adds the user first and then adds the User ID.

- Speed dial information is added in the **Speeddial** section. Available options depend on the selected Phone Button Template.
- Busy lamp field information is added to the **Busy Lamp Field** section. Options include:
  - Position
  - Label
  - Blf Destination
- Add busy lamp field directed details in the **Blf Directed Call Park** section. Values depend on the values on a valid Directed Call Park on Unified CM.
- Specify add on modules (if any) in **Add On Module**. The phone type must support the model you choose. Leave **Load Name** blank, unless you want to overwrite the default.
- Add a valid IP phone service subscription to the phone, in the **Services** section:
  - Choose the IP phone service from the **Service Name** field.

    Note: Subscribing a phone or a device profile to a service auto-populates the **URL** field in **Services**. To populate this field, when a service is added or updated the system retrieves the URL and a custom parameter (if any) from `device/cucm/IpPhoneService`.

  - To add the service to the device, add a number as the Uri button index to the **Url Button Index** field. If you don't add a number, only the service is added.
- In the **Mobile Identity** section, configure mobile identity details when selecting a Dual-Mode Phone.
  - These fields are auto-populated from the **Device Name** field: **Name**, and **Dual-Mode Device**.
  - Choose a mobility profile.
  - Mandatory. Specify a value for **Destination Number**. This option determines the destination number that is dialed when a call is made to the dual-mode phone.
- In the **Remote Destination** section, to configure your remote destinations when a Dual Mode Phone or Cisco Spark Remote Device is selected as the **Product**.

  Note:

  - Remote destinations represent the mobile (or other) phones that are able to accept transfer from the desktop phone and can be used to initiate calls. Set the Pattern for the Line Association to the Route Partition name. If you enter more than one Pattern and the new Pattern is not on the system, enter the Route Partition Name manually. The **Owner User Id** and **Dual Mode Device Name** fields are auto populated.
  - When a CTI Remote Device is selected as the **Product**, a **CTI Remote Destination** section replaces **Remote Destination**. This allows you to configure your remote destinations specifically for a CTI Remote Device. The **Owner User Id** and **CTI Remote Device** fields are auto populated.

- In the **Vendor Config** section, view and edit the configuration settings for each device. Available configuration settings depend on each product type chosen. Update the settings as required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note:

- The administrator password from the `AdminLoginDetails` in UCM is not stored in Automate. Data in Automate obtained from UCM.
- Automate cannot disable the `Override Enterprise/Common Phone Profile Settings` setting once this check box is enabled in the UCM GUI. This setting may be disabled on UCM (if required).

Related topics

- *Site defaults*
- *Manage number filters*
- Global Settings in the Core Feature Guide

Headset settings

The headset can be connected to a device associated with a user, so that the **Connected Device Name** reflects this device. The available headset details are:

- **Headset Serial Number**
- **Headset Model**
- **Connected Device Name**
- **Connected Device Model**
- **Headset Connection Status**: for example "Connected".

Extension Mobility settings

The **Extension Mobility** component configures a user's extension mobility settings.

Consider the following:

- Only one EM Profile can be added for extension mobility in Automate. If a user is associated with more than one EM profile on the Cisco UCM, and you sync with Automate, both will be displayed:
  - on the user's EM component (this component)
  - on the **Extension Mobility** list view (see *Add an extension mobility profile*).
- Values for the following fields are dynamic, based on selections in associated fields:
  - Product
  - Protocol
  - Phone Button Template

Note: For details of configuration options on this component, see the descriptions for the **Phones** component. The exception is remote destination information, which is not relevant for extension mobility.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Ensure that you associate the extension mobility profile and target phone for login with the extension mobility service.
- If the Enable Extension Mobility Cross Cluster (EMCC) feature is enabled on the **User** settings, you must choose a CSS for this device from the **Extension Mobility Cross Cluster CSS** drop-down. The selected CSS is used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. New CSS's or existing CSS's can be added or modified in Cisco UCM. Refer to the Cisco Unified Communications Manager Features and Services Guide for more details if required.

See also *Add an extension mobility profile* to add or edit an extension mobility profile, and associate it to one or more users.

Single Number Reach settings

On the **Single Number Reach** settings, note that you cannot add more than one Remote Destination Profile for Single Number Reach. However, you can add more than one Remote Destination Rdp.

To enable Extend and Connect in Automate, first complete the following task:

1. Select the **Enable Extend and Connect** checkbox.
2. Select the CTI remote device that you created from the **CTI Remote Device Name** drop-down list.

Voicemail settings

The **Voicemail** component configures the user's voice mail service, provided a valid Cisco Unity Connection server is available.

When configuring voicemail:

- PIN and Password can be left blank. In this case, the default credential policy on the Cisco Unity Connection is used.
- If the user on Cisco Unity Connection is LDAP integrated, the **Password** field is visible but should be ignored.
- The **Voicemail Line** drop-down list only shows lines with status 'Available' or 'Used' that are not already configured for Voicemail.

  Note: The Cisco Unity Connection (CUC) server uses this line as a caller ID, so you should set it to the user's default line.

- When adding Voicemail for a user, all **Call Forward To Voicemail** checkboxes, except **Call Forward All**, are enabled on the chosen Line, and the Voicemail Profile setting will be set based on the Site Default Doc setting "Default UCM Line Voicemail Profile" (**Line Defaults**).

Copyright © 2025 VisionOSS Limited. All rights reserved.

WebEx settings

The **WebEx** component configures the user's Webex details, if a valid server is available. The mandatory fields on this component are populated with the values entered on the **User** settings.

Note: Any updates on the **User** settings don't update these values; values are populated only during the Add workflow.

Webex App settings

The **Webex App** settings add a Webex App User and enables a user's services and roles.

Consider the following:

- Webex App is only available when:
  - A Webex App Service has been created at the required customer level (see *Webex Application Access (Webex Organization)*)
  - Webex App is enabled in the Entitlement Profile associated with the user.
- The following fields are read only and cannot be edited:
  - **Login Enabled**
  - **Invite Pending**
  - **On-Prem UCM Calling Service** (managed automatically by the Webex driver)
- **Assigned Licenses** can be selected from the available licenses on the Webex App service.
- Once you have successfully added the user as a Webex App user, the Webex App column displays status *Enabled* for this user.
- The user's e-mail address is required to enable Webex App for the user.

Pexip Conference settings

The **Pexip Conference** component adds and configures the user's Pexip services.

Consider the following:

- The **Pexip Conference** component is only available if a Pexip Conference service has been configured at the required hierarchy (via the Quick Add Group).
- Conferencing must be enabled in the entitlement profile associated with the user.
- Once a user is successfully added as a conferencing user, you can view the service as an enabled service in the **Conferencing** column on the **Users** list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Contact Center settings

On the **Contact Center** settings, you can add, remove, or update CCX agent capabilities for a user.

See also: *Contact Center*

The **Contact Center** settings display only if these conditions are met:

- CCX device has been added and is available to the hierarchy.
- Contact Center Service is configured and available to the hierarchy.
- Contact Center is enabled in the entitlement profile associated with the user.

For the agent:

- Since CCX restricts the use of special characters, these are restricted in the **Alias**.
- **Team**, **Resource Group** and **Skill** names need to be set up or synced from the CCX device before they can be assigned.
- **Automatic Available** is enabled by default.
- An IPCC extension is automatically managed for the Unified CM user associated with the Contact Center Agent.
- You may change the agent's **Controlled Device** to one that is already associated with the user.

Update a user

This procedure modifies settings for one or more users.

1. Log in as a Customer or Site administrator.

   Note: Only a subset of fields described in this procedure are visible to Site admins.

2. Choose the relevant site.
3. Go to **Cisco Advanced User**, or **Multi Vendor User**
4. Click on the relevant user to open their settings.
5. Make the changes you require. For details, see *Add a user*.

   Note:

   - You can add one or more phones.
   - If Extension Mobility is associated with more than one user, it will not be removed when removing it from one user.
   - Phone line settings can be edited directly on the **Users** page.

     Expanding the **Line** section of a Phone or Extension Mobility Profile displays a link directly to the line editing form. Once you've saved your changes, the User edit page re-opens.

     If your menu layout has more than one entry for `relation/LineRelation` and associated Field Display Policy, the link for the line edit applies to the first one found (searching from top to bottom) in your menu layout (if available).

6. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note:

- Filtering on the following columns on the Users list view is described in more detail below:
  - Located At

    Displays an abbreviated version of the hierarchy showing the lowest point in the hierarchy. The hierarchy type is shown in brackets. When filtering on this column, do not use text included inside the brackets in the filtering criteria. For example: “SiteName (Site)”, where (Site) = the hierarchy node type, only search using the “SiteName” portion of the field.
  - Device

    Allows you to filter on IP Address or Host Name.
  - Phone

    When filtering on this column, results include all phones at the current hierarchy, and below, regardless of the Phone column in which they reside.
- On saving a user, workflows will execute which will synchronize the user with its associated application: LDAP(top-down), Webex, UCCX, etc.

Deleting users

Overview

Users are deleted via **Cisco User** / **Cisco Advanced User**.

The system performs various actions when deleting a user via User Management. These actions depend on the user type and the user’s device associations.

User types

User types	Description
Non-LDAP synced users	• Users created in Automate and pushed to Cisco UCM • Users provisioned in Cisco UCM and synced in to Automate
LDAP integrated at Automate users	• Users that are LDAP integrated at Cisco UCM and synced in to Automate
LDAP synchronized users	• Users directly synced from an LDAP server to Automate.

Copyright © 2025 VisionOSS Limited. All rights reserved.

User associations

Users can have no device associations, or they can be associated with devices such as the following:

- Phones
- Extension mobility
- Single Number Reach (SNR)
- Voice mail
- Webex

Automate actions when deleting a user

The system performs these tasks when deleting a user via the **Users** page, depending on the user type and whether the user has associated devices:

User Type	With Devices	Without Devices
Non-LDAP Synchronized Users LDAP Integrated at Cisco Unified CM Users	Deletes all devices: • Phones: device/cucm/Phone • Single Number Reach: device/cucm/RemoteDestinationProfile • Extension Mobility: device/cucm/DeviceProfile • Voicemail: device/cuc/User • WebEx: device/WebEx/User Deletes the Provisioning Status.	Deletes the Provisioning Status.
LDAP Synchronized Users	Deletes all devices: • Phones: device/cucm/Phone • Single Number Reach: device/cucm/RemoteDestinationProfile • Extension Mobility: device/cucm/DeviceProfile • Voicemail: device/cuc/User • WebEx: device/webex/User Deletes the user from Cisco Unified CM: device/cucm/User Removes the Cisco Unity Call Manager from the Provisioning Status.	Deletes the user from Cisco Unified CM: device/cucm/User Removes the Cisco Unity Call Manager from the Provisioning Status.

Important: You can configure Automate to retain desk phones (hard phones, prefixed SEP or BAP) associated with a user you're deleting, and to update these phones via a configuration template (CFT) once the user is deleted. To do this, go to **Global Settings**, and on the **Phones** tab, set **Retain Desk Phones when User is deleted** to **Yes**, then select an option for applying a CFT to update the retained phone/s.

You can also configure that Webex accounts and Voicemail accounts associated with deleted UCM users will be retained (or removed) in the LDAP user sync that handles deleted UCM users. This is done via the **Global Settings > Webex App** tab or **Voicemail** tab, as applicable).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Global Settings in the Core Feature Guide
- User, Phones tab in the Core Feature Guide

Delete a user

This procedure deletes and unprovisions a user.

1. Log in to the Admin Portal as a Customer admin or Site admin.

   Note: Only a subset of fields described in this procedure are visible to Site admins.

2. Choose the relevant site.
3. Go to **Cisco Users** or **Cisco Advanced User**.
4. Select the checkbox for each user you want to remove; then click **Delete**.
5. Click **Yes** to confirm.

   The deleted user is removed from the list. All elements associated with the user are removed, except lines.

Note:

- If you have the global setting for phones configured to retain the user's hard phones, then only the soft phones are removed. See *Global Settings* in the Core Feature Guides (Phones tab).
- For scenarios that include an LDAP-integrated Cisco UCM, users are deleted from the LDAP directory and not from the Automate system. Set up a data sync to synchronize the removal of the user.

Add Subscribers: User

On the **User** tab, complete fields to add a Unified CM user and a VOSS Automate user.

Consider the following when adding a subscriber:

- Use only alphanumeric characters.
- A selected Entitlement Profile will be associated with the subscriber.
- The options available in the **Service Profile** drop-down menu are those that were imported from Unified CM.
- If an existing phone is to be associated with a subscriber, choose the device from the Associated Devices group.
- After an existing phone is associated to the subscriber in the **Associated Devices** group **Device** drop-down menu, click **Save**. The subscriber is updated so that the **Phones** tab is populated with the information of the new phone associated with the user.
- If the added subscriber is configured as an LDAP user, the **Password** and **Repeat Password** fields are hidden. The **Enable Mobility** check box is auto-enabled if any of the following are included or added: a remote destination phone, mobile identity for a phone, or remote destination profile (RDP).

  Note:

Copyright © 2025 VisionOSS Limited. All rights reserved.

To enable Extend and Connect in VOSS Automate, complete the following task:

1. Select the **Enable Mobility** check box.
2. Add the following three groups of users:
   a. Standard CCM End-Users
   b. Standard CTI Enabled
   c. Standard CCMUSER Administration

- If a Customer is configured for EMCC, and if you want the subscriber to have access to the EMCC feature, select the **Enable EMCC** check box.
- Choose a **BLF Presence Group** for the subscriber from the drop-down. The chosen group specifies the destinations that the subscriber can monitor and is configured in Cisco Unified Administration. BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. The **Busy Lamp** Field default is set according to the selected number and specifies the Standard Presence Group that is configured with installation.
- Choose the primary extension for the subscriber by choosing from the **Pattern** drop-down list, which includes all lines available to the subscriber. The selected option is displayed in the Primary Line column for the subscriber in the **Subscribers** list view.
- The Subscriber Language and Role can be set in the Site Defaults of the site hierarchy that the subscriber belongs to. If not set in the Site Defaults, hierarchy defaults apply.

Reset UC Passwords

Overview

VOSS Automate maintains details of user credentials A VOSS Automate user can also be a corresponding user on a number of devices. In particular, users can have password (and PIN) credentials for:

- VOSS Automate user
- Unified CM (also PIN)
- Cisco Unity Connection (also PIN)
- LDAP user on Unified CM
- LDAP user on Cisco Unity Connection
- Conferencing user - WebEx, Zoom or PexIP (also PIN)

The Reset UC Passwords feature allows you to select a username for a user on Unified CM at a selected hierarchy and then, given the configured services for the user, you can select a check box to reset the user's password and/or PIN for the services.

The feature can be used by an administrator at the provider, customer and site hierarchy. It will, given a selected username, also enable options to select other devices for password modification and also displays notices or warning messages to indicate available devices and exclusions.

For example, the password of a Unified CM user that is also an LDAP user, cannot be modified. Such a user is also not a VOSS Automate user. In other instances, the VOSS Automate password is also reset when a user's device password is reset.

If a user is an LDAP user on either Unified CM or Cisco Unity Connection and they are selected, then only the PIN for the device will be reset.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: When bulk loading updates to passwords,the bulk load sheet only needs to specify values for the user and updated passwords - other fields can be left blank. See: *Bulk loading files*.

Reset a UC Password

1. Log in as the provider, customer or site administrator and navigate to the hierarchy at which the Unified CM is available.
2. Choose **Subscriber Management** > **Reset UC Passwords**.
3. Choose the username on Unified CM from the User drop-down list.

   The **User First and Last Name** field will show the selected user's first name and last name.
4. Check boxes will show for the selected user according to the associated devices. The devices can be:
   - Reset CUC
   - Reset WebEx
   - Reset CUCM
   - Reset Pexip
5. Select the check boxes for the devices on which the user's password or PIN needs to be changed. Note that a PIN can only be reset for CUCM, CUC or Pexip, not for WebEx or VOSS Automate, because these have no PIN functionality.

   Read the displayed Password or Pin notices and warnings. The messages show the conditions as to when passwords and PINs will be reset.

   Note that the content of these messages must be inspected as the check boxes are selected or or cleared, because the conditions change according to the status of the check boxes.

   If no check boxes are selected, then only the VOSS Automate password can be changed. If the user is an LDAP user on either Unified CM or Cisco Unity Connection, then only the PIN for the device can be changed.
6. Click **Save**.

Provision the Pexip Conference service

Tip: *Use the Action search to navigate Automate*

Prerequisites:

The **Pexip Conference** tab is only available if:

- Pexip Conference service is configured and is available to the hierarchy (via the Quick Add Subscriber Group).
- Entitlement Profile: the **Conferencing** checkbox is selected and associated to the subscriber.

Perform these steps:

1. In the Admin Portal, go to **Subscribers** to open the list view, then click the name of the subscriber to be provisioned with Pexip Conference service.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Select the **Pexip Conference** tab.
3. In the **Pexip Conference** field, click the Plus icon (+) to open the Pexip Conference configuration settings.
4. Configure Pexip Conference, as required, for example:

Field	Description
Description	The name of the conference: contains the Subscriber username
Host PIN	4-20 digits, including any terminal #.
Allow Guests	Enables Guest PIN input. If enabled, the same digit specification as Host PIN applies.
Guest PIN	4-20 digits, including any terminal #. Allows you to set a secure access code for Guest participants who dial in.
IVR Theme	A theme for the conference can be selected or else the default applies.

   Refer to the interface tooltips and for details on all the form fields.

5. Click **Save**.
6. To verify, go to **Quick Add Subscriber** and select the same user from the **Username** drop-down list or verify on the **Pexip Users** menu.
7. Choose the **Existing Services** tab.
8. Make sure that "ACTIVATED" appears in the **Pexip** field.

If the subscriber is deleted, the **Pexip Conference** is either retained or also deleted - according to the Global Settings setting See: *Global settings*.

Related topics

- *Pexip Conference Users*
- *Add a Pexip Virtual Meeting Room (VMR)*

Pexip Conference Users

Overview

Pexip is a conferencing platform that provides users with their own personal Virtual Meeting Rooms (VMRs) to hold conferences, to share presentations, and for chat.

Virtual Meeting Rooms are set up as a part of VOSS Automate user management.

VOSS Automate integrates fully with Pexip, providing access to the following:

- *Add a Pexip server*
- Set Up and Manage Pexip Virtual Meeting Rooms and Conferencing:
  - *Add a Pexip Virtual Meeting Room (VMR)*
  - Provision the Pexip Service: *Provision the Pexip Conference service*

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - IVR Theme for a Pexip Conference
- Resetting the Pexip PIN (see *Reset a UC Password*)
- Pexip Conferencing upon subscriber deletion: *Global settings*

Related Topics

- *Add a user*
- *Cisco Quick User*
- *Provision the Pexip Conference service*

Add a Pexip Virtual Meeting Room (VMR)

1. In the Admin Portal, go to (default menus) **Subscriber Management > Pexip Conference Users**.
2. View existing Pexip VMRs on the summary list view.
3. Click **Add**.
4. Select the relevant site.
5. On the **Virtual Meeting Room** tab:
   - Mandatory. Fill out the **Name** and **Owner's email address** fields.
   - Configure optional settings:
     - Fill out a description.
     - Set a host PIN.
     - Select **Show names of participants**.
     - Select **Allow Guests**, and set a guest PIN.
     - At the **View** drop-down, choose the conferencing view layout that participants will see.
     - At **IVR Theme**, choose a theme to use with this service.

   Note:
   - The host PIN can be reset. See *Reset a UC Password*.
   - Selecting **Allow Guests** displays an additional field where you can enter a guest PIN.

6. On the **Advanced options** tab, configure the following optional settings:
   - Define whether guests can present, in addition to the host
   - Enable chat
   - Define maximum inbound and outbound call bandwidth
   - Set maximum media content (Conference capabilities). Options are: Main video + presentation, Audio-only, Main video only
   - Define maximum call quality for participants
   - Define media encryption settings.
   - Set a participant limit

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Set a service tag (a unique ID to track how this VMR is used)

7. On the **Alias** tab, configure one or more conference aliases.

Note: The alias is a dial string used to join the service, in the form that Pexip will receive it, including a domain, which is automatically added by the participant's endpoint or call control system, or dialed by the participant.

8. Click **Save**.

Note: The new VMR is added to the Virtual Meeting Rooms list view from the Services on the Pexip Conferencing Platform. Any changes to the VMR on the Pexip Conferencing Platform will also update the VMR in VOSS Automate.

8.3.2. Phone Quick Actions

Smart add phone

Tip: *Use the Action search to navigate Automate*

Overview

Automate's *Smart Add Phone* functionality allows you to add a phone *only to a site hierarchy node* by selecting the phone template that matches the required phone product. This selected phone template then also adds associated default attribute values. Optionally, you can also choose to add one or more lines and a non-default phone button template for the phone.

When a phone is added using *Smart Add Phone*, the phone details that were added by the phone template can be seen and modified if needed by selecting the phone from the **Phones** list.

If you need a customized phone template, the default template can be cloned, renamed and modified via the **Configuration Templates** page. This customization is then available in the **Phone Template** drop-down of the **Smart Add Phone** page.

The line defaults are obtained from the Site Defaults doc for the site. The default CUCM line partition must be set as the partition for the site.

Note: A cloned, custom phone template requires further customization in order to customize the line settings when it is used with *Smart Add Phone*. For details, refer to the topic on Custom Line Settings for Smart Add Phone Configuration Template in the Advanced Configuration Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a phone using Smart Add Phone

The *Smart Add Phone* feature is only available at a site hierarchy node.

1. Log in as an administrator.
2. Go to **Smart Add Phone**.
3. Choose the site where you want to add the phone.
4. Choose the **Phone Template** value that matches the phone to add. The Phone Product and Protocol values are input automatically and become read-only.
5. Optionally, choose a non-default **Phone Button Template** value for the phone, if one is available.

   You can override the default **Phone Button Template** value by entering a custom value in the **Phone Button Template** field. The entered value will be applied on CUCM if the CUCM allows it for that phone type.
6. Complete the device name. Based on the selected phone template, the **Device Name** prefix is added for the phone.
7. Optionally, add one or more lines to associate to the phone. The **INI Enabled** field shows if the Internal Number Inventory is enabled for the site or not and the **Default Line Partition** field indicates which default line partition has been set in the Site Defaults doc.

   The **Lines** input is enabled if the default Route Partition value for the site has been set in the site's Site Defaults Doc.

   - If **INI Enabled** is **YES**, then choose a number from the drop-down list of numbers from the Internal Number Inventory. Numbers that are marked as used, are also shown. Lines that are selected have additional properties set according to the Site Defaults Doc for the site.
   - If **INI Enabled** is **NO**, then the list of numbers are those Directory Numbers on CUCM with the Route Partition matching the site. You can choose a number from the drop-down or add a custom number that is not in the drop-down list, in other words, you can type in a number. Lines that are added have additional properties set according to the Site Defaults Doc for the site.
8. Click **Save**.
9. Go to the **Phones** page to view and modify the phone that is added using Smart Add Phone.

   Added lines are shown on the **Lines** tab of the **Phones** page. The line labels have the format: *<firstName> <lastName> <number>*, or a part of this format if *<firstName>* or *<lastName>* are not input.

Related Topics

- *Reserve numbers for a user*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Move Phones

provider

Tip: *Use the Action search to navigate Automate*

Overview

You can move phones between sites only if they are not assigned to users.

Moving a phone between sites handles the situation where a phone is either physically moved or logically assigned to a different site.

If a phone is assigned in the Associated Devices list of a CUCM user, the phone is moved during a user move. See *Move users*

Restrictions that apply when moving phones

You can only move phones when the following conditions are met:

- The phone you wish to move must not be assigned to a user
- Phones can only be moved from one site to another site:
  - Phones can't be moved from a customer to a customer.
  - Source and target site must reference the same NDL
  - Source and target site must have the same type of dial plan
  - Source and target site must have the same country

When moving a phone with an intercom line, the line is not moved or updated.

Related topics

- *Reserve numbers for a user*

Move a phone

This procedure moves one or more phones.

1. Log in as a provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer whose phones you are moving.
3. Go to **Move Phones**.
4. At **Action**, choose an option:
   - Move phones by name (bulk move):
     - Choose the source hierarchy (site from where you're moving the phones).
     - Choose the target hierarchy (site).

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - If you're moving all phones, select **Move All Phones**. Alternatively, select the phones to move.

    Click the Plus icon (+) at **Phones**, then choose a phone. You can type the first part of a phone name to filter the list. Repeat this step to choose additional phones to move.
  - Click **Save** to move the phones.
- Move phone by name (move one phone):
  - Choose the phone.
  - Choose the target site.
  - Click **Save** to move the phone.

5. To verify that the phone or phones were moved to the correct target site, go to **Phones**.

Moving phones from site to site

provider

Tip: *Use the Action search to navigate Automate*

As an administrator, you can move phones from one site to another.

Certain conditions must be met for a site-to-site move to succeed. When moving a phone between sites, Automate checks the following:

- The source and target sites must reference the same NDL
- The source and target sites must have the same country configured
- The source and target sites must have the same type of site dial plan deployed
- Whether the phones are assigned to users
- Whether the phones are under same customer
- Whether the phones are moving between sites

Note: Quick Add User with phone/line/EM/SNR/voicemail can be added to site and moved across the sites within the same country.

Models and Relations Moved (SLC)

For moves between sites with SLC type dial plans:

- `device/cucm/Phone` (includes `device/cucm/Line`)

Note:

- Lines are disassociated from the phone
- Warnings are logged for any lines associated with the phone

---

Models and Relations Moved (Non-SLC)

For moves between sites with non-SLC type dial plans:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `device/cucm/Phone`
- `device/cucm/Line`
- `device/cucm/InternalNumberInventory`

Note: Warnings are logged for any lines associated with:

- an E164 Inventory
- a Call Pickup Group
- a Hunt Group
- a Remote Destination

Moving Phones Between Non-SLC Sites with a DNR Configured

For moves between non-SLC sites with directory number routing (DNR) configured at *either* site, a warning appears stating that any lines associated to the phone being moved may not work correctly unless you take one of the recommended actions provided. See the Advanced Configuration Guide to perform the first recommended action.

Note:

- To see warning messages navigate to **Overbuild > Log Messages > Phone Move Logs**
- Movement of phones from Non-SLC to Non-dial plan site will not dissociate the lines, but movement from SLC to Non-dial plan site will dissociate the lines.

To support the Overbuild Tool for Managed Services, the certain fields are updated in the Phone and Line devices to the target site's default settings.

Within `device/cucm/Phone`, the following models and fields are updated:

- Phone
  - Device Pool Name
  - Location Name

Within `device/cucm/Line`, the following models and fields are updated:

- Line
- Call Forward All
  - Calling Search Space
  - Route Partition Name
  - Share Line AppearanceCssName

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure Phone Move Customizations

hcs-admin

If you have added customized models to VOSS Automate, you can configure the customizations to move with phones between sites. The default customizations will be applied when a phone move is executed.

Note: You can configure only one move-phone customization per hierarchy.

1. Log in to the Admin Portal as `hcsadmin`.
2. Go to **Default Move Phone Customizations**.
3. Enter a name (required) and description for the customizations.
4. Add one or more customizations for each group of lines that moves with a phone from one site to another:

   Displayed fields depend on the customization type selected. The table describes customization options:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Customization Operation	• Move/Execute Before Group - choose to move the customization before the corresponding group. • Move/Execute After Group - choose to move the customization after the corresponding group. • Update After Move - choose to apply the chosen configuration templates to the chosen data models after all the moves in that group finish.
Customization Type	Choose the customization type. You can move the following customization types: • DataModel • DomainModel • Device • Relation You can execute the following customization type: • ProvisioningWorkflow Note: For any group, if **Update After Move is** selected as the Customization Operation, selecting Relation or Provisioning Workflow as the Customization Type is not allowed. A note appears prompting you to choose another model type.
Customization Name	Choose the instance of the Customization Type you selected.
Customization Field	Choose the field to link to existing context models.
Context Model	Choose one of the following existing context models to link the new model to: • relation/LineRelation • data/InternalNumberInventory • device/cucm/Phone • device/cucm/Line
Context Field	Choose the field of the existing context model that is linked to the Customization Field.
Configuration Template	Choose the Configuration Template to apply to the chosen model.

5. Choose another customization for the same group, or select a customization for another group.

Note: If you select multiple customizations with the same Customization Operation for the same group, those items are moved in the order you specify them here. Use the up and down buttons to reorder your customizations.

6. When you have chosen all the customizations for the phone move, click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

PLAR (Hotdial)

Overview

Private Line Automatic Ringdown (PLAR), also called Hotdial, automates the Cisco Unified Communications Manager (CUCM, or CallManager) configuration required to set up PLAR for a phone.

PLAR provides an administrator with a single interface and workflow for managing the following parts of CUCM:

- RoutePartition
- CSS
- TransPattern
- Phone
- Line
- SIP Dial Rule

Additionally, the PLAR feature provides an administrator with the following:

- A simplified user interface to choose:
  - A phone that must be enabled for PLAR
  - A destination number
  - The destination CSS
- A workflow that creates and applies a number of elements to the relevant phone and number. These elements include:
  - The required CUCM partition
  - CSS
  - Translation pattern

To configure an existing phone for PLAR (Hotdial), you choose a pre-existing device and indicate that the device is a Hotdial device.

As soon as a PLAR-configured phone goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a pre-configured destination number. The phone can't dial any other number except the Hotdial destination that is configured for PLAR.

The PLAR configuration can be added or deleted, but not modified.

PLAR (Hotdial) Workflows

When adding a new Hotdial Phone (PLAR configuration), the following workflow is executed:

1. A CUCM route partition is created with:
   a. Name set to the Hotdial Phone selected, prefixed with "HotdialPT-". For example: "HotdialPT-SEP000000000000".
2. A CUCM CSS is created with:
   a. Name set to the Hotdial Phone selected, prefixed with "HotdialCSS-". For example: "HotdialPT-CSS000000000000".
   b. The Partition created above is made a member of the CSS.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. A CUCM translation pattern is created with:
   a. Partition name is set to the Partition added, prefixed with “HotdialPT-“, for example: “HotdialPT-SEP000000000000”.
   b. Calling Search Space Name set to the selected Destination Dialing CSS.
   c. Called Party Transformation Mask is set to the selected Hotdial Destination Pattern.
   d. Route Option is set to Route this pattern.
   e. Urgent Priority is enabled.
4. The CUCM phone selected is updated as follows:
   a. For SIP Phones only, a SIP Dial rule is created and the phone is set to use the SIP Dial Rule.
   b. CSS name is set to the “HotdialCSS-” added for the phone.
   c. Hotline Device is set to true if the phone is marked as a Hotline Device by the user on the input form.

VOSS Automate automatically resets the phone when required.

When deleting PLAR (Hotdial) for a phone (deleting the PLAR configuration), the following workflow is executed:

1. Update Phone CSS to the original CSS.
2. Delete the Hotdial Translation pattern.
3. Delete the Hotdial CSS.
4. Delete the Hotdial Route Partition.
5. For SIP Phones only, the device is updated to use a Dial Rule of “None”, and the Dial Rule is deleted.

EM Login/Logout

VOSS Automate allows a site administrator (or higher) to log a user in to or out from one or more phones configured for extension mobility (EM) at the Customer or Site hierarchy level.

Note: For the feature to work, the phone must be enabled for Extension Mobility **and** the user must have Extension Mobility (Device Profile).

Login User

Log a user in to a phone taking note of the following:

- The **User Name** drop-down (mandatory) contains only users who have Extension Mobility (Device Profile).
- The **Device Profile Name** drop-down is auto populated with the user’s first Extension Mobility (Device Profile). If the user has more than one Extension Mobility (Device Profile), choose the profile to use from the drop-down.
- The **Phone Name** drop-down (mandatory) contains only phones that are enabled for Extension Mobility.
- A **Login Duration (in minutes)** of ‘0’ (default setting) indicates that the user will remain logged in to the phone indefinitely. Enter, for example 180, if you want to log out the user from the phone after three hours.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **Status** field indicates either the currently logged in user or 'No User Logged In'.
- If you try to log a user into a phone that already has a logged in user, the **Force Login** check box is displayed. Select this check box and click **Save** to simultaneously log out the existing user and log in the new user.

Logout User

To log a user out from a phone:

1. Choose the **Phone Name** from which you want to log out the user and click **Save**.
2. The **Status** field displays either the currently logged in user or 'No User Logged In'.

Logout User from Phones

1. From the **User Name** drop-down (mandatory), choose the user you want to log out from a phone.
2. Move the phone/s from the 'Available' area to the 'Selected' area and click **Save**.

Replace phone

Note: This software release currently only fully supports the replacement of an existing desk phone type with any other desk phone type.

Tip: *Use the Action search to navigate Automate*

Overview

You will need to replace a phone when choosing a new phone for a user or when a phone type is no longer supported.

The feature provides an easy way to replace an existing (old) phone with a different phone model, while retaining as much of the old phone's configuration as possible.

Phone replace does the following:

- Copies the old configuration
- Deletes the old phone
- Adds the replacement (new) phone along with the old configuration
- Updates user information to reflect the change in the controlled devices

Note:

- Speed dial, Busy Lamp Field (BLF), Blf Directed Call Park, and Services settings are *not* copied from the old phone configuration. Configure these settings manually on the appropriate tab on the replacement phone **Phones** screen if required. See "Configure Phones".

Copyright © 2025 VisionOSS Limited. All rights reserved.

- If the new phone has attributes that weren't present on the old phone, you must manually set the required values if the default values are not appropriate. Alternatively, you can select an optional configuration template, which will override the configuration copied from the old phone as well as any manual settings.

If you need a customized Phone Template, a default template can be cloned, renamed, and modified via the **Configuration Templates** page. The new customized template is then available in the **Phone Button Template** drop-down of the Replace Phone feature.

The `Replace Phone Template Variable` template is available to allow for the option of manual input of the following fields:

- `phoneTemplateName`
- `product`
- `protocol`
- `securityProfileName`

Note: When using this template, *only* these fields are configured by the template.

See "Configuration Templates" for more details if required.

Related Topics

- *Reserve numbers for a user*

Replace a phone

To replace a phone:

1. Log in as Site administrator or higher.
2. Go to **Replace Phone**.
3. Choose the relevant site (where you want to replace a phone).

   Note: You can only replace a phone at the Site level.

4. On the **Existing Phone** tab:
   a. At **Device Name**, select the phone you wish to replace.

      Note:

      - Other fields on this form are read-only.
      - When choosing a phone name, you can configure (via the **Phones** tab in the **Global Settings**), how phone names display in this field. For example, the drop-down may list phones by their description only (default) or by first line only, or by description plus first line. At this drop-down, you can search for the phone using relevant criteria, for example, first letters of a description or line numbers (depending on the Global Setting for phone display).

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. On the **Replacement Phone** tab:
   a. Enter the **Device Name** of the replacement phone (mandatory).
   b. Optionally, choose a **Phone Template** for the replacement phone.

      Note: Values in the phone configuration template you choose will override attributes copied from the original phone, and any additional, manually applied settings in the rest of the fields on this tab.

   c. Choose the **Product** (phone model) of the replacement phone (mandatory).

      Note: If the existing phone was associated with an entitlement profile, the replacement **Product** drop-down only displays phone types that are allowed by the entitlement profile.

   d. Choose the **Device Protocol** (mandatory).
   e. Choose a **Phone Button Template** value for the replacement phone, if one is available (optional).
   f. Choose the **Security Profile** for the replacement phone (mandatory).
   g. Enter a **Description** for the phone (optional).
5. Click **Save**. View transaction progress and details in the Transaction Logs. See Transaction Logging topic.

Related Topics

- Global Settings in the Core Feature Guide.
- Transaction Logging and Audit in the Core Feature Guide.

VOSS phones

Tip: *Use the Action search to navigate Automate*

On the **VOSS Phones** page, phones are associated with the VOSS Phone Server (see *Introduction to VOSS phone server* and *Managing VOSS phone servers* in the Core Feature Guide.

- **Vendor**: all vendors configured in the library of phone types are offered. See *Add phone types* in the Core Feature Guide.
- **Model**: the phone model is selected. See See *Add phone types* in the Core Feature Guide.
- **Number of Lines**: available number is chosen.

These parameters are used to determine the template to use when creating the phone configuration file on the TFTP server.

- **Phone MAC Address**: required, with no vendor prefix as would be used with CUCM. E.g use `123412341234`, not `SEP123412341234`.
- **Group**: is selected. This represents the SIP realm to use for registration. Typically there will be a single realm or group for a customer, although more advanced configuration is possible and may be added to the Phone Server.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Line**: each line has the following parameters:
  - **Number**: The directory number from number inventory. Numbers can exist on Phone server phones or CUCM phones, but not both.
  - **Display Name**: The display name for presentation when making a call
  - **Busy trigger**: As per CUCM phones
  - **Max Calls**: As per CUCM phones
  - **Class of service**: This is the class of server as created by the CUCM dialplan. CoS is enforced on CUCM when using HCS mode.

Add controlled device to Cisco user

Tip: *Use the Action search to navigate Automate*

This procedure associates a user with a phone or device profile.

1. Log in to the Admin Portal, then go to **Add Controlled Device to Cisco User**.
2. At the **Username** drop-down, choose a user.
3. At **Device Type**, choose device (association type), either phone or device profile.
4. At **Device Name**, choose an option from the drop-down. Options depend on the device type you selected.

   Note: Phones and device profiles available in the drop-down are only those that are currently unassociated (phones that don't have an owner, or un-managed device profiles).

5. Click **Save**.

   The device is added to the user as a controlled device and the device itself is updated with the owner ID and line owner, as applicable.

8.3.3. Detailed User Service Listings

Voicemail

Tip: *Use the Action search to navigate Automate*

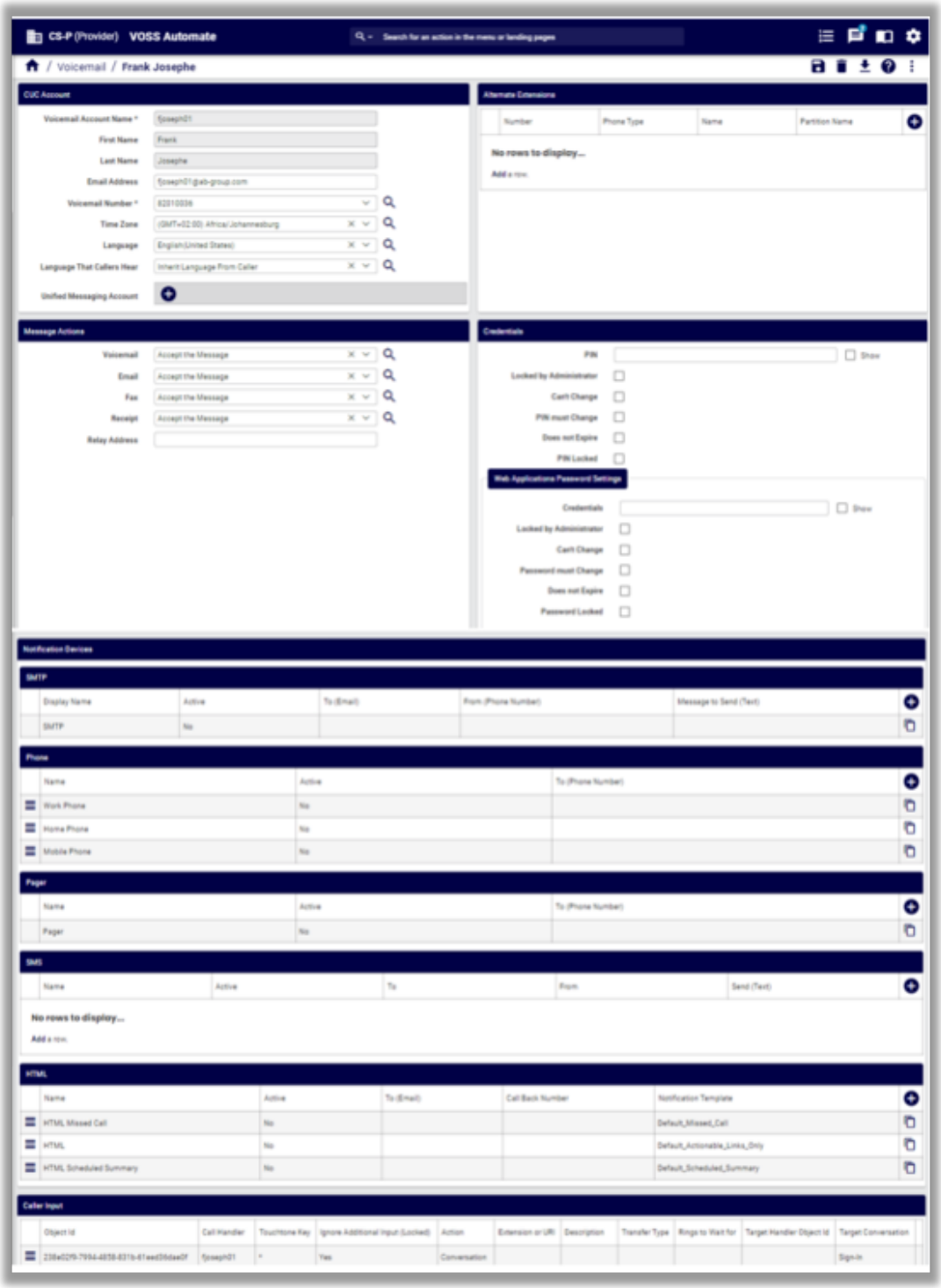
Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate allows admin users to add, update, or delete Cisco Unity Connection (CUC) voicemail accounts (voicemail users), and their associated voicemail services, via the **Cisco Voicemail Users** page.

Note: Optionally (depending on your deployment), Automate supports a Unity SIP integration feature that can be used in place of your existing voicemail service. See *Introduction to Unity SIP integration*

Copyright © 2025 VisionOSS Limited. All rights reserved.



Important: Users and associated services added through Automate are also added to Cisco Unity Connection (CUC) voicemail system.

If a user identifier is updated on the CUC integrated LDAP server, the alias update on the CUC server is deferred to the next LDAP-CUC sync. The alias change is then synced in to Automate in the Automate-CUC sync that follows the LDAP-CUC sync. The updated alias displays in the CUC Account settings, in the

Copyright © 2025 VisionOSS Limited. All rights reserved.

Voicemail Account Name field.

Related Topics

- Call Handler (Auto Attendant) in the Core Feature Guide

Unified Messaging account

Unified Messaging (Single Inbox) is a Cisco Unity Connection (CUC) service that enables users to have a single inbox in their e-mail client that is used for their e-mail as well as their Voicemail.

Note:

- Automate only supports either the Exchange or Office 365 Unified Messaging Service, MeetingPlace is **not** supported.
- Only *one* Unified Messaging Account (Single Inbox) per user can be added by Automate. However, if an existing CUC user is imported into Automate already has more than one account, then all associated services are imported, and will be available in Automate.
- Administrators must manually sync Automate with Cisco Unity Connection to obtain the required Unified Messaging Services. A manual sync must also be done whenever changes are made to the Cisco Unity Connection server.
- Automate does not automatically integrate CUC servers with Microsoft Exchange, the details for that process can be found here: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html

The following CUC settings, set to 'True' (On), are included in Unified Messaging:

- EmailAddressUseCorp - Use Corporate Email Address
- EnableMailboxSynchCapability - Synchronize Connection and Exchange Mailboxes (Single Inbox)

The following two models were added to the Model Type List **CUCXN Overbuild Resources** for Unified Messaging:

- device/cuc/ExternalService
- device/cuc/ExternalServiceAccount (the actual Cisco Unity Connection User's model which contains their Unified Messaging Account)

Automate also added a new model type list **CUCXN Unified Messaging Services**, and added the same two models: `device/cuc/ExternalService` and `device/cuc/ExternalServiceAccount`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add, edit, or delete a voice mail account

Prerequisites:

- The admin adding the voicemail account must be at the relevant Provider, Customer, or Site level.
- A CUC Server (VM Server) must already be provisioned at the Provider or Customer level.
- A Network Device List (NDL) and NDLR points must exist.

Perform these steps:

1. In the Automate Admin Portal, go to **Voicemail**.
2. From the summary list view, choose an option:
   - **Edit an existing voicemail account**

     To edit an existing voicemail account, click on an account in the list, make your changes, and save.

     Note: Edits may involve updating options configured when adding the account, or to add new voicemail services, for example, to add additional alternate extensions and/or notification devices.

   - **Delete an existing voicemail account**

     To delete an existing voicemail account, select the relevant account in the list, or click on it to open its configuration screens, then click the **Delete** button.

     Note: When deleting a voicemail account:

     – All elements associated with the voicemail account are deleted.

     – Modular Delete workflows can be carried out as a part of a Modify workflow.

     – When deleting a voicemail account at the Site level, the related CUCM Line's Park Monitoring and CFWD settings are disabled accordingly.

     – When deleting a voicemail account at the Customer level (that is, recently synced from CUC but not yet moved to Site level), the related CUCM Line's Park Monitoring and CFWD settings *are not disabled*.

   - **Add a new voicemail account**

     To add a new voicemail account, click the Plus (+) icon, then choose a site from the hierarchy picker. Go to the next step to configure the new voicemail account.
3. At **CUC Account**, configure CUC account details, such as voicemail account name (the user), voicemail number, and the language the caller hears. For details, see *Unified Messaging account*

   Note:

   - If a user identifier is updated on the CUC integrated LDAP server, the alias update on the CUC server is deferred to the next LDAP-CUC sync. The alias change is then synced in to Automate in the Automate-CUC sync that follows the LDAP-CUC sync. The updated alias displays in the CUC Account settings, in the **Voicemail Account Name** field.
   - The **Voicemail Number** drop-down only shows numbers associated to the selected user (chosen for voicemail account name).
   - Email address is auto-populated when selecting an existing user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Click the Plus icon (+) at **Unified Messaging Account** to add a unified messaging service. See *Unified Messaging account*. Once saved, the summary header is the user's email address. It is only possible to add one CUC messaging account per user in Automate.

  To change from one Unified Messaging Account type to another, delete the existing entry and click **Save**. Then add the new Unified Messaging Account type in the **Unified Messaging Service** field.

4. At **Alternate Extensions**, add alternate extensions available to the CUC voicemail user, if applicable.
   - Click the Plus icon (+) at **Alternate Extensions**.
   - Enter the number, choose a phone type and partition name, and specify a name for the alternate extension.

   Note: Once you've saved these changes you can log in to Cisco Unity Connection, choose the user you updated, and go to **Edit > Alternate Extensions** to view the alternate extension configured in Automate.

5. From **Alternate Extension** choose the Partition from the drop-down and click **Save**.
6. At **Message Actions**, define how incoming voicemail, email, fax, and receipt messages are handled. If the selected message action involves relaying the message, enter a valid email address in the **Relay Address** field.

   Note: You can accept the default message actions and update them later.

7. At **Credentials**, configure a password and PIN.

   Note: The admin user configuring the account can lock these credentials or require the user to change the credentials on first login. The CUC user password template and CUC user PIN template in the user's Quick Add Group (QAG) are applied. See *Quick Add Groups, default model*.

8. At **Notification Devices** tab, add devices used to notify this CUC user of voicemails sent to them.

   Note:
   - While the system automatically provisions default notification devices, you can add additional devices when adding a voicemail account.
   - SMS notification is only available if an SMPP Provider has been added on the relevant Voicemail server.

9. At **Caller Input**, click on the required key (*, #, or 0 to 9), then select an action from the drop-down to associate caller input keys to specific actions (to configure default caller input keys). See *Caller Input tab/panel*.

   Note:
   - The **Caller Input** settings display only once the CUC account (including voicemail account name) has been created and saved.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Additional fields are exposed when choosing certain options. For example, when you choose the **User with Mailbox** call action, the **User with Mailbox** and **Transfer** / **Greeting** fields are exposed.

10. Save your changes to add or update this voicemail account.

Note: Once you've added a voicemail service to a user, the lines lines used by any devices associated with the user are updated to reflect the proper call forward and voicemail profile settings to enable the following buttons: **Call Forwarding to Voicemail** and **Voicemail**.

Related topics

- *Reserve numbers for a user*

Single number reach

Tip: *Use the Action search to navigate Automate*

Overview

Single number reach (SNR) is the remote destination number configured for a user.

Note: While you can add one or more Remote Destination Profiles (RDP) to a user, only one RDP may be added to a user's SNR service.

View and Manage Single Number Reach

This procedure displays, moves, exports, and updates existing single number reach (SNR) remote destination profiles (RDPs), and adds new RDPs for SNR. For example, you can configure ring schedules, choose a mobility profile and a single number reach voicemail policy, or set up *answer too soon* / *answer too late timers*.

Pre-requisites:

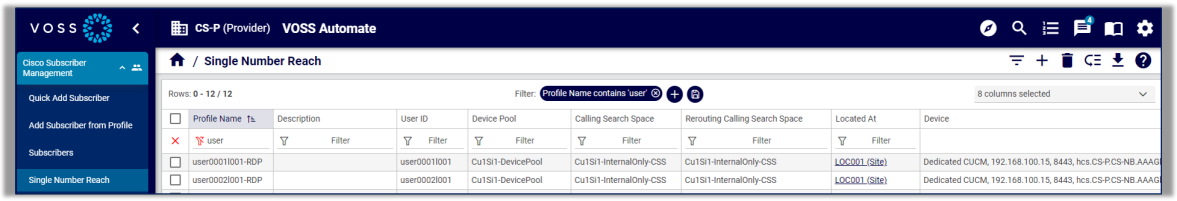
- The user must have been assigned a remote destination profile (RDP) and an entitlement profile that allows SNR.

To view, add, or update a user's SNR:

1. In the Automate Admin Portal, go to **Single Number Reach** to open the list view.

Note: You can also view a multi vendor user's SNR details (line and mobile number) via the Users page, then click the Edit icon (wrench) to update their SNR settings, or click the Delete icon to remove their SNR. See *Multi vendor users*.

Copyright © 2025 VisionOSS Limited. All rights reserved.



2. View existing single number reach (SNR) profiles.
3. Choose an option:
   - **Delete** - to delete one or more single number reach (SNR) instances, select the relevant SNR instances, then click **Delete**.
   - **Move** - to move one or more single number reach (SNR) instances, select the relevant SNR instances, then click **Move**. Choose the target hierarchy.
   - **Export** - to export one or more single number reach (SNR) instances, select the relevant SNR instances, then click **Export**.
   - **Edit** - to edit a single number reach (SNR) instance, click on the relevant instance to open its configuration page. Update the instance, then click **Save**.
   - **Add** - to add a single number reach (SNR) instance, click the Plus icon (+) to add a new record, then fill out configuration details, and click **Save**.

   – Mandatory. Choose a user ID where you want to assign the SNR profile.

   Note: The user must have **Enable Mobility** enabled. You can verify via the **Users** page, click on the user, and select the **User** tab.

   – Mandatory. At **Profile Name**, fill out a remote destination profile (RDP) name, which must be their user name, followed by *"-RDP"*. For example: *jsmith-RDP*.

   Note: You can use a maximum of 50 characters in the RDP name. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Optional. Fill out a description for the RDP name.
- Optional. Choose the relevant device pool.

  Note: The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

- Optional, if relevant to your scenario. At **Calling Search Space**, choose the Calling Search Space (CSS) to be used for routing mobile voice access or enterprise feature access calls.

  Note: Calling Search Space (CSS) is relevant here only when you're routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls.

- Optional, if relevant to your scenario. At **Rerouting Calling Search Space**, choose a calling search space to be used to route Cisco Unified Mobility calls.

  Note: Ensure that the gateway configured for routing mobile calls is assigned to the partition that belongs to the Rerouting Calling Search Space.

  Cisco Unified Communications Manager (CUCM) determines how to route calls based on the remote destination number and the Rerouting Calling Search Space.

  The Rerouting Calling Search Space setting applies only when you are routing calls to the remote destination or mobility identity, which specifies the outbound call leg toward the remote destination or mobility identity when a call comes in to the user enterprise number. Cisco Unified Mobility calls do not get routed to the dual-mode mobility identity number that corresponds to the dual-mode mobile phone number if the device associates with the enterprise WLAN and registers with CUCM.

  Cisco Unified Mobility calls get routed to the dual-mode mobility identity number only when the device is outside the enterprise.

- Mandatory. At **Privacy**, select the relevant privacy option for the RDP. Options are Off, On, Default.

  Note: When selecting *Default* (the default value), the setting matches the value of the Privacy Setting service parameter. If you change and save the value for **Privacy**, you must return to the Remote Destination Profile Configuration window for a remote destination profile that specifies *Default* and save your changes.

  You can't transfer a call from a cell phone to a desk phone if the value for **Privacy** is *On*, and "Enforce Privacy Setting on Held Calls" is *True*.

- Select **Dnd Status** to enable *Do not disturb* on the phone, else, leave this checkbox clear.
- At **User Locale**, choose the locale associated with the phone user interface.

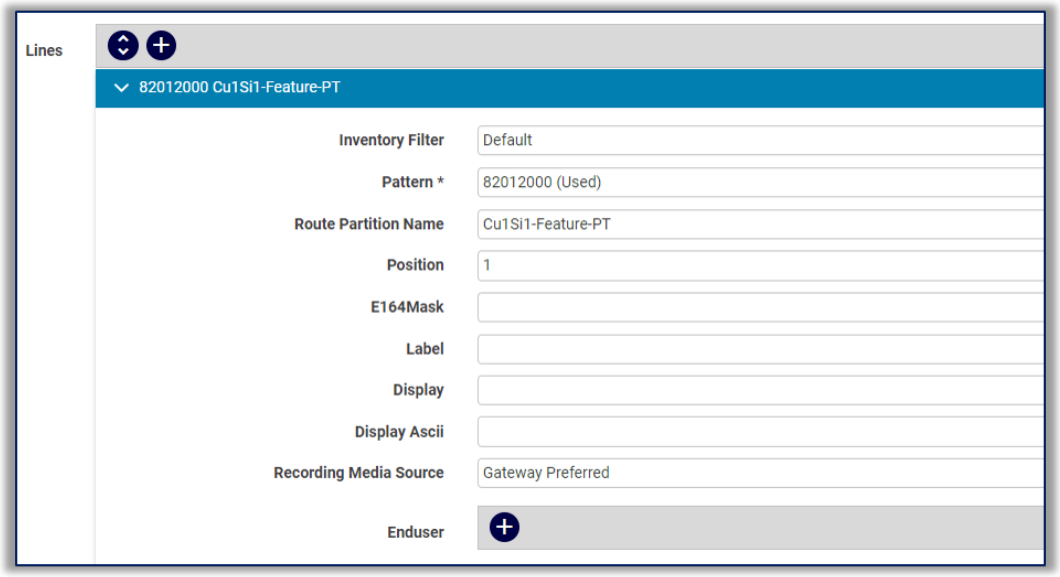
  Note: User locale defines phone details that supports users, such as language and font, on phone models that support localization. When selecting a locale other than English,

Copyright © 2025 VisionOSS Limited. All rights reserved.

ensure the locale installer is installed. Refer to the Cisco Unified Communications Manager documentation for locale installation.

– At **Network Locale**, choose the location of the network.

– At **Lines**, click the Plus icon (+) to add lines (one or more).



Note: Lines you add are listed by their unique ID.

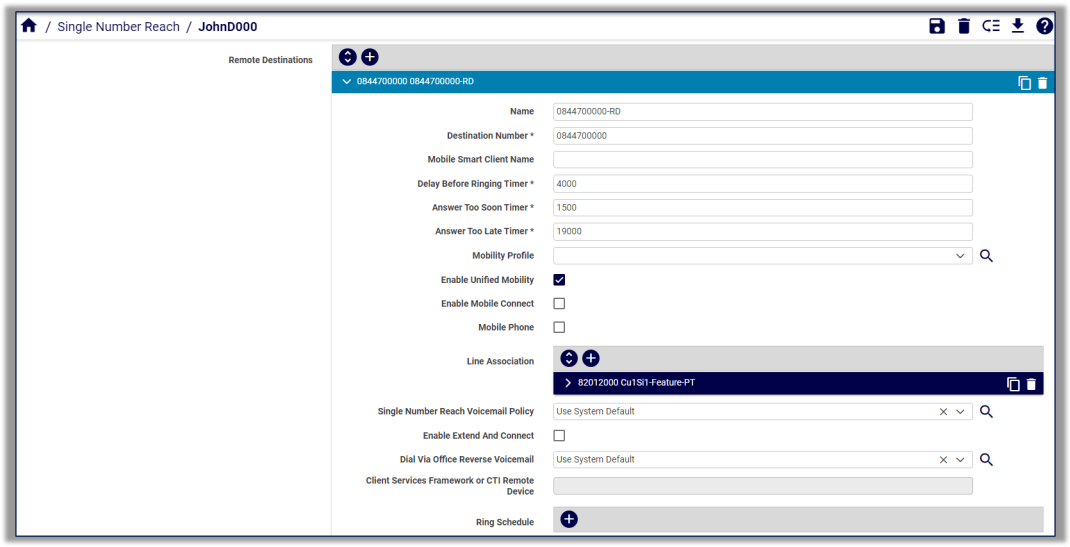
The table describes the line configuration settings:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Inventory filter	Options are: * Default (default) * Show Unused Numbers (Site Only) * Show Unused Numbers * Show Unused Numbers with Associated E164's ((Site Only) * Show Unused Numbers with Associated E164's * Show Used Numbers (Site Only) * Show Used Numbers * Show Numbers belonging to this user (See *Reserve numbers for a user*)
Pattern	Mandatory.
Route partition name	Mandatory.
Position	Integer.
E164 Mask	String.
Label	String.
Display	String.
Display Ascii	String.
Recording media source	Options are: * Gateway Preferred (default) * Phone Preferre
Enduser	Add associated end users, one or more, and select their user ID.

– At **Remote Destinations**, click the Plus icon (+) to add remote destinations (one or more) associated with the profile.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes the remote destination settings:

Setting	Description
Name	Fill out a name to identify the remote destination or mobile identity.
Destination Number	Mandatory. The PSTN telephone number for the destination, including the area code.
Mobile Smart Client Name	Not relevant for dualmode phones.
Delay Before Ringing Timer	Mandatory. Default is 4,000 milliseconds. Enter the time that elapses before the mobile phone rings when a call is extended to the remote destination. Range: 0 - 30,000 milliseconds. Note that when using a hunt group, lines ring only for a short period of time. You may need to manipulate the *Delay Before Ringing Timer* setting and make it zero to allow a remote destination call to be established, ring, and answer, before the hunt list timer expires and pulls the call back.
Answer Too Soon Timer	Mandatory. Default is 1,500 milliseconds. Enter the minimum time, in milliseconds, that CUCM requires the mobile phone to ring before answering the call. This setting accounts for situations where the mobile phone is switched off or is not reachable, in which case the network may immediately divert the call to the mobile phone voice mail. If the mobile phone is answered before this timer expires, Cisco Unified Communications Manager pulls the call back. Range: 0 - 10,000 milliseconds Default: Default: 1500

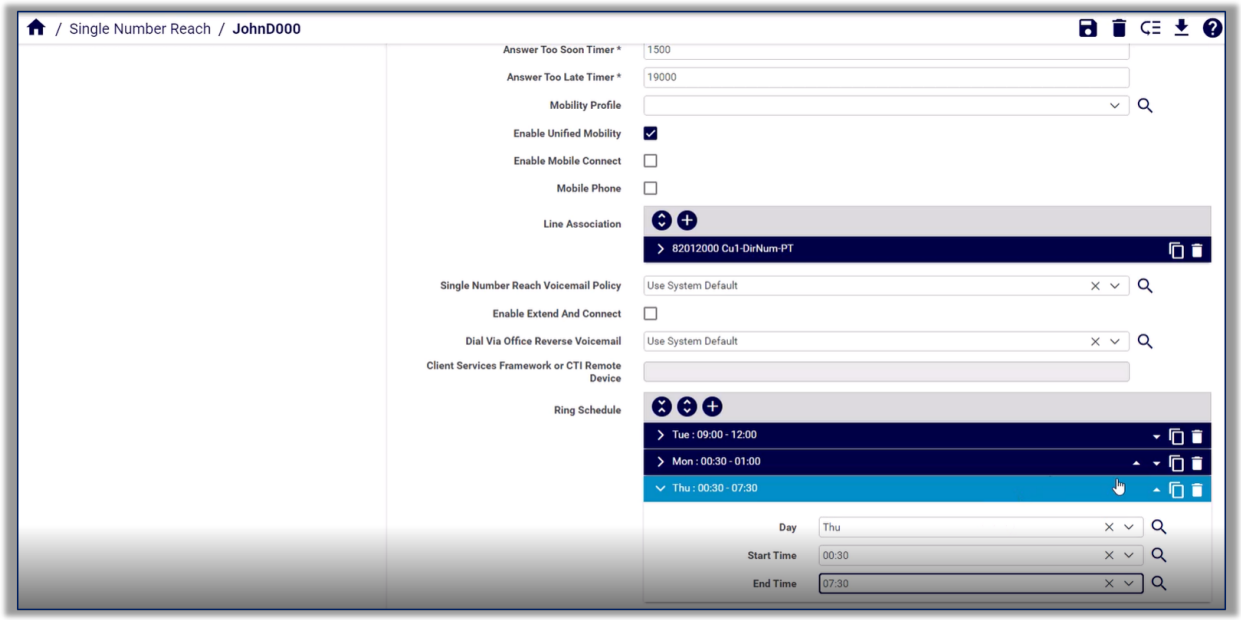
Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Answer Too Late Timer	Mandatory. Default is 19,000 milliseconds Enter the maximum time, in milliseconds, that Cisco Unified Communications Manager allows for the mobile phone to answer. Range: 0 and 10,000 - 300,000 milliseconds If the value is set to zero, the timer is not started.
Mobility Profile	The mobility profile you want to use for this remote destination.
Enable Unified Mobility	

Enable Mobile Connect	Defines whether to allow an incoming call to ring your desk phone and remote destination at the same time. Default is Tru
Mobile Phone	Defines whether to have calls that the desk phone answers to be sent to a mobile phone as the remote destination. Set to True to ensure that, if Send Call to Mobile Phone is specified (by using the Mobility softkey for remote destination pickup), the call is extended to this remote destination. Not relevant for dual-mode phones that are running SIP nor to dual-mode phones that are running SCCP, such as the Nokia S
Line Association	The line association for this remote destination. The line to be associated must already be added to the remote destination profile. All directory numbers specified must already exist in the databa For each line you add, choose the Pattern (a directory number, which is already associated to RDP), Route Partition Name.
Single Number Reach Voicemail Policy	Choose a policy to define how mobile device users answer calls that terminate on a remote destination (RD). Users have a voice mail box for their mobility if the RD call reaches an external voice mail system. Options are: * Use System Default (default) * Timer Control * User Control Note User Control works only when *Enable Enterprise Feature Access* is set to True.
Enable Extend and Connect	Disable if you wish to delete Extend and Connect

Copyright © 2025 VisionOSS Limited. All rights reserved.

Dial Via Office Reverse Voicemail	Define how dual mode device users answer Dial-via-Office Reverse (DVO-R) calls that terminate on the Mobile Identity (MI). Allows users with a single voicemail box for their mobility, if the RD call reaches an external voice mail system. Options are: * Use System Default (default) * Timer Control * User Control
Client Services Framework or CTI Remote Device	ctiRemoteDeviceName tag will be used to associate either CTI Remote Device or a Cisco Spark Remote Device with a Remote Destination.
Ring Schedule	Manage ring schedules (maximum of 7 members in the schedule) for single number reach, to define working days and hours, for one or more days of the wee These fields display only when the CUCM server version is v11.5 and up Only ring schedules added via the Admin Portal can be managed in the Admin Portal. Ring schedules added via Self-service can only be managed in Self-service.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Intercom Lines

Tip: *Use the Action search to navigate Automate*

Overview

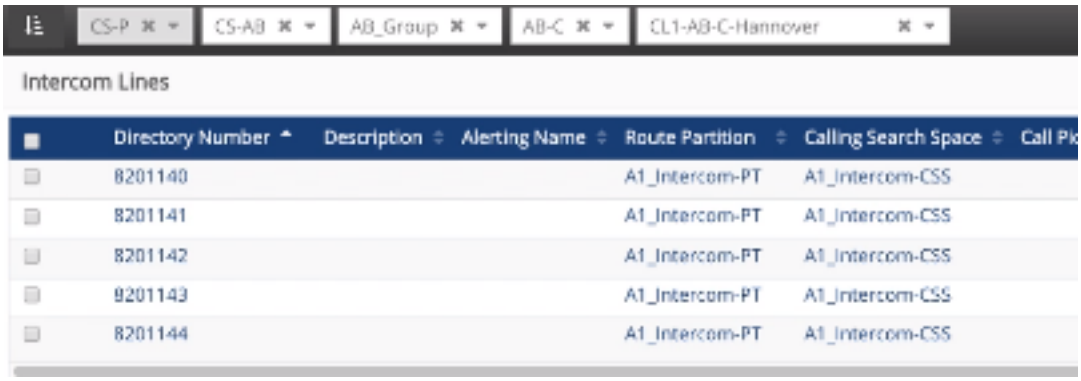
The Intercom Lines feature allow you to manage Intercom lines at a site level independently of the management of lines at a site.

Intercom lines are associated from phones or users - they can then be set up and then associated to phones and user phones simply by first selecting the Intercom Route Partition.

Managing Intercom Lines

When Intercom lines are set up, administrators can navigate to a site and access the **Intercom Lines** menu under the user management pages for the site.

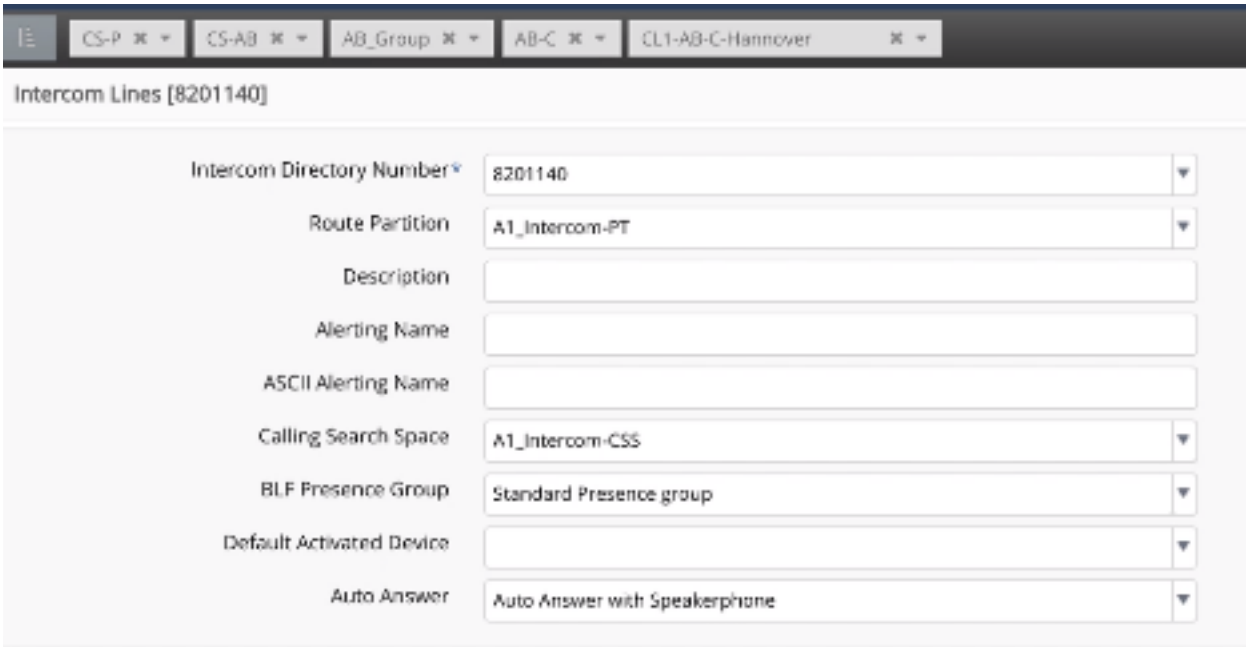
On the Intercom Lines page you can view a list of Intercom lines, and add, delete or modify Intercom lines.



The Intercom lines configuration screen is simpler than the Lines configuration page, and shows only relevant fields.

Note: Intercom lines should be not be managed from the **Lines** menu.

Copyright © 2025 VisionOSS Limited. All rights reserved.



When adding or modifying Intercom lines:

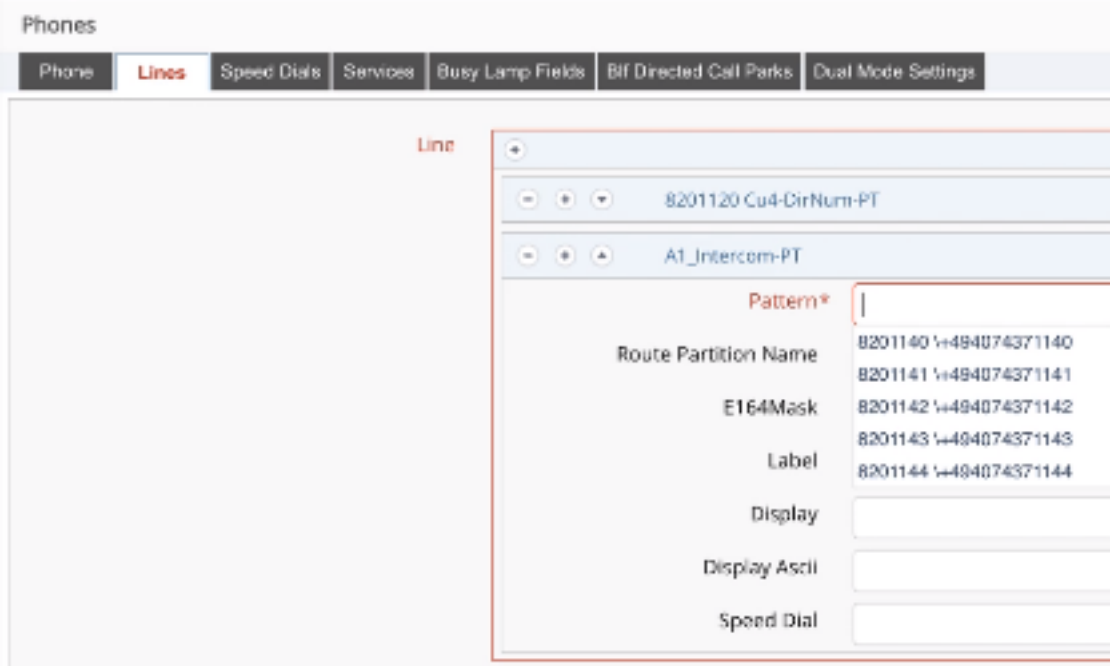
- The **Route Partition** drop-down only shows Intercom partitions.
- The **Calling Search Space** drop-down only shows Intercom calling search spaces.
- For **Default Activated Device**, select the supported device from the drop-down list.
- The **Auto Answer** drop-down only shows supported options.
- If the **Description** field is left blank, it takes a default value “Intercom Line”.

Associating intercom lines to phones

1. Log in to the Admin Portal.
2. Choose the relevant site.
3. Go to **Phones**.
4. On the **Phones** configuration page, select the **Lines** tab.
5. To associate Intercom lines, first specify an Intercom partition for the **Route Partition Name**.

   On the **Line** page, view supported Intercom lines fields to be configured.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- The **Pattern** drop-down *only* shows existing Intercom lines. No new lines can be added.
- Intercom and non-Intercom lines can both be associated to a single phone.
- Associated Intercom lines will also show as “used” in the list view of the **Directory Number Inventory** menu under **Dial Plan Management** and its **Description** in the list will also show as “Intercom Line”.
- Deleting the phone on the **Phones** list view will then also show the Intercom line as not in use.

Intercom lines in user management

1. Log in to the Admin Portal.
2. Choose the relevant site.
3. Go to the **Users** page.
4. When adding a phone to a user, to associate an Intercom line to the phone on the **Phones** tab, also first specify an Intercom partition for the **Route Partition Name**.

   View supported Intercom line fields to be configured.

   - The **Pattern** drop-down *only* shows existing Intercom lines, including those in use.
   - No new lines can be added as a part of user management - they are added on the **Intercom Lines** menu.
   - Associated Intercom lines will also show as “used” in the list view of the **Directory Number Inventory** menu under **Dial Plan Management** and its **Description** in the list will also show as “Intercom Line”.
   - Deleting the phone on the **Phones** list view will then also show the Intercom line as not in use.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Extension mobility

Tip: *Use the Action search to navigate Automate*

Overview

Extension mobility (EM) profiles (also known as roaming profiles), allow users to log onto a phone in another location and the phone automatically adopts the profile for that user.

An EM profile is required for users who move between locations on a regular basis, or for users in an organization or location, who have been assigned an extension mobility profile rather than a permanent phone.

Automate provides three ways to create, manage, and associate extension mobility profiles:

- Add an EM profile to a user when adding a user in a standard add process
- Add a user using Quick Add User, and choose an EM profile
- Add a standalone EM profile (see *Add an extension mobility profile*)

Add an extension mobility profile

Standalone extension mobility (EM) profiles allow administrators to create and manage all EM profiles at the specified organization level.

- Add or update a user's extension mobility (EM) profile via Automate's user management list view. From the list view, open a user, and select the **Extension Mobility** tab. See *Add a user*.
- Add or update a standalone EM profile via the **Extension Mobility** page. From the list view, choose an EM profile to open its configuration screen, and select the **Extension Mobility** tab.

When adding or editing EM profiles, you can personalize the profile for each user.

The table describes common rules for adding an extension mobility (EM) profile:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Extension Mobility tab	Name must be unique. The name cannot be the same as a device name on Unified CM since both are device types. This field is read-only when editing an EM profile.
Lines tab	• Extension mobility (EM) can be associated to multiple users. If the **Show Numbers belonging to this Subscriber** option is chosen as the **Inventory Filter**, only the directory numbers associated to the first user on the **Subscribers** tab are displayed. See also *Reserve numbers for a user* • Line settings can only be changed for the original line, not the clones. • All line settings changed for a line automatically apply for the clones of that line (if any).
Speed Dials tab	Allows you to manage the speed dial numbers associated with the EM profile.
Services tab	Extension mobility (EM) profiles can be subscribed, unsubscribed, and re-subscribed to IP Phone Services such as Intercom Calls, Login/Logout, or SingleWire. Once you choose the IP phone service, the system retrieves the URL and a custom parameter (if any, for example, Ext1 and Ext2) from `device/cucm/IpPhoneService` and populates the **URL** field.
Users tab	Allows you to associate the EM profile to one or more users. You can also disassociate an EM profile from a user by clearing the name from the **Username** drop-down, and saving the change. The **User** link on an existing EM profile links to the associated user's **Extension Mobility** page.

Related topics

- *Reserve numbers for a user*

Delete an extension mobility profile

You can delete a standalone extension mobility (EM) profile via the **Extension Mobility** list view.

When deleting an EM profile, the following elements are automatically removed/cleared:

- Speed dials
- Busy lamp fields
- Service URL's
- IP phone service subscriptions

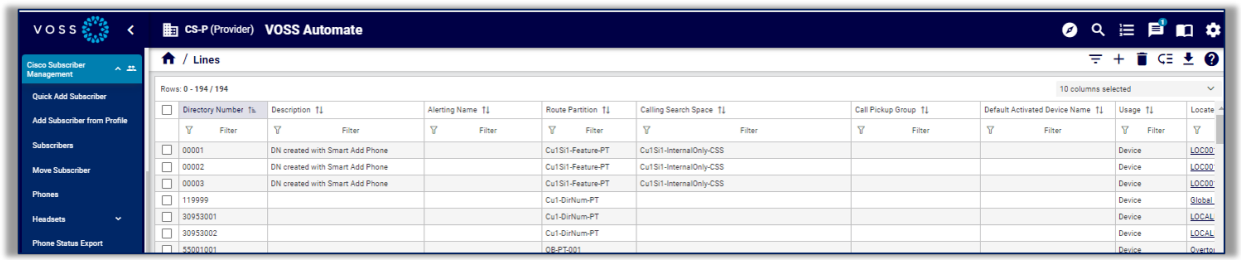
Copyright © 2025 VisionOSS Limited. All rights reserved.

Lines

Tip: *Use the Action search to navigate Automate*

Overview

In Automate you can view, add, edit, and delete the lines (directory numbers) and line configuration of Cisco users.



Related topics

- *Reserve numbers for a user*

Shared lines

A Cisco Unified Communications Manager (CUCM) line is uniquely defined by the pattern (number) and route partition combination.

Lines with the same pattern but different route partitions are defined as two separate lines, not duplicate lines. A shared line therefore indicates that the same line pattern/route partition combination (not just the pattern) is associated with multiple services.

Shared	Associated with more two or more services.
Not shared	Associated with zero or one service.

The table describes the current services that are used to determine the “shared” status of a line:

CUCM	• Devices (phones) • Extension mobility (device profiles) • Single number reach (remote destination profiles) • Hunt lists (hunt pilots) • Call pickup groups • Analog gateways
Cisco Unity Connection (CUC)	Call handlers

Copyright © 2025 VisionOSS Limited. All rights reserved.

Assigning existing, associated line (shared/not shared) in Quick Add User

In Quick Add User, to update an existing, associated line for a new or existing user, the Line configuration template (CFT) related to the selected Quick Add Group (QAG) must be configured to do so.

The table describes the conditions under which QAS updates a line via an applied QAG Line CFT:

Line is NOT updated via the QAG Line CFT	For existing lines that *are* associated with multiple services, the line is in a "shared" state, and is NOT updated via the applied QAG Line CFT. If the QAS workflow evaluates the line as "shared", it skips CFT updates of the line.
Line IS updated via QAG Line CFT	For existing lines that *are not* associated with any services or are associated with only one service, the line is not in a "shared" state and IS updated via the applied QAG Line CFT.

View and manage lines

This procedure displays all lines in the list view, exports, moves, or deletes lines, and updates line configuration.

Note:

- When CSS filtering is enabled at the customer dial plan, the only calling search spaces (CSS) available are those marked *Class of Service* (see the settings for the site, via the **Class of Service** page). If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

  When CSS filtering is disabled, the available calling search spaces (CSS) are CSSs configured on CUCM.
- For additional details around line configuration parameters, such as partitions and CSS, see the "Provider HCS Dial Plan Management Support Guide".
- You may, for example, wish to add additional directory URIs and directory URI partitions. Manual configuration must first be done on the CUCM before URIs will function.
- Not all line settings are configured on the **Lines** page. Some line settings, for example, device-specific settings (such as caller ID display, line label, E.164 mask, and associated end user), are configured via the **Phones** page.

Prerequisites:

- Your system administrator must enable the *number inventory* functionality for your system to allow you to add lines.

  If *number inventory* functionality is disabled, you can only select lines from a drop-down of available numbers.

Perform these steps:

1. Log in to the Automate Admin portal.

   Note: If you're logged in as the Customer admin for a specific site, all fields described in this procedure are visible. If you're logged in as Site admin, only a subset of these fields may display.

Copyright © 2025 VisionOSS Limited. All rights reserved.

2. Go to the **Lines** list view.

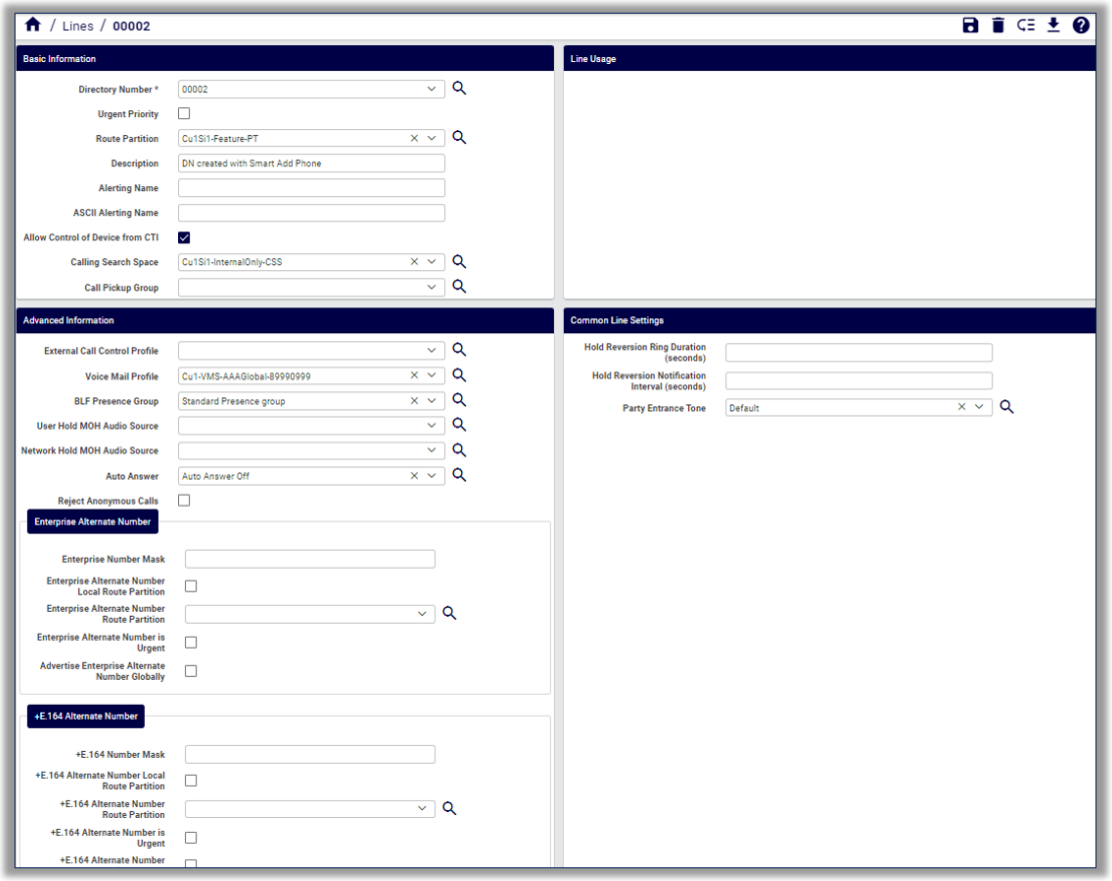
Note: The default configuration template sets the value in the **Usage** column of the list view. For *Intercom DN* and *Intercom Translation* patterns the usage tag value must be specified explicitly as *Device Intercom* and *Translation Intercom* respectively. For all other patterns, such as *Device*, this is a read-only tag.

---

3. View summary details for lines that exist in your system.
4. **Choose an option**:
   - **Move one or more lines**? Select the relevant lines, then click the **Move** icon, and select the target hierarchy (customer or site).
   - **Delete one or more lines**? Select the relevant lines, then click the **Delete** icon. Once the delete transaction completes, the line disappears from the list view.

     Note: If lines are deleted while the numbers are in a Cooling or Reserved state, these numbers only become available once the release date is reached.

   - **Export one or more lines**? Select the relevant lines, then click the toolbar **Export** icon.
   - **Edit a line**? Click on the relevant line in the list view to open its configuration page, make the changes you require, and save.



Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Add a line**? Click the toolbar Plus icon (+), choose the target site, then fill out the line configuration in the fields on this page. The table describes the type of details required:

Fieldset	Description
Basic Information	Configures basic line settings, such as the directory number (mandatory), a route partition, calling search space, and the call pickup group to which the line belongs. **Note:** The **Directory Number** field is either a drop-down list, or a free text field, or a drop-down containing only the available directory numbers (depending on whether the *number inventory* feature is enabled or disabled). Only the actual Directory Number is mandatory.
Advanced Information	Configures profiles, groups, and other advanced settings for the line, for example, music on hold (MOH) audio source, and voice mail profiles.
Shared Devices	Displays any phones, device profiles, or remote destination profiles associated with a particular line.
Common Line Settings	Configures hold reversion ring duration, hold reversion notification interval, and party entrance tone.
AAR Settings	Defines whether automated alternate routing (AAR) voicemail is enabled, and configures the AAR destination mark, AAR group, and whether to retain the destination in the call forwarding history.
Park Monitoring	Defines whether the line is enabled for external and internal voice mail, configures external and/or internal destinations, internal and/or external calling search space (CSS), and reversion timer.
Call Forwarding	Configures all call forwarding settings for this line.
Line Usage	Details for devices and users where the line is used. Includes links to the user, profile, or phones where the line is used.

5. Save your changes.

   All new and updated lines and their settings also reflect in CUCM. You can verify the configuration via **Transaction**.

Shared line across sites

Overview

The ability to have shared lines across sites allows lines to be shared across sites, and is accomplished by introducing the concept of an “inventory site”, in addition to “real sites”:

- The inventory site is used to provision the shared lines first
- Then the real sites make use of the shared lines by assigning them to phones

Devices are only provisioned on real sites (not in the inventory site).

The “shared lines** feature also supports *hunt groups* and *call pickup groups* across sites by leveraging the *inventory site* to provision all of the lines to be included in the hunt group or call pickup group.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Lines used in the hunt groups and call pickup groups that are provisioned in the inventory site can span multiple real sites; that is, they're used by devices on the real sites. The key requirement is that all the lines to be used by a given hunt group or call pickup group must be configured in the inventory site, along with the hunt group and call pickup group itself.

The "shared line across sites" deployment model is 100% backward compatible with the previous directory number (DN) and line configuration. Existing deployments are not impacted when the system is upgraded, and all existing dial plan configuration procedures are supported. The deployment configuration shown in *Example of shared line across sites* is optional and is only required when sharing lines across sites.

Tip: If a line is potentially shareable, it is recommended that you create the line in the inventory site, even if it won't be shared across sites immediately.

The system does not support the ability to move a line from a real site to an inventory site, so to convert a line from *site-local* to *cross-site shared*, the line would need to be deleted from the real site and recreated in the inventory site.

Note: See the Glossary for descriptions of the following terms related to *shared lines across sites* functionality:

- Directory Number (DN)
- DN Inventory
- E.164 Number
- E.164 Inventory
- Line / Line Relation
- Line Appearance
- Class of Service (CoS)
- Directory Number Routing (DNR)
- E.164 Associations

Limitations of shared lines across sites

When considering using shared lines across sites, consider the following limitations:

- A new inventory site is required for each new combination of network device list (NDL) and Country (a "site group"); that is, lines configured at the inventory site are specific to the NDL and Country defined for that site.
- All real sites that reference lines in an inventory site must be defined with the same NDL and Country. Ensure that this requirement is met, as it is not enforced in Automate.
- Shared lines can't span countries or NDLs. This is necessary because Cisco UCM doesn't support shared lines across clusters. The country must be consistent so that line CoSs (defined in the inventory site) are correct for each device referencing the line (defined in the real site). Ensure that the correct association is made between inventory sites and real sites, as it is not enforced in Automate.
- When configuring a phone or user at a real site, any reference to a DN that does not exist in the inventory site results in a new line being created at the real site as it did prior to this Cisco HCS release.

Copyright © 2025 VisionOSS Limited. All rights reserved.

If the inventory site doesn't exist, or a line hasn't been configured in the inventory site first, the system behaves as it did in previous Cisco HCS releases (backwards compatible).

- If a line can be potentially shared, create it in the inventory site before referencing it by any devices. If the DN is used in a device before it's configured in the inventory site, the line is created in the real site and may not have the desired CoS or other configuration desired for a shared line.
- When a line has been created (either at the inventory site or a real site), it can't be moved. To move the line, delete it and re-add it. For example, if you forget to define the line at the inventory site first and configure a device with a line, the line is created at the real site. You would need to delete the line from the real site and add it to the inventory site, then reassign it to the phone.
- A site admin logged in to a real site is not able to see the line configuration that exists at the inventory site. A custom admin (or above) can view the line configuration at all of the sites.
- The "shared lines across sites** functionality only works when using a *flat* dial plan since other dial plans have site location codes in the DN that won't make sense if the DN is shared by multiple sites. The default Automate template bundle includes a *Type 4 flat dial plan*. Other, non-site-specific custom dial plans can be used.
- Self-provisioning does not work for DNs defined at the customer level.
- Although an admin can delete inventory sites, this is not recommended. If an inventory site is deleted, all hunt groups, call pickup groups, voicemail pilot associations, and lines that are part of the inventory site are deleted. If there are devices on the "real" sites that reference these lines, they will no longer reference these lines as they will have been deleted. The customer-level DN inventory is still intact, though no lines are associated with these DNs because they are deleted when the inventory site is deleted. The hunt groups and call pickup groups are self-contained to the inventory site and are therefore deleted as part of the deletion of the inventory site.
- When the inventory site is deleted, this deletes all shared lines, Classes of Service, DNR, and any other configuration added at that site. The shared lines are removed from all devices on "real" sites that may have referenced them.
- If an emergency number is dialed from any shared line, the number displayed on the other end should be the Emergency Call Back Number of the corresponding site.

Example of shared line across sites

Phones are always configured on *real sites*, and can use both shared and *site-local* lines. For example, each phone can have one *site-local* line (for example, 1000), and one *cross-site shared* line (for example, 9000). The following is a summary of the configuration that resides at each hierarchy type:

a. Customer hierarchy

   - **DN inventory** - for the lines to be shared across sites.

   Note: The DN inventory is visible across all sites under the customer. Allowing DN Inventory to be configured at the customer hierarchy node is an enhancement for the Shared Line Across Sites feature. Note that DN inventory can only be created at the customer hierarchy node when a non-SLC-based customer dial plan has been deployed. A transaction error is sent if the administrator attempts to create customer level DN inventory with an SLC-based dial plan.

b. Inventory site, includes:

   - **Line relations** - for the DNs to be shared across sites.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Directory Number Routing (DNR)** entry for the line relations configured at this site to make the DNs inter/intra-site dialable.
- **E.164 inventory** - for the line relations configured at this site.
- **E.164 associations** - for the line relations configured at this site.
- **Line Class of Service (CoS)** - for the lines configured at this site. CoS is discussed in more detail in *Class of service for shared line across sites*.
- **Short codes** - for the line relations configured at this site.

c. Real site, includes

- **DN inventory** - for lines to be used only at this site. Note that these DNs can be shared by multiple phones within the site.
- **Users** - configured via **Users** page or **Quick Add User**.
- **Line relations** - for the DNs configured at this site. These line relations do not have to be configured first; they are configured automatically any time a phone, extension mobility profile, or remote destination profile references a line that doesn't exist in the inventory site.
- **Directory Number Routing (DNR)** - for each of the line relations configured at this site.
- **E.164 inventory** - for lines created at this site.
- **E.164 associations** - for lines created at this site.
- **Device Class of Service (CoS)** - to be used for the phones configured at this site.
- **Phones** - these phones can reference lines that were defined in the inventory site or the Real Site where the phone exists.
- **Extension mobility** - these profiles can also reference lines that were defined in the inventory site or the Real Site where the phone exists.
- **Single Number Reach** - these profiles can reference lines that were defined in the inventory site or the Real Site where the profile is defined.

Fields in Automate that reference DNs, such as the **Pattern** field in the **Line** tab of a phone, are in a drop-down list of DN inventory. The drop-down list of DNs includes inventory defined at the customer level, combined with the inventory defined at the current site context. The administrator can chose either a cross-site shared DN or a site-local DN.

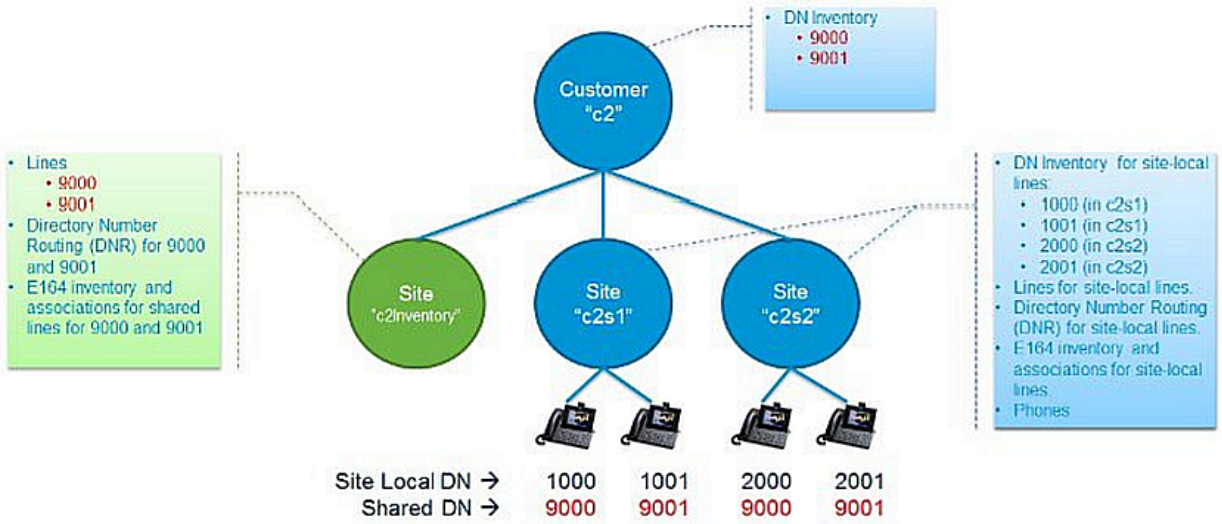
Diagram showing shared line across sites configuration

The image provides a basic *shared line across sites* configuration:

- Uses one inventory site ("c2Inventory") and two real sites ("c2s1" and "c2s2")
- Shows two shared DNs (9000 and 9001 shown in red) and four site-specific DNs (1000 and 1001 at c2s1, 2000 and 2001 at c2s2).
- The inventory for the shared DNs are provisioned at the *customer* hierarchy to make them visible to all sites under the customer. This allows the sites to configure the associated line and assign the line to a device.
- The inventory for the non-shared-across-sites DNs is still configured at the real sites (in blue) as it was in previous Cisco HCS releases.

  Note that both shared DNs and non-shared DNs can co-exist for the same customer.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Configure shared line across sites

Tip: *Use the Action search to navigate Automate*

The steps for configuring shared lines across sites is generally the same as with conventional lines. This section highlights the differences.

- **Conventional, site-local lines**: Lines can be configured automatically as part of the phone, user, or Quick User workflows. Lines don't need to be configured separately first
- **Lines to be shared across sites**: Lines must be configured first in the inventory site, then referenced from phone, user, or Quick User workflows.

Configure shared line across sites at customer

The customer configuration is similar except that you create DN inventory at the customer hierarchy for lines you would like to share (or potentially share) across sites.

1. Configure the Cisco UCM and Cisco Unity Connection (CUC) devices. These can be at the customer level (dedicated) or above (shared).
2. Configure the customer normally (for example, c2).
3. Configure the Network Device List (NDL) for the customer (for example, c2Ndl) that will be used for your site group (NDL/Country combination).
4. Deploy the customer dial plan.

   This must be a flat dial plan (for example, Type 4) since shared lines across site dictates that DNs cannot be site-specific. The Type 4 dial plan does not impose site-specific structure (in other words, site location codes). When configuring the customer dial plan, ensure that the Site Location Code check box is unchecked.
5. Configure the DN inventory to be used across sites for shared lines (via the **Directory Number Inventory**). Note that you should leave the site drop-down list empty to create the inventory on the Customer hierarchy node.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure shared line across sites at inventory site

The *inventory site* is only needed if you want to configure shared lines across sites. If you do not have this requirement you do not need an inventory site and configuration is exactly as it is done normally. Most of the inventory site configuration is the same as configuration for a real site (for example, deploy site dial plan, configure DN inventory, and so on). The areas that are unique to the inventory site are provided in Steps 1, 3, and 5.

1. Configure the inventory site and specify the NDL and Country, for example, c2InventorySite. A different inventory site is needed for each NDL/Country combination (site group). If the customer only has one NDL and one Country, they only need one inventory site.
2. Deploy the site dial plan (Type 4 will automatically be used based on the customer dial plan that was deployed).
3. Create the new Classes of Service to be used as the default line CSS and update the Site Defaults procedure for the inventory site.

   See *Class of service for shared line across sites*.
4. Configure Directory Number Routing (DNR) for the shared lines (via **Directory Number Routing**).
5. Create line relations for each shared line (via **Line**).
6. Create E.164 inventory (via **Add E164 Inventory**).
7. Associate E.164 to DN (via **E164 Associations (N to N)**).
8. Configure Hunt Groups that use shared lines (via **Hunt Groups**).
9. Configure Call Pickup Groups that use shared lines (via **Call Pickup Groups**).

Configure shared line across sites at real sites

Configuration at the real sites is almost exactly the same as in past Cisco HCS releases. The major difference is that the Shared Lines Across Sites exist at the inventory site and therefore any configuration associated with those lines (CoS, DNR, E.164 associations, and so on) exists at the inventory site.

1. Configure the real site (for example c2s1, c2s2, and so on). Use the same NDL and Country as the inventory site (same site group).
2. Deploy the site dial plan on each of the real sites (again, the customer dial plan enforces that the flat dial plan is used).
3. Create DN inventory for an DNs that will be used only at this site.
4. Create Directory Number Routing (DNR) for any DNs created at this site.
5. Create E.164 inventory and associations for an DNs created at this site.
6. Create Device Class of Service if needed. See *Class of service for shared line across sites*.
7. Create Line Class of Service if needed for your site-specific lines. Refer to *Class of service for shared line across sites*.
8. Configure users and phones (via **Quick Add User**, or **Phones**).
   a. When configuring normal lines (lines that aren't shared across sites), select a line from the local site DN inventory, not the customer-level DN inventory. The line is created at the local site as normal; you can configure line CoS, DNR, E.164 associations at this site as normal. Note that this includes shared lines that are only shared within the site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

b. When configuring a shared line across sites, select a customer-level DN from the drop-down list. Remember, the line should be configured at the inventory site first.

9. Configure site-specific Hunt Groups that use lines local to the real site.
10. Configure site-specific Call Pickup Groups that use lines local to the real site.

Dial plan type for shared line across sites

The *shared lines across sites* functionality only works if you're using a flat dial plan (Type 4), or a custom, non-site-specific, dial plan. This is because other dial plans (Types 1 to 3) have site location codes in the DN that don't work if the DN is shared by multiple sites.

If you're using predefined dial plans, ensure the **Site Location Code** checkbox is clear (disabled) when deploying the customer dial plan.

Class of service for shared line across sites

Class of Service (CoS) refers to a Calling Search Space (CSS) that is specifically used to define call routing and feature processing for a line or a phone.

Several CSSs are defined when a customer and site dial plan are deployed. Some of these are only used internally (don't select these CSSs in the CSS drop-downs when configuring a line or phone).

Class of Service CSSs are listed on the **Class of Service** page. A few example CoSs are predefined when a site dial plan is deployed, but the intent is for the administrator to create their own CoSs to meet the desired call routing and feature processing behavior. Below is a summary of Class of Service as it pertains to Shared Lines Across Sites feature.

Class of service is used in two places in Automate:

- Line calling search space (via the **Lines** page, Directory Number Basic Information tab, Calling Search Space)
- Device calling search space (via User Management GUIs, Phones page or Users page, Calling Search Space Name setting)

Additionally, CoS can provide line-based routing (LBR) or device-based routing (DBR). For each call made from a phone, the device CSS of the phone is combined with the line CSS of the line from which the call is being made, and the features and routing for the call are processed based on the combined list of partitions of these two CSSs. The default set of CoSs provided when a site dial plan is deployed includes a device CoS for emergency dialing only, and several line CoSs for feature processing, national dialing, and international dialing and that support either DBR and LBR. The following table shows the default allocation of feature and routing duties between the two sets of CoSs.

Feature	Default Device CoS	Default Line CoS
Emergency call routing	yes*	-
Intrasite routing	-	yes
Intersite routing	-	yes
Local PSTN call routing	-	yes**
National PSTN call routing	-	yes
International PSTN call routing	-	yes
Feature processing	-	yes

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table: Default Class of Service for Shared Line Across Sites Feature

* Emergency call routing is dependent on the country configured for the site. The country is used to route to the correct emergency number for that country (for example, 911 routes to 112 in the United Kingdom). Emergency call routing is assigned to the Device CoS because it is location-dependent, and must be tied to the site where the phone/user actually resides.

** Local call routing is dependent on local area codes defined in the site dial plan. The local area codes configured in the site dial plan allow dialing local dialing (for example 7-digit dialing in the United States).

As shown in the table above, routing is weighted heavily toward the line CoS because when the CoS is assigned to the line, it applies equally to the phone, extension mobility, and single number reach, which all typically share the same line configuration and provide similar dialing behavior for a given user. However, this assumes that the lines and devices are all constrained to individual sites. When we open up lines to be shared across sites, the site-specific configuration becomes more important in order to determine what to put in the device CoS versus the line CoS.

Class of Service (CoS) management for Shared Lines Across Sites is heavily dependent on the customer's specific deployment scenario. The distribution of work between the device CoS and the line CoS depends on the type of country dial plan, and the dialing behavior the customer wants.

For example, if the country dial plan is flat and closed like the Swiss dial plan, meaning that the user numbers are not variable length and there is no site-specific area codes (only national dialing), then most of the routing can occur in the line CoS because there is not much site-specific dialing behavior.

However, if the country dial plan uses area codes and the customer wants a local dialing experience (ability to dial a shorter number such as 7-digit dialing in the United States, and relying on the dial plan to fill in the local area code), then local call routing must be in the device CoS because the device context is needed to determine which area codes to apply to the dialed number. Feature processing partitions can almost always stay with the line CoS since there is usually no geographic dependencies for the feature processing. The exception to this is Time of Day (TOD) routing which may vary depending on the site.

The table provides details for determining how to distribute routing and feature processing between the line CoS and device CoS.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Feature	Line CoS	Device CoS
Emergency call routing	-	Emergency routing should always be location-specific
Intrasite routing	Always using the PrelSR route partition	-
Intersite routing	Always using the PrelSR route partition	-
Local call routing	When full E.164 number is always dialed for offnet calls, for example, national dial plans with no local call routing	When site-specific area codes and/or variable length user numbers (local dialing behavior) are defined
National call routing	If local dialing is line-specific, national dialing should be line-specific.	If local dialing is device-specific, national dialing should be device-specific.
Toll-free call routing	If local dialing is line-specific, toll-free dialing should be line-specific.	If local dialing is device-specific, toll-free dialing should be device-specific.
International call routing	If local dialing is line-specific, international dialing should be line-specific.	If local dialing is device-specific, international dialing should be device-specific.
Service call routing	If local dialing is line-specific, service number dialing should be line-specific.	If local dialing is device-specific, service number dialing should be device-specific.

To speed up the process of configuring lines and phones when you create new Classes of Service, set the site-specific default line CSS and site-specific default device CSS (**Site Management > Defaults**). These fields appear in the following tabs:

- **Device Defaults > Default CUCM Device CSS**
- **Line Defaults > Default CUCM Line CSS**

Call forward considerations for shared line across sites

As the administrator, you can create the Call Forward CSS as a CoS for a particular deployment scenario. Considerations must be made based on whether the local, national, and/or international dialing is configured on the device CoS or line CoS.

Be aware that if the Call Forward CSS allows national and local PSTN routing, you may need to consider call forward scenarios when a line is not associated to a device and PSTN dialing is in the device CoS.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Phone, user, and Quick User for shared line across sites

Phones and users should only be created at *real* sites and not at *inventory sites*. However, the system workflows don't enforce this rule, but will help facilitate ongoing management of the configuration data for the customer.

Lines referenced in the **Phone** screen, the **Users** screen, or the **Quick Users** screen are created automatically if they have not already been provisioned in the inventory sites and pushed to Cisco UCM. This is acceptable as long as you intend for these lines to be only referenced within one site. If a line gets created on a *real* site that you intended to share across sites, it is recommended that you delete the line, and recreate it in the *inventory* site.

Relevant fields for *shared lines across sites* on the **Phone** screen are:

- **Phone** tab: On this tab you specify the Calling Search Space Name (that is, the device-based routing CoS, which is by default the emergency routing CSS). Depending on choices made above in the Class of Service section, you might chose a different CSS here.
- **Lines** tab: On this tab you select the DN (Pattern) from the drop-down list, and configure the *E.164Mask* used for line presentation. The **DN** drop-down includes DNs from the Customer DN inventory combined with the current site DN inventory.

  At the time of writing, the E.164Mask is a free-form field and is not tied to the E.164 inventory; it must be manually entered.

The **Route Partition Name** field is automatically populated with the correct directory number partition based on the Pattern (DN) chosen. Similar fields exist in the **User** tabs.

Hunt groups and call pickup groups for shared line across sites

Hunt groups and call pickup groups can be set up in either the *inventory site* or in the *real sites*, with the following conditions:

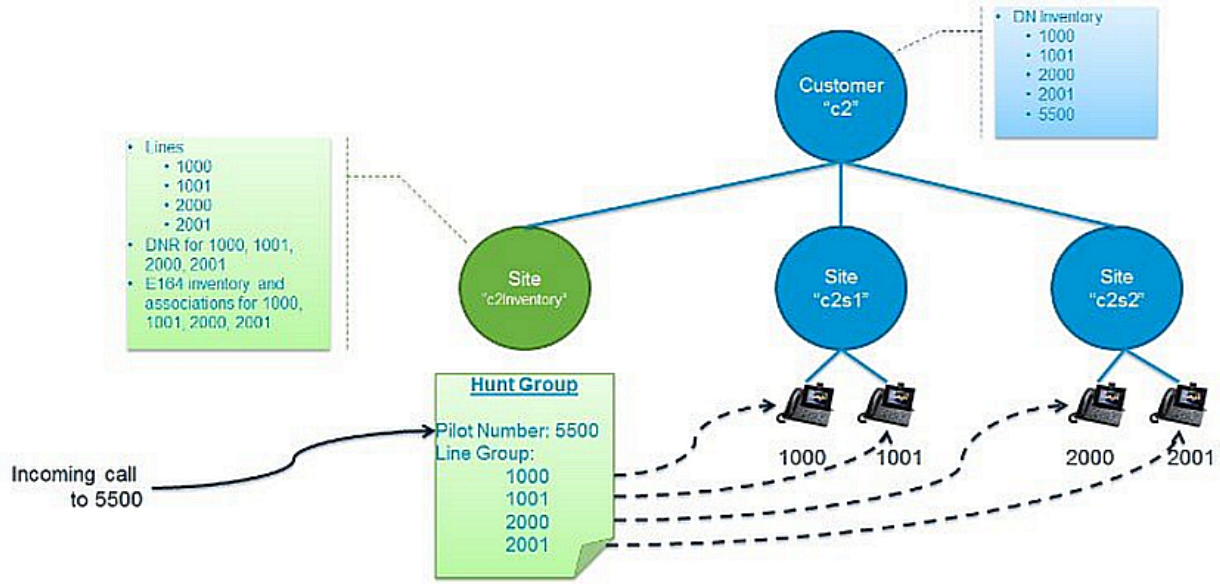
- **Inventory site**: When configured in the *inventory site*, the hunt groups and call pickup groups can include any line created in that site, but not from other sites.

  The recommended setup is to use the *inventory site* if your hunt group or call pickup group needs to include lines from multiple sites.
- The **real sites**. When configured in the *real site*, the hunt groups and call pickup groups can include lines from the *real site*, but not from other sites.

Example scenario

The image provides an example of a hunt group that uses lines spanning multiple sites.

Copyright © 2025 VisionOSS Limited. All rights reserved.



In this example, the hunt group includes the following lines:

- 1000
- 1001
- 2000
- 2001

These lines are *not* shared across sites, but to include them all in one hunt group, they must all be configured at the *inventory site* so that they can all be grouped under a single hunt pilot number, *5500*.

Note:

- The hunt pilot directory number (DN) inventory is at the customer level.
- Once the hunt pilot is assigned, that DN becomes unavailable for other uses:
  - It can't be assigned to a device as a line
  - It can't be used for another service pilot number

Handling voicemail to secondary shared lines

To handle voicemail to secondary shared lines, create a separate user for each shared line at the Inventory Site level, then enable the voice mailbox for that user so that it can be managed by all shared lines.

This approach:

- Offers the ability to differentiate between voice mail deposited for primary and secondary lines
- Provides separate message waiting indication (MWI) notifications for voice mail in the phone's primary and secondary line
- Allows all configuration to be done in Automate. There are no separate manual configurations required in Cisco Unity Connection (CUC) or Cisco Unified Communications Manager (UCM).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: One additional license is required for the shared line user mailbox.

Inventory site

Tip: *Use the Action search to navigate Automate*

Overview

An inventory site is the same as any site, except that it is designated (**Inventory Site** checkbox is enabled) as the repository for lines to be shared across sites. It is deployed in the same way as any other site.

The inventory site is created on the **Site** page. It requires an NDL and a country, and requires a site dial plan to be deployed.

Note: There is no enforcement of configuration ensuring that, for example, only lines are configured at the Inventory Site and not phones. It is the responsibility of the administrator to ensure the proper procedures and conventions are followed as documented in this guide. Therefore, it is important to ensure a good understanding of how the Inventory Site is to be used, and how the Inventory Site configuration relates to the configuration of the "real sites".

There are several caveats and restrictions that must be followed when using the Inventory Site as summarized below. Detailed configuration procedures are provided later in this document. For the purposes of this discussion, the term *Site Group* is used to describe an Inventory Site combined with the "real sites" which use the shared lines defined in the Inventory Site.

All sites in a site group must conform to the following rules:

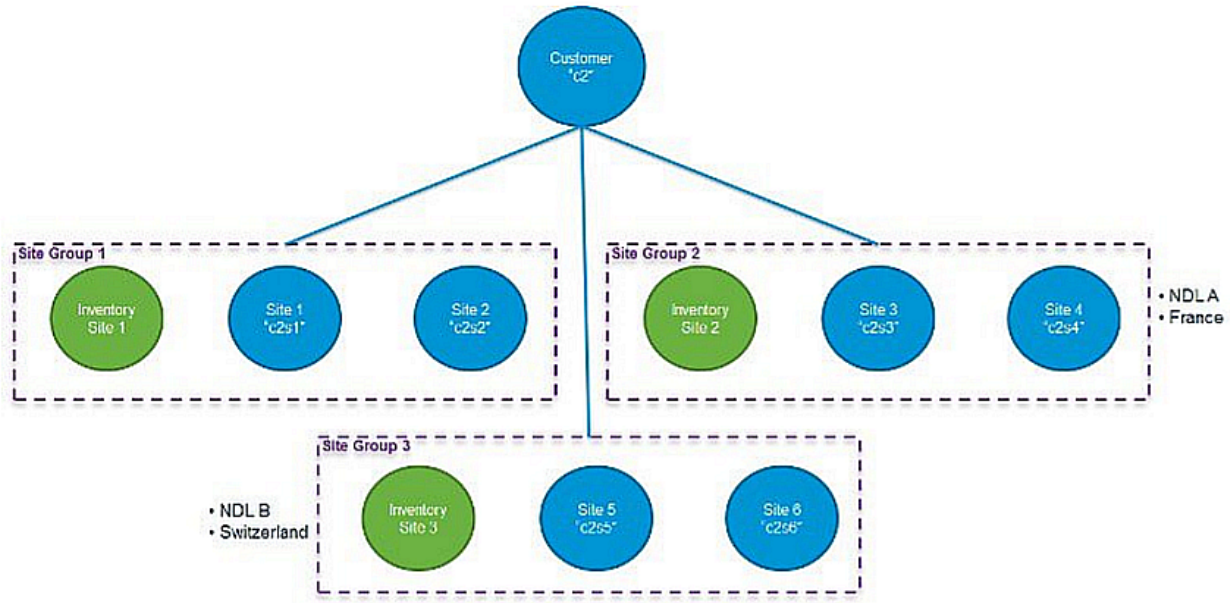
- The sites must be configured with the same NDL and country. Any site that has the same NDL and country as the Inventory Site can participate in the same site group. In fact, the NDL and country settings are what defines the site group.
- Shared lines configured in the Inventory Site of a site group can only be used by other sites in the same group, not in other groups. This means that shared lines cannot span NDLs, and cannot span countries.

Tip: If a line is potentially shareable, we recommend that you create the line in the Inventory Site, even if it will not be shared across sites immediately. The system does not support the ability to move a line from a real site to an Inventory Site, so to convert a line from site-local to cross-site shared, the line would need to be deleted from the real site and recreated in the Inventory Site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Inventory site diagram

The diagram shows a customer with three site groups:



8.3.4. Additional Phone Management Functions

Cisco Phone Status Export

Tip: *Use the Action search to navigate Automate*

Overview

The **Cisco Phone Status Export** tool allows you to export the status of Cisco UCM phones based on selected filters.

The exported phone status report can be opened from the **File Management** form and downloaded as a `.csv` file. The `.csv` file can be opened as a spreadsheet in Microsoft Excel, where each phone status that matches the configured filters will appear as an individual line.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Create and view a Cisco phone status report

1. In the Admin Portal, go to **Cisco Phone Status Export**.
2. Select the hierarchy where you want to create the phone status report.

Note: When running the tool from a hierarchy higher than Customer, a Call Manager filter is mandatory.

2. At **Phone Status Export**, fill out a file name prefix.
3. In the **Filters** fields, fill out at least the mandatory fields:
   - Mandatory. Select a status.

     Note:
     - When choosing a status of *None*, all phones without a registration status on the API will appear in the phone status report.
     - When choosing a status of *Any*, all phones will appear in the phone status report, regardless of the phone registration status.

   - Mandatory (Customer hierarchy only), select a value for **Unified CM Cluster**.
   - Optional. Specify a device name, directory number, and IP address.

     Note: Only phones matching these filters display in the phone status report. For example, if specifying *BAT* as device name, then only phones with a device name prefix starting with *BAT* will appear in the report. The filter on **Device Name** text is case insensitive. For example, “bat” will match “BAT” in the filter.

4. Save your changes.
5. Once the transaction completes, go to **File Management** to view the phone status report.
6. Select the phone status report you wish to export (file-name-prefixXXXX.csv).
7. Click the toolbar **Export** icon, then, on the dialog that appears, select **JSON**, and click **Export** to export a zip file.

   Note: The Excel export option is similar to the JSON export. Only fields that have values are exported.

   When exporting as Excel formatted, all fields (as seen on the GUI), with or without values, are exported.

8. Open the *.csv* file in Excel.

   Note: The first column on the report reflects the phone hierarchy. Subsequent columns provide the (Phone) Name, Status, and information such as: `cm_node`, `ip_address`, `DirNumber`, `DeviceClass`, `Model`, `Product`, and so on (depending on the selected filters).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add application users to device

Tip: *Use the Action search to navigate Automate*

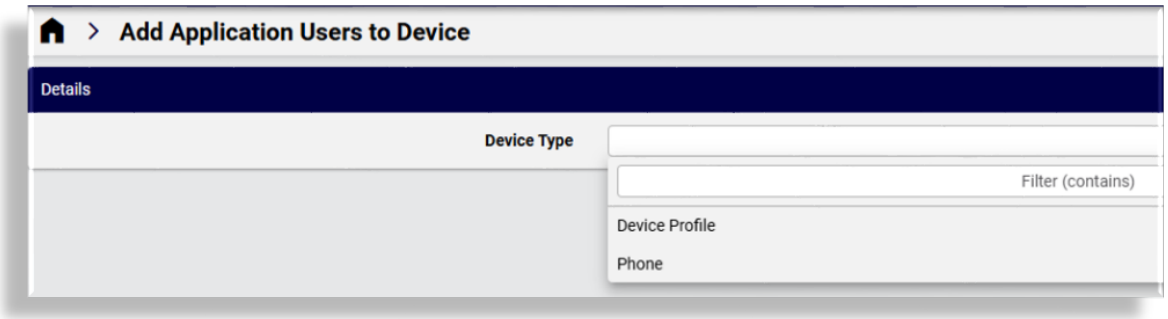
Overview

The **Add Application Users to Device** tool for CUCM allows a site admin to view all CUCM application users associated with or available to be associated with a selected device or device profile at a site, and to associate or disassociate one or more application users from that device or device profile at the site.

Associate or disassociate App users and a device or device profile

This procedure allows a site admin (or higher level admin) to view all CUCM application users currently associated with a selected device or device profile, and to associate one or more application users to the selected device or device profile.

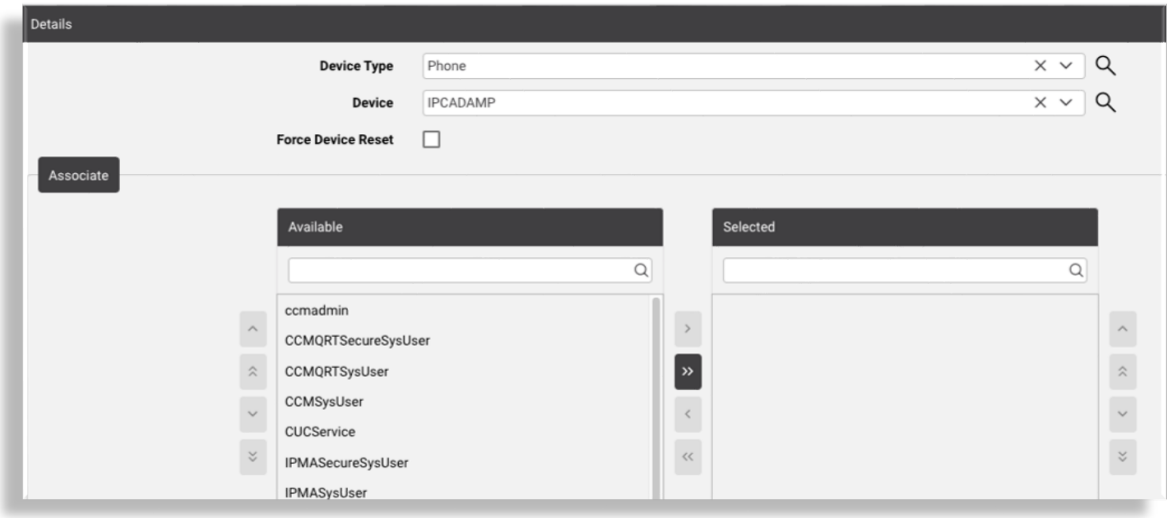
1. Log in to the Automate Admin portal.
2. Select the site.
3. Go to **Add Application Users to Device**
4. On **Add Application Users to Device**, select the relevant device type, either of the following:
   - Device profile
   - Phone



5. At **Device**, select the relevant device.

   Note: The lists in the **Associate** and **Disassociate** transfer boxes populate based on the application users that can be associated or disassociated from the selected device.

Copyright © 2025 VisionOSS Limited. All rights reserved.



6. At **Force Device Reset**, define whether to reset the phone or device profile. Default is false (do not force reset).
7. At the **Associate** transfer box, if this is your use case, select one or more application users from the **Available** field, and move these to the **Selected** field.
8. At the **Disassociate** transfer box, if this is your use case, select one or more application users from the **Available** field, and move these to the **Selected** field.
9. Click **Save** to update the device.

Related topics

- *Add devices to application user*

Add devices to application user

Tip: *Use the Action search to navigate Automate*

Overview

The **Add Devices to Application User** tool for Cisco UCM allows a site admin to view devices and device profiles currently associated with a selected application (app) user at a site, and to associate and disassociate one or more devices and device profiles to an app user at the site.

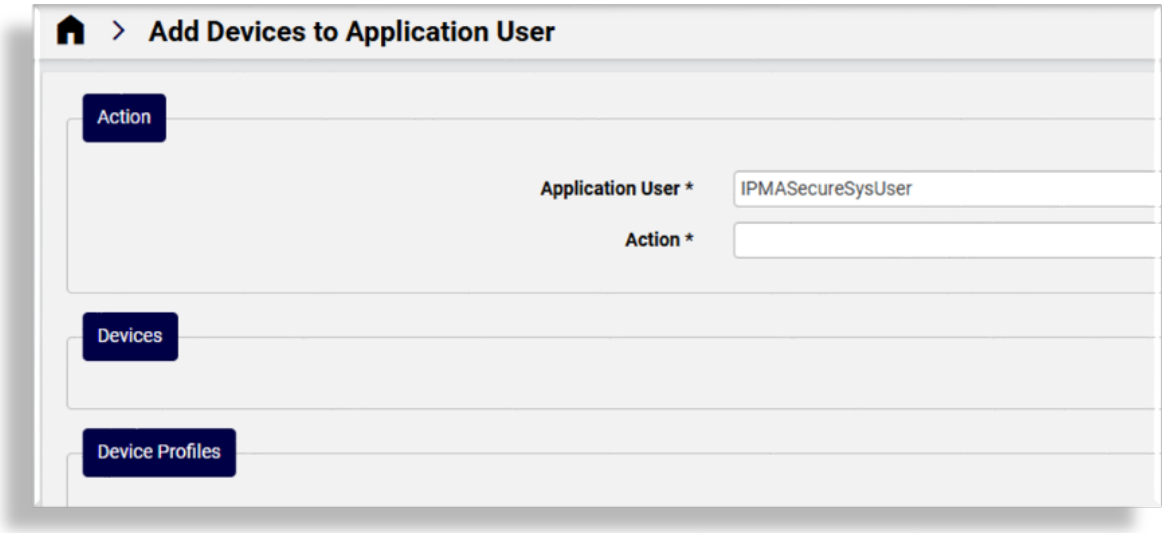
Copyright © 2025 VisionOSS Limited. All rights reserved.

Associate or disassociate devices and device profiles and app user

This procedure allows a site admin (or higher level admin) to view devices and device profiles currently associated to a selected application user at a site, and to associate or disassociate devices and device profiles with that application user.

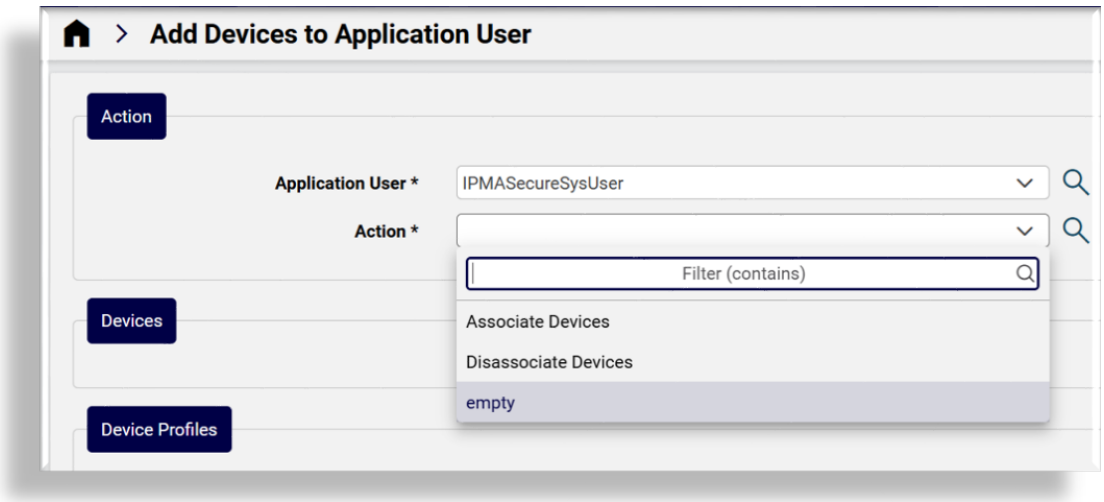
Note: While you're working with the tool, the system places a lock on the devices so they can't be associated with another application user until your transaction is complete.

1. Log in to the Automate Admin portal.
2. Select the site.
3. Go to **Add Devices to Application Users**.
4. On **Add Devices to Application Users**, select the relevant application user.



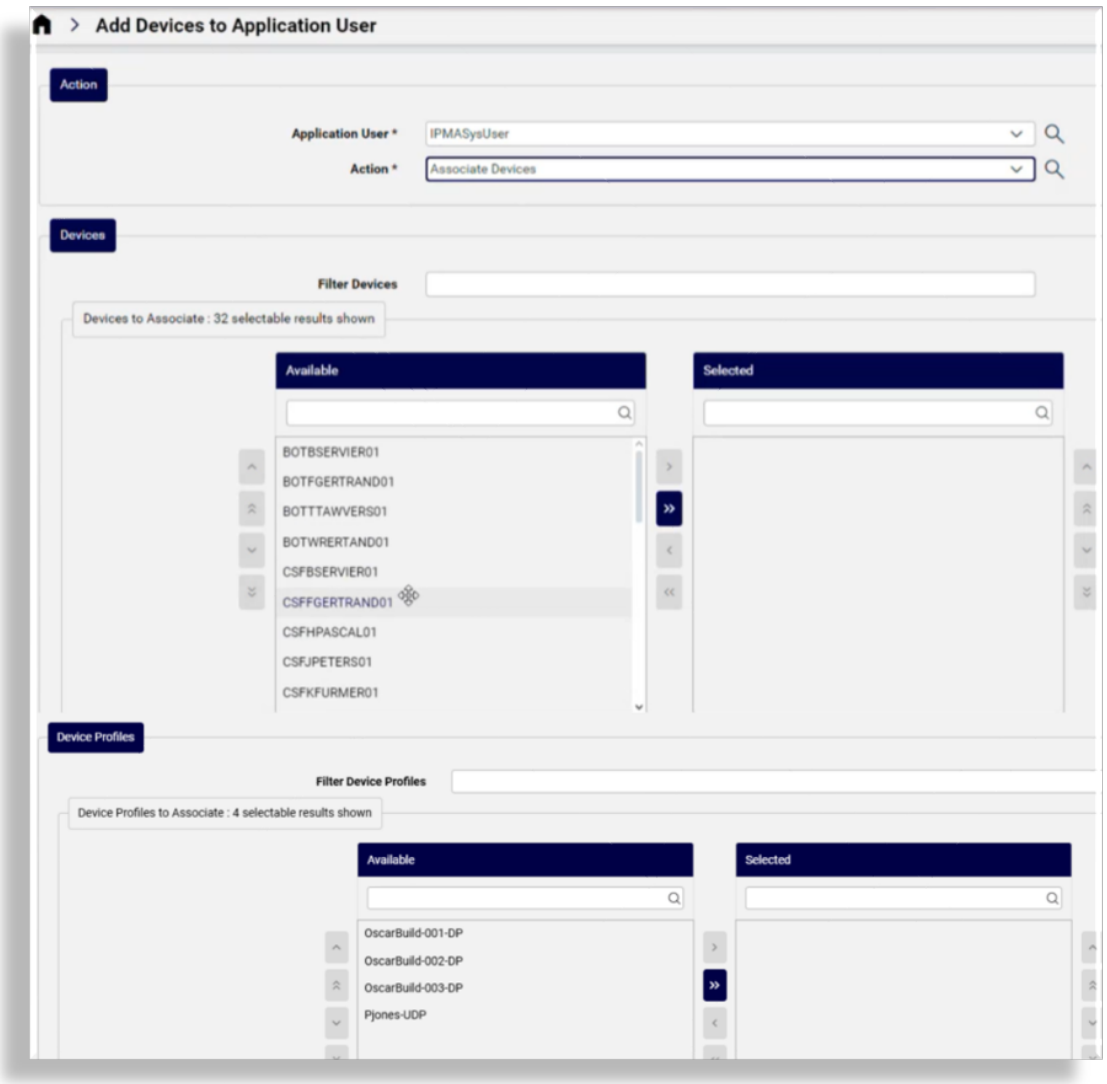
5. **Choose an option**:
   - **View devices and device profiles currently associated with the selected app user**? Choose an action, one of the following:
     - Associate Devices
     - Disassociate Devices

Copyright © 2025 VisionOSS Limited. All rights reserved.



Once you choose an app user and an action, the app user's currently associated and disassociated devices and device profiles populate the lists for **Devices** and **Device Profiles** on the page. You can use the **Filter** fields to display a selection of these devices and device profiles.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- **Associate devices and device profiles to this app user**?
  - From the **Action** drop-down, select **Associate Devices**.
  - At the **Devices** transfer box, select one or more devices from the **Available** field and move these to the **Selected** field.
  - At the **Device Profiles** transfer box, select one or more device profiles from the **Available** field and move these to the **Selected** field.
  - Click **Save**.

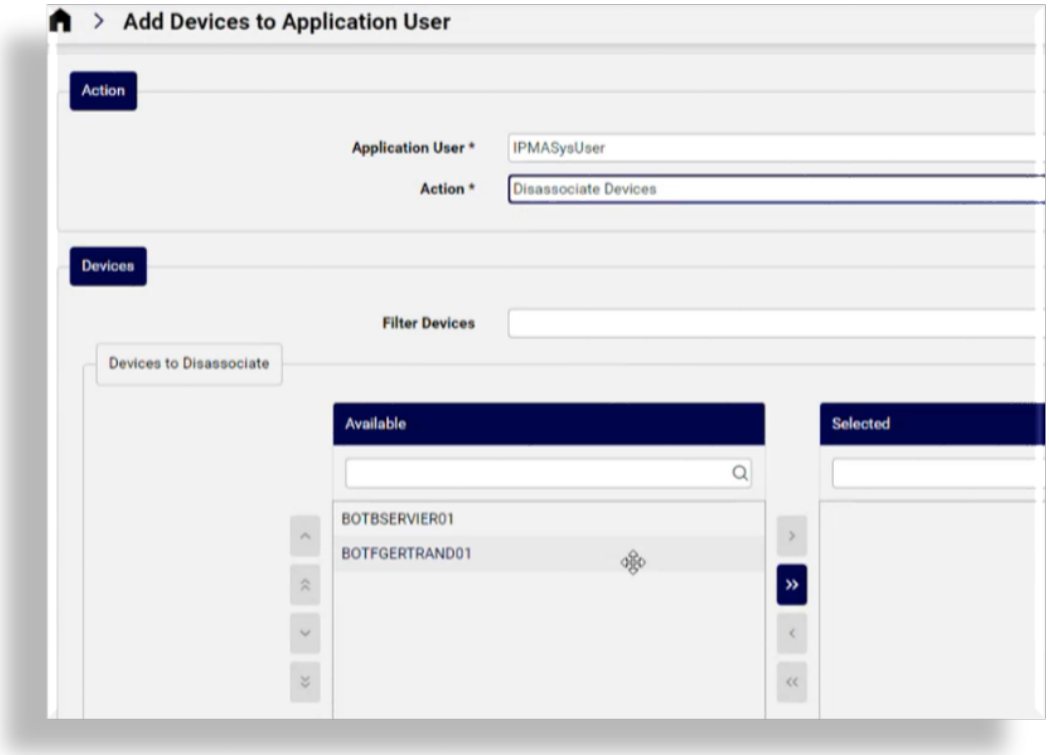
    The Cisco UCM application user is updated and associated with the devices and/or device profiles you selected.
- **Disassociate devices and device profiles from this app user**?
  - From the **Action** drop-down, select **Disassociate Devices**.
  - At the **Devices** transfer box, select one or more devices from the **Selected** field and move these to the **Available** field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

– At the **Device Profiles** transfer box, select one or more device profiles from the **Selected** field and move these to the **Available** field.

– Click **Save**.

The Cisco UCM application user is updated and disassociated with the devices and/or device profiles you selected.



Related topics

- *Add application users to device*

Reset-Restart Site Phones

This feature allows an administrator to reset or restart all phones at a specified site.

Note:

- This feature only works for devices that are registered with Unified CM.
- For phones sharing a line or within a device pool, these can all respectively be reset from the shared line or device pool. In other words, administrators who have been configured with access to the models `device/cucm/Line` and `device/cucm/DevicePool` in their MenuLayout, as well as to the `reset` action of these models in their Access Profile, can then carry out this task.

---

1. Browse to the required site at which you want to reset or restart phones.
2. Open the **Reset-Restart Site Phones** form (default menu **Subscriber Management** > **Reset-Restart Site Phones**) and from the **Action to Take** drop-down select either:

Copyright © 2025 VisionOSS Limited. All rights reserved.

    - Reset All Phones. To shut down devices and bring them back up.
    - Restart All Phones. To restart devices without shutting them down.
3. Click **Save**.

Individual phones can also be reset or restarted by clicking on the phone on the **Phones** list view (default menu **Subscriber Management > Phones**):

- Click the **Restart Phone** button to restart a device without shutting it down.
- Click the **Reset Phone** button to shut down a device and bring it back up.

8.4. Provisioning

8.4.1. End-user provisioning workflow

This topic describes an example end-user provisioning workflow.

Prerequisites:

Complete the following customer onboarding tasks before performing end-user provisioning with Automate:

- Devices defined (UCM, UC apps, WebEx)
- Network Device Lists (NDLs) created
- Single Sign On enabled, if necessary
- LDAP integration enabled, if necessary
- Any customer equipment to be monitored defined
- Customer sites defined with associated NDLs
- Customer and site dial plans configured
- Directory Number Inventory configured
- Voice Mail service defined and associated with a customer

Note: If you're syncing in users with a number that already exists at a site, by default, the system creates a duplicate of the number. To prevent duplicate numbers in the number inventory, enable the following global settings: *Prevent duplicate numbers*.

To perform end-user provisioning:

Note: Not all steps apply for all customers. Some steps can be performed in alternate order.

1. Sync users from the LDAP server:
    - Set up LDAP for user syncs
    - Sync users from LDAP
2. If LDAP sync is not used and users are provisioned on Cisco UCM, you can sync users from Cisco UCM. For more information, see *Sync Cisco UCM users, lines, and phones*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

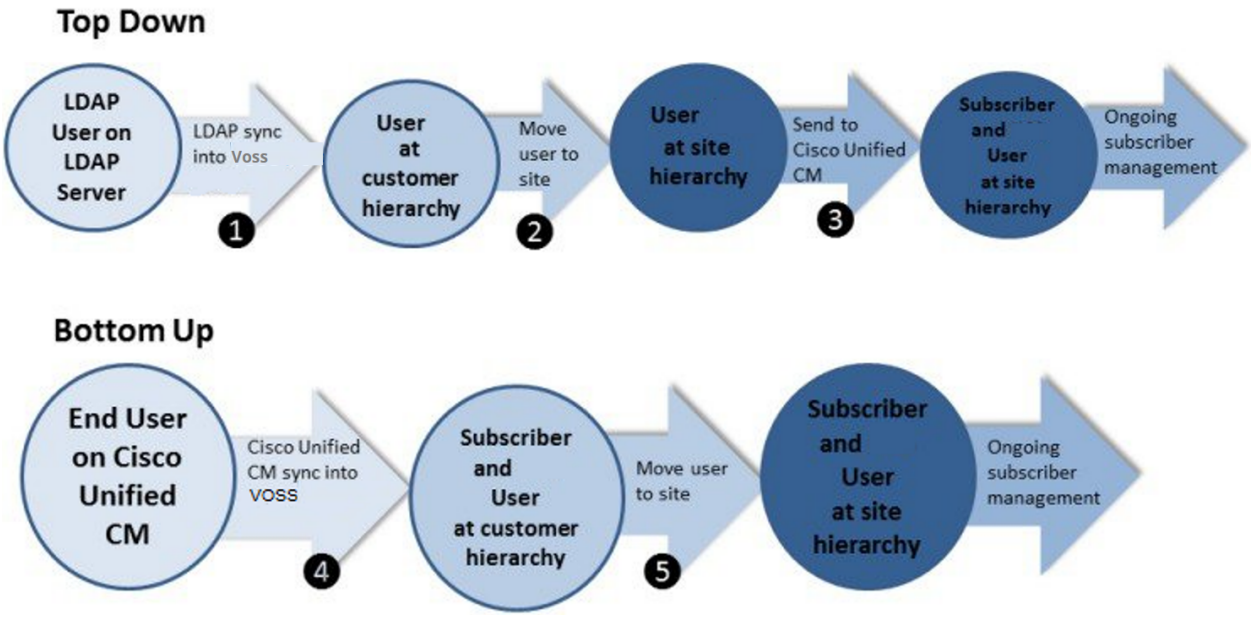
3. In addition to synchronizing users, you can manually create users. Refer to *Add admin user*.
4. (Optional) You can explicitly assign a credential policy to a user. For more information, see *Assign a credential policy to a user*.
5. Move users to sites using any of the following methods:
   a. Define move filters. Refer to *Create a filter to move users*.
   b. Enable automatic user moves for synchronization. For more information, see Automatically move users synced from Cisco UCM.
   c. Manually move users. Refer to *Move users*.
6. Push manually created and LDAP-synced users to Cisco UCM. Refer to *Manually add users to Cisco UCM*.
7. Manage users. Refer to *Add a user*):
   a. Configure a phone with a line.
   b. Associate a phone to a user.
   c. (Optional, Provider) Change the Class of Service for the user from the Class of Service set in the Site Defaults. For more information, see *Configure Class of Service*.
8. (Optional) Associate voice mail to a user (see under *Add a user*):
   a. Associate the voice mail service to a user.
   b. Associate a voice mail profile to a line.
   c. Enable call forward to voice mail.
   d. Reset a phone.
9. (Optional) Associate the extension mobility service to a user (see under: *Add a user*):
   a. Add Login/Logout Service on UCM.
   b. Import UC services and service profiles.
   c. Subscribe the Login/Logout service to a phone.
   d. Associate the extension mobility service to a user.
10. (Optional) Configure conferencing. For more information (see *Introduction to conferencing* and *Add a user*).
11. Configure single number reach for a user (see under: *Add a user*).
12. Associate a service profile to a user and enable IM and Presence.

8.4.2. User provisioning use cases

The image is a diagram describing two typical user provisioning use cases:

- Top-down
- Bottom-up

Copyright © 2025 VisionOSS Limited. All rights reserved.



Tasks performed on users in Automate (as outlined in the diagram) are done via the following pages in the GUI:

1. **LDAP Users**
2. **Move Users**
3. Performed by any of the following:
   - **Users**
   - **Users**
   - **Quick Add User**
4. **CUCM Users, Lines, Phones**
5. **Move Users**

In each diagram:

- The user starts on an external server, either LDAP (for example, Open LDAP or Active Directory), or on Cisco Unified Communications Manager (Cisco UCM).
- When the user is synced into Automate, either an Automate user is created, or both an Automate user and provisioned user are created.
- For each step, the diagram also shows the hierarchy node where the user exists. The result in both cases is that both a non-Automate and Automate user exist. From that point, the user is primarily managed via Automate's User management GUI.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.4.3. View a user's provisioning status

Tip: *Use the Action search to navigate Automate*

To view a user's current provisioning status.

1. Log in as provider, reseller, or customer administrator.
2. Go to the **Users** list view.
3. Click on the user to open the Users[username] page.
4. Select the **Provisioning Status** tab.
5. View The information is displayed for the user as it is visible to the administrator.

   The **Provisioned** checkbox is selected by default so that *only provisioned data* is shown. You can clear the check box to show all un-provisioned data.

   Example application fields as provisioned:

Field	Description
VOSS user	User's username.
CUCM	Unified CM server to which the user is synced.
CUC	Unity Connection server to which the user is synced.
LDAP	LDAP server to which the user is synced.
Webex App	Webex App server where the user exists.
Pexip	Pexip server where the user exists.
Synced To	Hierarchy level where the user was originally synced to or created at.
VOSS User Hierarchy	User's current hierarchy node in VOSS Automate.
CUCM User Hierarchy	User's current hierarchy node on Unified CM.
CUC User Hierarchy	User's current hierarchy node on Unity Connection.
LDAP User Hierarchy	User's current hierarchy node on LDAP.
Webex App User Hierarchy	User's current hierarchy node on Webex App.
Pexip User Hierarchy	User's current hierarchy node on Pexip.
CUCM 1	An alternate Unified CM server to which the user is synced.

8.5. Authentication

8.5.1. User login options by auth method and server auth scope

Overview

This topic provides two views of user login authentication:

- A flowchart (*Login authentication process*) that outlines Automate's authentication checks when the authentication method is set to *Automatic*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Two matrices showing successful user login based on specific server and user configurations, and whether the user uses an SSO login URL:
  - *IdP (SSO): User on IdP server, and SSO login URL used*
  - *No IdP (SSO): LDAP configured and enabled for authentication*

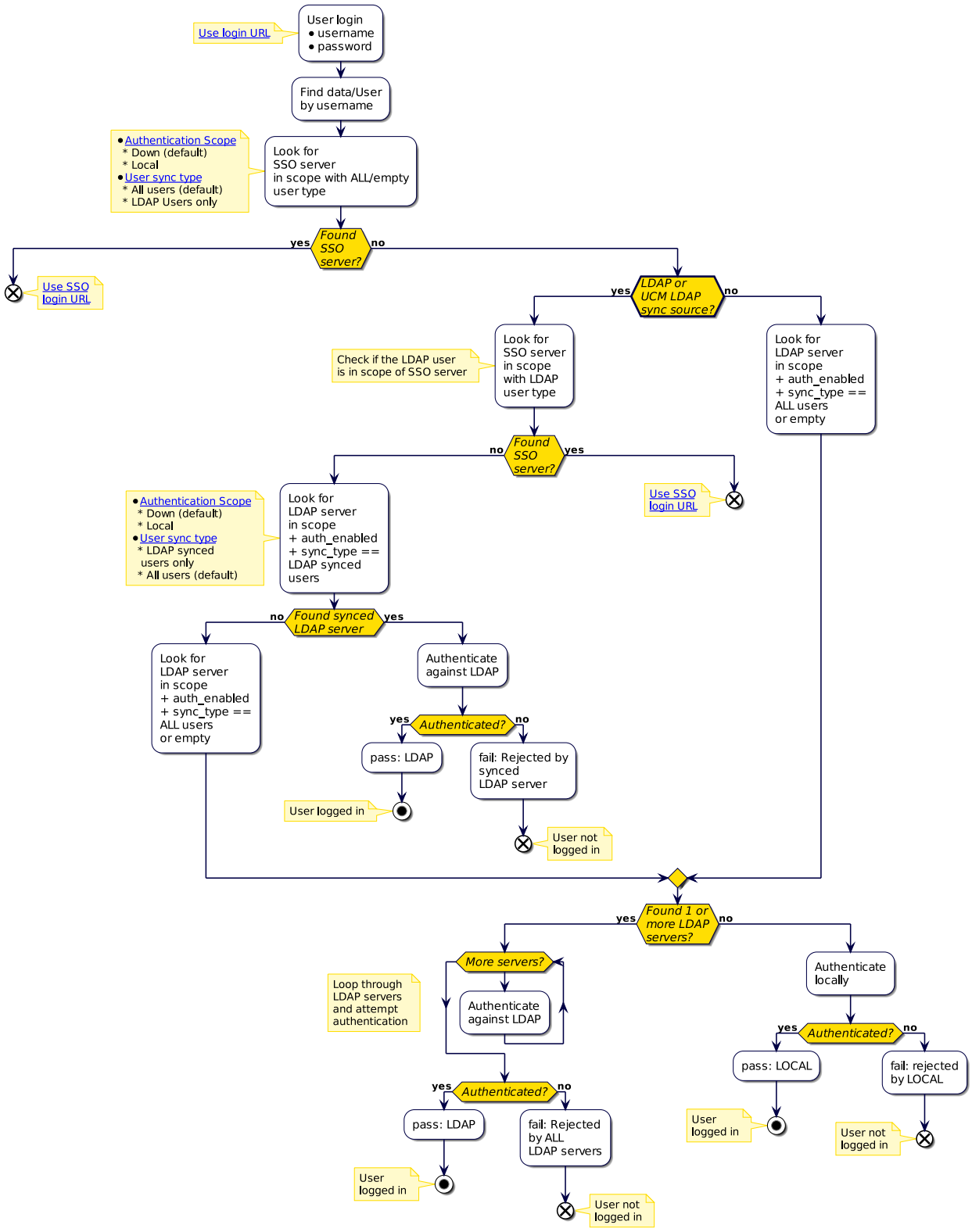
Login authentication process

The flowchart below shows the authentication process in VOSS Automate when a user logs in where the the authentication method on VOSS Automate is set to *Automatic*.

Settings and conditions to check include:

- User login and settings (user and authentication)
- Servers (SSO, LDAP) set up and their settings (scope and authentication)
- System settings (global authentication method)

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Authentication matrix

Users can log in to VOSS Automate (Yes or No) based on their authentication method, the user sync type, and the server authentication scope:

User authentication method	The *Auth* method, either *Local*, *LDAP*, *SSO*, or *Automatic*. See also: • *User authentication* • *Add admin user*
User sync type	Who can authenticate, either *all users* or *LDAP-synced*. See also *LDAP server*
Server authentication scope	The hierarchy, either of the following: • Current hierarchy and below • Current hierarchy only See also: *LDAP server* and *Configure SSO IdP*

Note: If an IdP server is in scope and authentication method is set to *LDAP*, authentication is attempted against LDAP on login.

If the authentication method is set to *Automatic*, *IdP (SSO)* authentication takes precedence.

IdP (SSO): User on IdP server, and SSO login URL used

The table displays a matrix indicating either Yes (Y) or No (N) for whether users can log in to VOSS Automate based on the user authentication method, their sync type, and the server authentication scope, for users on an IdP (SSO) server, using a SSO log in URL:

User auth method	**Server authentication scope (hierarchy):**			
	Current hierarchy and below		**Current hierarchy only**	
	User sync type - who can authenticate:			
	All users	**Synced users**	**All users**	**Synced users**
Local	N	Y	Y (If user not at server node)	Y
LDAP	N	Y	Y (If user at server node)	Y (If user at server node)
SSO	Y	Y (If LDAP synced user)	Y	Y (If user LDAP synced at server node)
Automatic	Y	Y (If LDAP synced user)	Y (If user at server node)	Y (If user LDAP synced at server node)

Copyright © 2025 VisionOSS Limited. All rights reserved.

No IdP (SSO): LDAP configured and enabled for authentication

The table displays a matrix indicating either Yes (Y) or No (N) to define whether users can log in to VOSS Automate based on the user authentication method, their sync type, and the server authentication scope, for users not on an IdP (SSO) server, where LDAP is configured and enabled for authentication:

User auth method	Server authentication scope (hierarchy):			
	Current hierarchy and below		Current hierarchy only	
	User sync type - who can authenticate:			
	All users	Synced users	All users	Synced users
Local	N	Y	Y (If user not at server node)	Y
LDAP	Y	Y	Y (If user at server node)	Y (If user at server node)
SSO	N	N	N	N
Automatic	Y (if synced user)	Y (if synced user)	Y (If user synced at server node)	Y (If user synced at server node)

8.5.2. Standard users and login

Overview

For a system user that uses the standard authorization method, the password is stored in the internal system database.

Note: VOSS Automate uses the PBKDF2 algorithm with an SHA256 hash, a key stretching mechanism recommended by the National Institute of Standards Technology (NIST), Computer Security Resource Center (CSRC).

Login URL and page theme

Standard users log in at the following URL: `https://{hostname}/login`

A login page page theme can be applied to the login page during the log in process. To do this, add a suffix `?theme={theme_name}` where `{theme_name}` is an available theme.

Example: `https://{hostname}/login/?theme=default`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Username format and hierarchy

When logging in, the username can be entered in either of the following formats:

- `{username}@hierarchy`
- `{email address}`
- `{username}`

Important: If logging in with just `{username}`, your username must be unique at the hierarchy level, else login fails. In this case, log in using either `{username}@hierarchy` or `{email address}`. Email address must be unique in the system.

Hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created. On the login form, the hierarchy is prefixed with `sys`.

Example: `johndoe@sys.VS-OPS.VS-Corp.Chicago`

Related Topics

- *Standard users and login*
- *Setting the default theme* (if a theme is applied to the login screen)

8.5.3. LDAP users and login

Overview

When creating a system user using the LDAP authorization method, specify the LDAP server and the LDAP username.

The LDAP username corresponds to the login Attribute Name specified in the LDAP network connection.

Login URL

LDAP users log in at the following URL: `https://{host name}/login`

LDAP username format

When logging in with LDAP credentials, the username is in the following format: `{user ID}[@hierarchy]`

Regardless of the login Attribute Name specified in the LDAP network connection, the user email address can be used to log in.

Note:

- `@hierarchy` is not required when the user ID corresponds to the user's email address.
- `{user ID}` corresponds to the login attribute name (for example, email address, user principal name, sAMaccountName). The login attribute name is configured in the Authentication attribute of the LDAP device connection associated with this hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

8.5.4. SSO users and login

Overview

When creating a system user using Single Sign-On (SSO) authorization, the SSO Identity Provider (IdP) must be specified, and the SSO username.

Login URL

SSO users log in at these URLs, which point to the IdP for SSO authentication with VOSS Automate, and eventual redirect to the relevant interface:

- SSO log in URL: `{{"https://{host name}/sso/{Login URI}/login}}"`

  Example: `https://host.Agency1.CustomerA.com/sso/CustomerA/Agency1/login`

  Note: This URL format also applies to self-service users.

- Admin role log in URL: `{{https://{host name}/admin/sso/{Login URI}/login}}`

  This URL is specific to the admin role. It points to the IdP for SSO authentication, and redirects to the admin portal: `{{https://{host name}/admin/sso/{Login URI}/login}}`

Note: SSO URLs redirect to the default `admin` portal, with endpoint: `/portal/`. See also the section on SSO Users at: *Log in*.

IdP(SSO) credentials

Log in using the relevant SSO identity provider (IdP) credentials.

SSO scenarios for user roles

The table maps user roles to the log in URLs - single role or multiple role (includes Authorized Admin Hierarchy):

Copyright © 2025 VisionOSS Limited. All rights reserved.

User Role	Auth Admin?	URL used	UI (Session Limiting)	Expected Behavior
selfservice	Yes	https://<hostname>/sso/<login-uri>/login	administrator	Redirect to Self-service
selfservice	Yes	https://<hostname>/admin/sso/<login-uri>/login	administrator	Redirect to Admin Portal
selfservice	No	https://<hostname>/sso/<login-uri>/login	selfservice	Redirect to Self-service
administration	Yes	https://<hostname>/sso/<login-uri>/login	administrator	Redirect to Admin Portal
administration	Yes	https://<hostname>/admin/sso/<login-uri>/login	administrator	Redirect to Admin Portal
administration	No	https://<hostname>/sso/<login-uri>/login	administrator	Redirect to Admin Portal
administration	No	https://<hostname>/admin/sso/<login-uri>/login	administrator	Redirect to Admin Portal

Administrators set up with SSO but who have multiple user roles and who wish to access the *Self-service* interface must navigate to the Self-service portal URL upon login:

```
https://<Hostname>/selfservice/#/
```

8.6. User Services

8.6.1. Enable multi vendor users

Tip: *Use the Action search to navigate Automate*

Overview

This procedure enables and sets up multi vendor users, and involves the following tasks:

- Enable relevant Global Settings.
- Configure the multi vendor field display policy (`MultiVendorFDP`).
- Configure entitlement profiles.
- Verify that you have appropriate servers installed and configured.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Multi vendor users in the Core Feature Guide
- Global Settings
- *Configure quick actions for multi vendor users*

Step 1: Enable multi vendor users in global settings

1. Log in to the Admin Portal.
2. Select the hierarchy.

   Note: The global setting to enable multi-vendor is typically defined at the customer hierarchy, although it may be enabled/disabled at any level.

3. Go to **Global Settings**.
4. On the **Enabled Services** tab, enable services, as required.
5. Save your changes.

   Note: For new installs of Automate, once a Cisco UCM is imported and a customer hierarchy and some sites have been created, UCM services are enabled by default at system level; other services must be enabled, as required. The Global Settings are retained on upgrade.

Step 2: Configure multi vendor user field display policy

1. In the Admin Portal, go to **Field Display Policies**.
2. Click on the default multi vendor field display policy (`MultiVendorFDP`) to open its editing screen.
3. Click the toolbar **Clone** icon to create a copy of the default FDP.

   Note:

   - It is recommended that you clone default templates rather than overwriting default settings.
   - The multi vendor FDP is associated with the model *relation/MultiVendorSubscriber*.

4. Edit the cloned multi vendor FDP for your requirements:
   - To add a new card, click the Plus icon (+); then, configure the card.
   - To delete a card, click the Minus icon (-).
   - To edit a card, click the down-arrow on the card to display editing options:
     - Click **Move Up** or **Move Down** to rearrange the position of cards.

       Note: It is recommended that you leave the **User Details** card and the **Quick Actions** in their default positions at the top of the dashboard.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Change card titles.
- Choose whether to display the card as a fieldset with columns.
- Define the actions you require in the Quick Actions.
- Add fields to a card by selecting and moving fields from **Available** to **Selected**.
- Remove fields by selecting and moving fields from **Selected** to **Available**.

Important: Select valid fields for the model (allowed services). Only valid fields will display on the service cards once you apply the FDP.

Check the field naming convention when choosing fields, for example:

- Field names prefixed `account_information` are valid for the **User Details** card.
- Field names prefixed `cisco_webex` are valid for Webex.
- Multi vendor field name formats, such as `mvs_user_qa`, where:
  - `mvs` is the alias for *multi vendor user**
  - `_qa` is *Quick Action*

  For example, the `mvs_user_qa.qa_update_group_membership` field allows for the **Update Group Membership** quick action which opens a transfer box containing a list of MS 365 groups that can be assigned to or removed from the user. If the MS 365 groups have licenses assigned to them, these will then also respectively be applied to or removed from the user. See also the Quick Add Group assigned to the user: *Multi vendor users* and *Quick Add Groups*.

  If a service or action is disallowed in the global settings, entitlement profile, or if required servers are not installed for the service, the system verification check does not allow display of the service or action on the User management dashboard (defined via the FDP), and the user cannot be provisioned with this service. For example, if the Microsoft service is disabled in Global Services, then Microsoft-related quick actions such as Quick Add, User Staging, and Offboard User are not available.

5. Save your changes.

Step 3: (Optional) Configure entitlement profiles for multi vendor

1. In the Admin Portal, go to **Profiles**.
2. Click on the relevant entitlement profile to open its editing screen.
3. Select the services you wish to enable for the profile.
4. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Step 4: Verify servers

To verify that you have the appropriate servers installed and configured:

1. In the Admin Portal, go to **UCM Servers**.
2. Select the relevant server.
3. Repeat this step to verify the presence of all required servers.

8.6.2. Role-based access for multi vendor users

Tip: *Use the Action search to navigate Automate*

Overview

Role access profiles define the permissions that allow users to access services and resources.

Validation checks

When provisioning multi vendor services, the system runs validation checks for multi vendor user against each of four tiers in the system, at the relevant hierarchy. The service must be enabled at each tier before the system allows access to the service:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Validation	Interface	Description
1. Global Settings	Admin Portal Go to **Global Settings (Enabled tab)**.	Enable the service type at the user's hierarchy level, or above.
2. Entitlement profile	Admin Portal Go to the **Profiles** page.	Enable the service in the entitlement profile assigned to the user, at the relevant site. Services can only be provisioned to a user if their entitlement profile allows those services. The entitlement profile lists the provisioning vendor (per service).
3. Device management	Admin Portal Go to the **Servers** page.	The relevant servers must be installed and configured before a service can be provisioned. For example, a UCM server must be installed before UCM services, such as phones, can be provisioned. If you have two or more vendors provisioning devices, Automate verifies that the required servers and devices are configured and available for your system.
4. Field display policy	Admin Portal Configure multi vendor FDP via **Field Display Policies**	Clone and edit the default multi vendor user field display policy (default name: `MultiVendorFDP`).

Multi vendor user access validation example

In this example scenario, a customer admin (or higher) provides a user with site admin role with the ability to view and edit user voice services. The customer admin wants to control the actions the site admin may perform.

- Only the Cisco Voice service is enabled for this site admin
- The site admin may edit user services
- The site admin may not add or delete user services

The table describes the configuration steps to set up this scenario, and the result:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configuration steps	1. Ensure the system has multi vendor user functionality installed. 2. At customer level or above, in the Global Settings (**Enabled Services tab**), enable Cisco UCM only. 3. In the Entitlement Profile for this user, enable Cisco UCM Voice Service only. 4. At site level, configure the multi vendor user field display policy for the profile: • Remove all service cards except Voice. • Remove Add/Delete fields from the Quick Actions panel.
Result	The site admin logs in to a multi vendor user enabled system, at the relevant site hierarchy, and: • Is unable to add or delete services. Only Edit is available in the Quick Actions

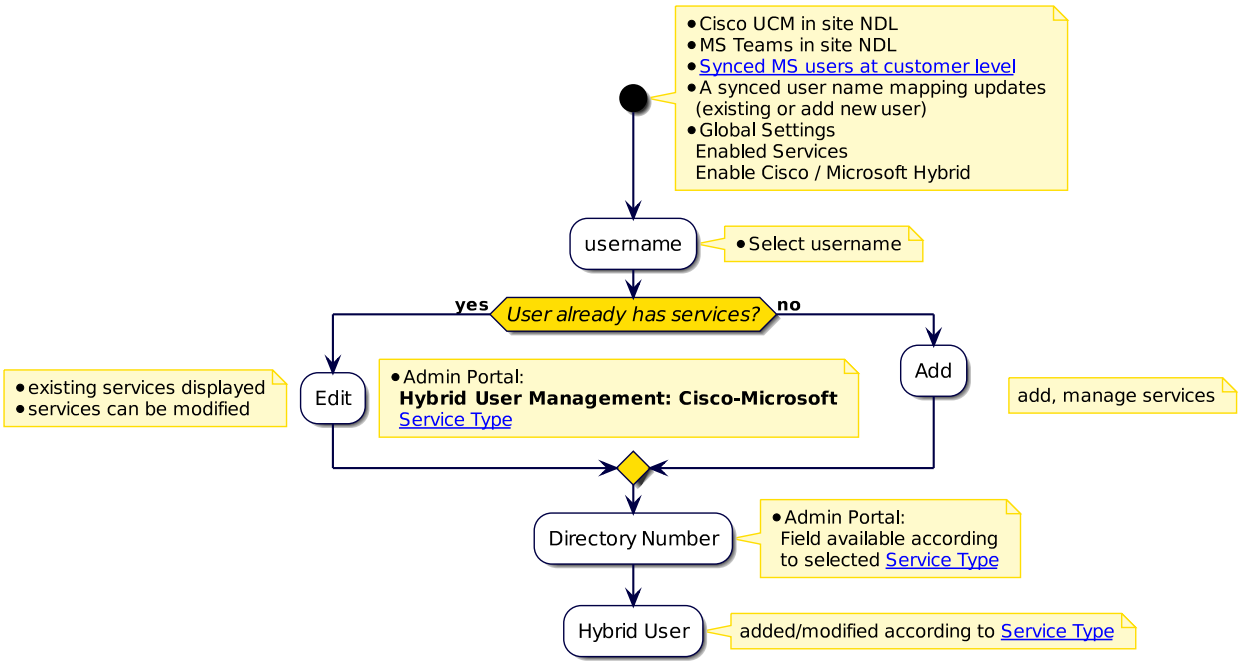
Related topics

- Role-based access in the Core Feature Guide
- Multi vendor users in the Core Feature Guide
- Global Settings in the Core Feature Guide
- Entitlement in the Core Feature Guide

8.6.3. Introduction to Cisco-Microsoft hybrid

The flowchart outlines a Cisco-Microsoft hybrid set up in Automate.

Copyright © 2025 VisionOSS Limited. All rights reserved.



8.6.4. Hybrid Cisco-Microsoft management

Overview

Use the **Hybrid Subscriber Management: Cisco-Microsoft** menu to provision and manage subscribers with Cisco and Microsoft devices and services.

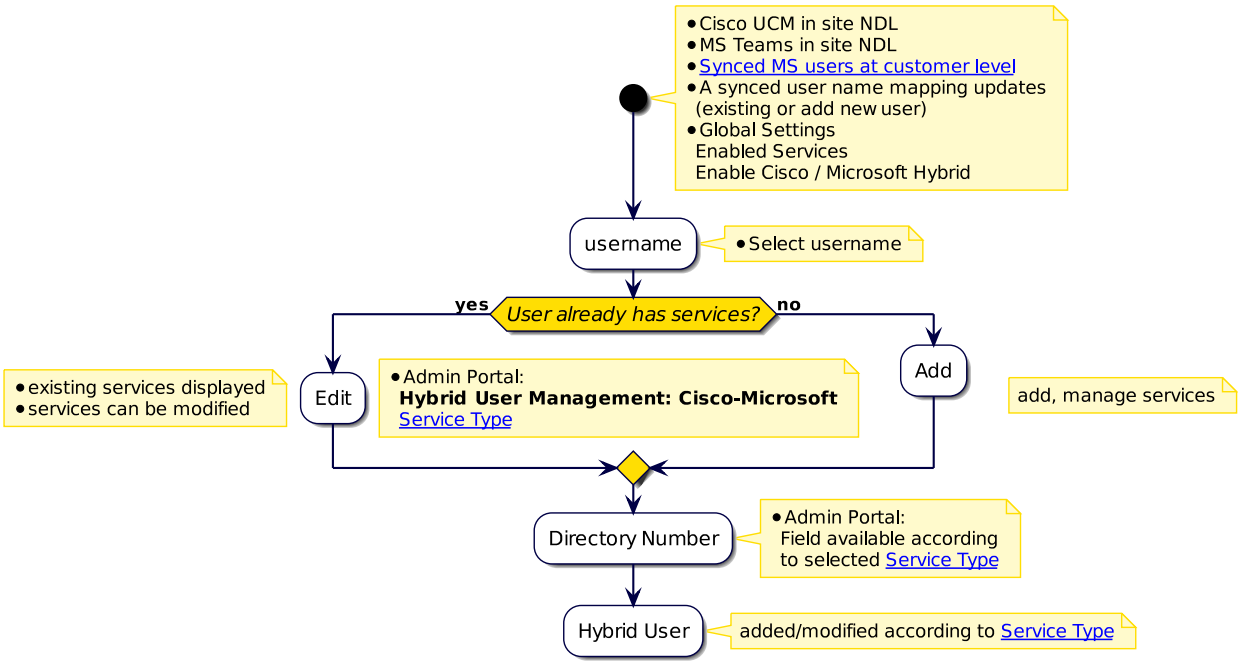
Tip: *Use the Action search to navigate Automate*

Related Topics

- *User profiles*
- *Hybrid service definitions*
- *Global settings*
- the Number Inventory Updates for Hybrid Support topic under Number Management

Copyright © 2025 VisionOSS Limited. All rights reserved.

Provisioning workflow



Prerequisites

- The Global Setting **Enable Cisco** / **Microsoft Hybrid** is enabled, so that the **Hybrid Cisco-Microsoft Management** menu is available. See: **Enabled Services** at *Global settings*.
- To add new hybrid users, sync in the MS Teams users at the customer level. For the management of Microsoft users, see: *Microsoft Quick Start Guide for Automate*.

Workflow steps

Note: For a user selected on the **Users** page, these hybrid user management tasks can also be carried out on the **Hybrid Status** tab of the user by selecting the **Update Hybrid Status** link.

---

1. Log in to the Admin Portal as a provider admin, at the customer level.
2. Go to **Hybrid Subscriber Management: Cisco-Microsoft**
3. Choose the relevant site.
4. On the **Hybrid Subscriber Management: Cisco-Microsoft** page:
   - In the **Username** field, select the user. MS Teams users should be synced in.

     The user's **CUCM User Identity** / **AD UserPrincipalName** should match **MS Teams UserPrincipalName**
   - To include users higher in the hierarchy in the **Username** drop-down, select **Include users at higher hierarchy**.
5. When managing a user who already has Cisco or Microsoft services, these services will be displayed in the list of fields on the **Existing Services** - **User Status & Existing Services** form.

Copyright © 2025 VisionOSS Limited. All rights reserved.

6. Select the required hybrid **Service Type** from the drop-down list.

   The **Entitlement Profile** and **Quick Add Group** are hidden as these are associated with the service type.

7. The **Directory Number** drop-down list is available to select a number after selecting a service type.

Note: If the "Cisco-MS-Hybrid" service type is selected, the choice of Directory Number (Internal or E164) will determine the provisioning.

For details on all the service types, see: *Hybrid service definitions*.

8.6.5. Hybrid service definitions

Note: Consult with VOSS to customize the configuration of Hybrid Service Definitions as well as dialplan additions.

A hybrid service refers to a particular multi-vendor configuration in VOSS Automate and is characterized by a collection of settings, templates and workflows that apply to the management of a user to whom it is assigned.

This collection then determines a particular set of vendor services, entitlement profiles, dial plan additions for the user as well as workflows to run during user management.

Note: Hybrid services require:

- the configuration of the relevant multi-vendor devices on VOSS Automate
- vendor device user sync into VOSS Automate

When selecting the **Hybrid** option in a **Subscriber Profile**, a **Hybrid Service** can be selected and associated with the profile. This service in the profile is associated with a service definition.

Hybrid user management allows for devices and services to be added to *or removed* from a subscriber in accordance with the current and newly selected hybrid service for a user. The workflows in the current hybrid service run to remove elements prior to the execution of workflows in the new hybrid service to add elements.

For example:

- If a subscriber has service type **MS-Only-Hybrid** and is subsequently updated to have no Microsoft service type, the subscriber is updated to service type **No-Hybrid-Service** and associated entitlement profile.
- If a subscriber has service type **Cisco-MS-Hybrid** and is subsequently updated to service type **Cisco-Only**, MS Teams devices are removed from the subscriber, preferred voicemail is updated to be "Cisco" instead of "MS-Teams" and all multi-vendor entitlement profiles are updated accordingly.

The following hybrid services are defined, with default attributes indicated:

- **Cisco-MS-Hybrid**

  User has both Cisco Devices and a Teams Device with an associated E164 number. Cisco Unified CM dial plan configuration allows incoming and outgoing calls.

  - **Quick Add Group**: "System Quick Add Group Hybrid Enable User" - contains MS Teams User Template to enable MS Teams

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Class of Service** and **Entitlement Profile**: by default empty. Select a **Class of Service** to apply to MS Teams users and their calling rights.

The service type offers automatic configuration of services according to the selected **Directory Number** in the Admin GUI: disabling **Use next available line** and then the selected **Line**.

This is carried out by a workflow selecting the appropriate dialplan template addition.

Important: Automate provides standard template additions to the standard Cisco HCS dialplan. Contact VOSS if you wish to use alternative dial plan additions.

  - Both Cisco Devices and a MS Teams Device have an associated E164 number.

    The E164 Number is shared across all devices, for example:

    * INI entry = 3334567, mapped to E164 = +15553334567.
    * The number +15553334567 is set up in Microsoft as the line.

    Calls from colleagues with Cisco phones to the user's Cisco phone will *simultaneously* dial this phone and the MS Teams client. A SNR profile is used on the Cisco User to fork calls to the Teams Client.

  - Internal number selected

    User has both Cisco Devices and a MS Teams Device with no associated E164 number. An E164 number is generated by adding a prefix (+88800) to the internal number for setup in Microsoft, for example:

    * INI = 3334567
    * The number +1888003334567 is generated for use in MS Teams for that user.

    The MS Teams user can dial:

    * internal MS Teams users
    * internal Cisco users
    * external PSTN number (off-net via CUCM)

- **Cisco-No-Services**

  All Cisco and Teams devices, multi-vendor subscriber services will be removed from the user.

  - **Quick Add Group**: "System Quick Add Group Hybrid Disable User" - contains MS Teams User Template to disable MS Teams
  - **Class of Service** and **Entitlement Profile**: by default empty Select a **Class of Service** to apply to MS Teams users and their calling rights.

- **Cisco-Only_MV_SD**

  User has only Cisco devices with an associated E164 Number. Multi-vendor, MS Teams services removed if present.

  - **Quick Add Group**: "System Quick Add Group Hybrid Disable User" - contains MS Teams User Template to disable MS Teams
  - **Class of Service** and **Entitlement Profile**: by default empty

- **MS-Only-Entvoice_MV_SD**

  User has only a MS Teams Device and selected Directory Number. MS Teams Dialplan.

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Quick Add Group**: “System Quick Add Group Hybrid Enable User” - contains MS Teams User Template to enable MS Teams
  - **Class of Service** and **Entitlement Profile**: by default empty Select a **Class of Service** to apply to MS Teams users and their calling rights.
- **MS-Only-Hybrid_MV_SD**

  User has only a MS Teams Device and selected Directory Number. Cisco Unified CM dial plan configuration allows incoming and outgoing calls. Cisco subscriber services are removed if present.
  - **Quick Add Group**: “System Quick Add Group Hybrid Enable User” - contains MS Teams User Template to enable MS Teams
  - **Class of Service** and **Entitlement Profile**: by default empty Select a **Class of Service** to apply to MS Teams users and their calling rights.
- **MS-Only-No-Entvoice_MV_SD**

  User has only a MS Teams Device and no Directory Number. No MS Teams Dialplan.
  - **Quick Add Group**: “System Quick Add Group Hybrid Disable User” - contains MS Teams User Template to disable MS Teams
  - **Class of Service** and **Entitlement Profile**: by default empty Select a **Class of Service** to apply to MS Teams users and their calling rights.
- **No-Hybrid-Service_MV_SD**

  User has no Cisco or MS Teams Devices.
  - **Quick Add Group**: “VOSS-QAG_ExecUser - 88XX SIP”
  - **Class of Service** and **Entitlement Profile**: by default empty

Note: When managing the hybrid services of administrator users by means of bulk loader sheets:

- Values for the `mvs_hybrid_status` field needs to be one of the service names as listed above.
- To unset this value in a bulk load sheet, leave the cell value for the `mvs_hybrid_status` field empty.

Related Topics

- *Hybrid Cisco-Microsoft management*
- *User profiles*
- the Cisco - Microsoft Hybrid Number Inventory topic under Number Management

8.7. Sync & Purge Users

8.7.1. Introduction to user syncs

Overview

Users pushed to Cisco Unified Communications Manager (Cisco UCM) are synced between Automate and Cisco UCM. Adding, updating, or deleting a user in one place is automatically reflected in the other.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Users and default entitlement profiles

New users added to Automate using user management functionality are checked for entitlement against the nearest default entitlement profile, located above the site where you're adding the user.

If no default entitlement profile exists, no restrictions apply to this user. If a default entitlement profile is found, and the user you're adding has devices or services to which this user is not entitled (based on the default entitlement profile), the user add will fail.

User management scenarios

This section provides details on the actions that are carried out when a user is managed, given the absence or presence of the same user in Automate applications or LDAP.

Add user sync scenarios

The table below details add and update scenarios when a user is added that may exist on Automate, applications or LDAP and the *default* Sync Source precedences apply. The cases are:

- if either the user exists or does not exist on LDAP
- if either the user exists or does not exist on any application that is a sync source (APP SOURCE)

Field sync takes place according to:

- Sync Source - see *User sync source*.
- The User Field Mapping that applies - see: *User field mapping*.

Important: Sync Source precedence may override user input. If you update a user on Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (Automate) data

the data of these fields will be updated from the sync source and not the user input added in Automate. The Admin Portal would typically render these fields read-only.

The detailed scenarios for the operation: *adding a user* (model: `relation/User`) are:

Copyright © 2025 VisionOSS Limited. All rights reserved.

data/User exists	device/ldap/User exists	device/<APP>/User exists	Hierarchy	Action	User Sync Source
Y			same as user	Error: user exists	
			current	Create data/User	LOCAL
	Y		same as LDAP user	Create data/User, Update data/User, based on sync source	LDAP
		Y	same as APP user	Create data/User, Update data/User, based on sync source	APP SOURCE
	Y	Y	same as APP user	Create data/User, Update data/User, based on sync source	LDAP
	Y		below LDAP user hierarchy	Create data/User, Update data/User, based on sync source, Move LDAP user to data/User hierarchy	LDAP
		Y	below APP user hierarchy	Create data/User Update data/User based on sync source Move App user to data/User hierarchy	APP SOURCE
	Y	Y	below APP user hierarchy	Create data/User Update data/User based on sync source Move LDAP user to data/User hierarchy	LDAP
	Y		above LDAP user hierarchy	Error: Create User Log entry with message	LDAP
		Y	above APP user hierarchy	Error: Create User Log entry with message	APP SOURCE
	Y	Y	above APP user hierarchy	Error: Create User Log entry with message	LDAP

Update user sync scenarios

The table below details data sync sources and update actions when a user is updated and the *default* Sync Source precedence applies. The cases are:

- if either the user exists or does not exist on LDAP
- if either the user exists or does not exist on any application that is a sync source

Field sync takes place according to:

- the User Field Mapping that applies - see: *User field mapping*.

Important: Sync Source precedence may override user input. If you update a user on Automate:

- that exists on a sync source
- has mapped fields

Copyright © 2025 VisionOSS Limited. All rights reserved.

- has a higher precedence than LOCAL (Automate) data

the data of these fields will be updated from the sync source and not the user input added in Automate. The Admin Portal would typically render these fields read-only.

The detailed scenarios for the operation: *updating a user* (model: `relation/User`) are:

`data/User` exists	`device/ldap/User` exists	`device/<APP>/User` exists	Hierarchy	Action	User Sync Source
Y			same as user	Update `data/User`	LOCAL
Y	Y		same as user or LDAP user	Update `data/User` Non Mapped Fields only Update `data/User` based on sync source	LDAP
Y		Y	same as user or APP user	Update `data/User` Update App/User using reverse App map	APP SOURCE
Y	Y	Y	same as any of user, APP LDAP user	Update `data/User` Non Mapped Fields only Update `data/User` based on sync source Update App/User using reverse App map	LDAP
Y	Y		below user or LDAP user	Update `data/User` Non Mapped Fields only Update `data/User` based on sync source	LDAP
Y		Y	below user or APP user	Error: Create User Log entry with message RBAC issue	APP SOURCE
Y	Y	Y	below any of user, LDAP, APP user	Error: Create User Log entry with message RBAC issue	LDAP
Y	Y		above user or LDAP user	Error: Create User Log entry with message	LDAP
Y		Y	above user or APP user	Error: Create User Log entry with message	APP SOURCE
Y	Y	Y	above any of user, LDAP, APP user	Error: Create User Log entry with message	LDAP

LDAP add sync scenarios

The table below details data sync sources and update actions when an LDAP user is added and the *default* Sync Source precendences apply. The cases are:

- if either the user exists or does not exist on LDAP
- if either the user exists or does not exist on Automate or any application that is a sync source

Field sync takes place according to:

- the User Field Mapping that applies - see: *User field mapping*.

Important: Sync Source precedence may override user input. If you update a user on Automate:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (Automate) data

the data of these fields will be updated from the sync source and not the user input added in Automate. The Admin Portal would typically render these fields read-only.

The detailed scenarios and actions for the operation: *syncing an LDAP user* (sync source is always LDAP) are:

Copyright © 2025 VisionOSS Limited. All rights reserved.

data/User exists	device/ldap/User exists	device/<APP>/User exists	Hierarchy	Action
Y			same as user	Update data/User
				Create data/User
	Y		same as LDAP user	Error Create User Log entry with message Purge current LDAP user
		Y	same as APP user	Create data/User Update data/User based on sync source Update APP data based on sync source
	Y	Y	same as LDAP or APP user	Error Create User Log entry with message Purge current LDAP user
Y			below user	Update data/User Move LDAP user to data/User hierarchy
	Y		below LDAP user	Error Create User Log entry with message Purge current LDAP user
		Y	below APP user	Create data/User Update data/User based on sync source Update APP data based on sync source Move data/User and LDAP user to APP hierarchy
	Y	Y	below LDAP or APP user	Error Create User Log entry with message Purge current LDAP user
Y			above user	Error Create User Log entry with message Purge current LDAP user
	Y		above LDAP user	Error Create User Log entry with message Purge current LDAP user
		Y	above APP user	Create data/User Update data/User based on sync source Update APP data based on sync source
	Y	Y	above LDAP or APP user	Error Create User Log entry with message Purge current LDAP user
Y		Y	above user or APP user	Create data/User Update data/User based on sync source Update APP data based on sync source

Copyright © 2025 VisionOSS Limited. All rights reserved.

LDAP update and delete sync scenarios

The table below details data sync sources and update actions when an LDAP user is added and the *default* Sync Source precendences apply. The cases are:

- if either the user exists or does not exist on LDAP
- if either the user exists or does not exist on Automate or any application that is a sync source

Field sync takes place according to:

- the User Field Mapping that applies - see: *User field mapping*.

Important: Sync Source precedence may override user input. If you update a user on Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (Automate) data

the data of these fields will be updated from the sync source and not the user input added in Automate. The Admin Portal would typically render these fields read-only.

The detailed scenarios and actions for the operation: *deleting an LDAP sync* - manually (M) or automatically (A) - are:

Operation	`data/User` exists	`device/ldap/User` exists	`device/<APP>/User` exists	Action	User Sync Source
LDAP DELETE SYNC (M)	Y	Y		Update `data/User`	LOCAL
LDAP DELETE SYNC (M)		Y			
LDAP DELETE SYNC (M)	Y	Y	Y	Update `data/User` based on sync source Update APP data based on sync source Convert UCM user to local user	LOCAL
LDAP DELETE SYNC (A)	Y	Y		Delete `data/User`	
LDAP DELETE SYNC (A)		Y			
LDAP DELETE SYNC (A)	Y	Y	Y	Delete `data/User` source Delete `relation/Subscriber`	

The detailed scenarios and actions for the operation: *updating an LDAP sync* (sync source is always LDAP) are:

Copyright © 2025 VisionOSS Limited. All rights reserved.

data/User exists	device/ldap/User exists	device/<APP>/User exists	Action
Y	Y		Update data/User
	Y		Create data/User
Y	Y	Y	Update data/User based on sync source Update APP data based on sync source

8.7.2. User sync source

VOSS Automate provides a list of applications from which to sync user data and internally maintains a sync precedence hierarchy of these applications in order to determine the master sync source.

Application:

- MS_LDAP
- OPEN_LDAP
- LDAP
- CUCM
- CUC
- AVAYA_SYSTEM_MANAGER
- BROADWORKS
- MICROSOFT
- MS_365
- PEXIP
- UCCX
- WEBEX_TEAMS
- ZOOM
- MS_TEAMS
- LOCAL

Choose **User Sync Source** to see the default application.

Related Topics

- *Add user sync scenarios*
- *Update user sync scenarios*
- *LDAP add sync scenarios*
- *LDAP update and delete sync scenarios*

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.7.3. Authentication and passwords in user syncs

Users synced from LDAP to Automate (no sso)

LDAP authentication is enabled by default in Automate on users that are synced top-down from LDAP into Automate.

When LDAP users are pushed to Cisco Unified Communications Manager (CUCM) and Cisco Unity Connection (CUC), authentication is either LDAP or local, depending on how the applications are configured. If LDAP authentication is not configured in CUCM or CUC, the user is considered to be a *local* user in UC applications.

Users synced from LDAP to Automate (sso-enabled)

For users synced from LDAP to Automate with SSO enabled, passwords are created and enforced at the Identity Provider (IdP).

Users synced from LDAP to CUCM

For users synced from LDAP to Cisco Unified Communications Manager (CUCM), passwords are not synced like other user details retrieved from LDAP.

When LDAP authentication is enabled, the password in the LDAP server is used unless the password was changed locally in CUCM, forcing the CUCM password to be used.

When LDAP authentication is disabled, the default password is whatever was configured in CUCM as the default. If no default password is defined, then configure a password manually.

Users synced from CUCM to Automate

When users are synced from Cisco Unified Communications Manager (CUCM) to Automate, their passwords are not transferred. An administrator will need to configure the passwords before the accounts can be used.

This affects CUCM users that were manually added to CUCM, and users synced from LDAP.

8.7.4. Re-provision synced LDAP users

This procedure re-provisions users that were synced from an LDAP server, specifically, those users that have been updated on the LDAP server and for which these updates have not been propagated through VOSS Automate.

The re-sync forces an update of the selected users on all UC apps by executing an update data sync as well as its associated workflow.

Tip: *Use the Action search to navigate Automate*

1. Log in as a customer administrator or higher.
2. Go to **LDAP Re-Provision Users**.
3. Choose the LDAP server on which the users need to be re-synced.

Copyright © 2025 VisionOSS Limited. All rights reserved.

4. From the LDAP Users control, add one or more users to re-sync.
5. Click **Save** to start the re-sync action.

8.7.5. Sync Cisco UCM users, lines, and phones

This procedure syncs users, lines, and phones from Cisco UCM.

Note: Syncing lines and phones is intended only for self-provisioning. It is not intended for a full migration scenario. Only Jabber and desk phones can be synced from CUCM. Single Number Reach (SNR) and Extension Mobility are not supported in terms of adding to CUCM first and then syncing into Automate.

Use model instance filters (MIF) to detect users that haven't been synced, and purge them from the affected site. After the users are purged, re-import the CUCM.

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, set the hierarchy path to the hierarchy node where the CUCM server exists.
2. Go to **CUCM Users, Lines, and Phones**.
3. Fill out configuration options for the sync:

Field	Description
Remove Log Messages	Defines whether you want to remove user management logs before syncing.
Remove Log Direction	Displays only if **Remove Log Messages** is selected. Options are *Local* or *Down*. • Select **Local** to remove logs at the hierarchy of the selected CUCM. • Select **Down** to remove logs at and below the hierarchy of the selected CUCM.
Action	Mandatory. Select **Synchronize users, lines, and phones from CUCM**
Cisco Unified CM	Mandatory. Choose the CUCM server. Data is synced from the selected CUCM.

4. Click **Save** to start the sync.

   You can view transaction progress and details in the Transaction Logs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Transaction Logging and Audit in the Core Feature Guide

8.7.6. LDAP sync actions

LDAP Sync Action allows you to perform a bulk sync for users from multiple Organization Units (OU) of any LDAP server.

Note: You can also select the required OUs of a single LDAP server, and perform the users sync only from the selected OUs.

Tip: *Use the Action search to navigate Automate*

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.
2. Go to **LDAP Sync Actions**.
3. Choose the required sync action from **Action** drop-down:

Action	Description
Import	Bulk syncs users from multiple Organization Units.
EnableScheduleSync	Enables syncing for already LDAP scheduled job.
DisableScheduleSync	Disable syncing for already LDAP scheduled.

4. Select the required LDAP Server from the **Available** field to the **Selected** field.
5. Click **Save**.
6. Click **Move Up** or **Move Down** to alter the order of user syncing action for LDAP Server.

8.7.7. Purge a Cisco UCM user from Automate only

This procedure purges a single Cisco UCM user from the Automate database only, while leaving it on the associated UCM.

Note: If the same user is synced from multiple UCMs, it results in a duplicate user on Automate.

Tip: *Use the Action search to navigate Automate*

1. Log in as provider administrator or higher.
2. Set the hierarchy path to the hierarchy node where the CUCM server is.
3. Go to **Local-Purge CUCM User**.
4. Complete the following fields.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Cisco Unified CM	Choose the CUCM from which the user was synced.
User Name	From the **User Name** drop-down list, choose the user you want to delete from Automate.

5. Click **Save** to purge the selected user from Automate.

Note: The user remains on the associated UCM.

8.8. Self-provisioning

8.8.1. Introduction to self-provisioning

The Cisco Unified Communications Manager (Cisco UCM) self provisioning feature allows an end user or administrator to add an un-provisioned phone to a UCM system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user.

The following process is used to self-provision a phone:

1. The user or admin connects the phone to the network.
2. The phone auto-registers.
3. The user or admin dials the IVR application and satisfies the prompts.
4. The IVR application deletes the auto-registered phone and adds it back using templates associated with the user via their user profile.

There are two requirements related to self-provisioning:

1. Before a phone can be self-provisioned, the user must exist in UCM along with their primary extension, Self-service ID, and user profile.
2. After the phone is self-provisioned, in order to do additional subscriber management for the user in Automate, the user, line, and phone must be at the site level in the Automate hierarchy.

8.8.2. Bottom-up user management

A bottom-up approach to user management means users are configured on Cisco Unified Communications Manager (CUCM) and synced into Automate.

There are two possible methods for bottom-up user management:

- Sync LDAP directory into CUCM. Do not configure the LDAP directory sync in CUCM to use a line mask or DN pool to create the user's primary extension. Instead, the user's primary extension and self-service ID are generated in Automate, using a line mask, universal line template, and self-provisioning user profile at the site level.

  Note: During LDAP sync to CUCM, the user is assigned a user profile via the feature group template associated with the LDAP directory. In order for the line mask configured at the site on Automate to be

Copyright © 2025 VisionOSS Limited. All rights reserved.

applied, the user profile assigned previously must be empty or it must be named the 'Standard (Factory Default) User Profile'.

- Use CUCM Quick User/Phone Add to create a user and the user's primary extension.

8.8.3. Top-down user management

A top-down approach to user management means users and lines are configured on Automate and pushed into Cisco UCM. Users may be added via LDAP sync, the Admin Portal, or bulk loading. When users are pushed to UCM the user's primary extension is created, and when a phone is self-provisioned for the user, the phone is automatically moved to the user's site.

Use either of the following methods to configure the user in Automate:

- Generate the user's primary line and self-service ID using a line mask, universal line template, and a user profile at the site level.
- Set the self-service ID per user using Quick user.

Note: You can associate multiple devices (Jabber, iPhone, iPad, 78xx series IP phones, and 88xx series IP phones) to a single subscriber via Automate's user management. This cannot be done through Quick user (QAS) as the default 9971 is added through QAS.

Using a combination of the methods above is possible but is not recommended. For example, you can enable the line mask at the site and use Quick user to set the primary line for some users while not setting it for others. When the line mask is applied, it first checks to see if a primary extension is already assigned to the user (perhaps via Quick user). If a primary extension is already assigned, the line mask is not applied.

8.8.4. Cisco UCM configuration for self-provisioning

To use self-provisioning, regardless of whether top-down or bottom-up user management is used, you must complete these one-time configuration tasks on Cisco UCM:

- Ensure that the Cisco UCM, Cisco CTIManager, and self-provisioning IVR services are activated
- Configure auto registration
- Create one partition and calling search space unique for self-provisioning
- Configure an application user and credentials so the system can connect to the IVR self-provisioning service
- Configure a CTI route point (provides the number that users dial to connect to the IVR)
- Configure self-provisioning with the application user and CTI route point

Refer to the Cisco UCM documentation for details.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.8.5. Site configuration for self-provisioning

Tip: *Use the Action search to navigate Automate*

Regardless of whether top-down or bottom-up user management is used, ensure that the following items are configured in VOSS Automate:

Enterprise deployment:

- Site Defaults (via **Defaults** page)
- Internal Number Inventory (via **Internal Number Inventory** page)

Provider deployment:

- Site Dial Plan (via **Dial Plan** page)
- Site Defaults (via **Defaults** page)
- Directory Number Inventory (via **Add Directory Number Inventory** page)

8.8.6. Generate a user's primary line

For top-down management, the system creates the user's primary line, associates the line as the primary extension, sets the self-service ID, and sets the user's profile. These activities occur when users are pushed to Cisco UCM.

For bottom-up management, the user's primary line is created (if necessary) when the user is moved to a site, or updated once at a site.

You create the line when you perform these tasks.

- Apply the line mask to a user attribute (typically the user's phone number).
- Use the Universal Line Template (ULT) to determine the route partition name and other line attributes. The ULT is specified in the self provisioning user profile, which is specified in the site's default user profile.

For this approach, the administrator configures these items at the site level.

1. Configure universal device templates. See *Add a self-provisioning universal device template*.
2. Configure universal line templates. See *Add a self-provisioning universal line template*.
3. Configure self provisioning user profile. See *Add a self-provisioning user profile*.
4. Configure a site default user profile. See *Set a default user profile for a site*.
5. Configure the line mask. See *Add self-provisioning line mask*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.8.7. Specify the primary line per user

Tip: *Use the Action search to navigate Automate*

In the top-down method that uses Quick Add User, the primary line pattern is specified by the admin. This creates the user's primary line, associates it as the primary extension, sets the self-service ID, and sets the user profile. The line attributes come from Quick Add Group configuration. Therefore, the Universal Line Template does not need to be configured.

Perform these steps:

1. Configure Universal Device Template(s). See *Add a self-provisioning universal device template*.
2. Configure Self-Provisioning User Profile(s). See *Add a self-provisioning user profile*.
3. Configure a Site Default User Profile. See *Set a default user profile for a site*.
4. Configure primary line per user.

For Quick Add User, add at least one line, and select the Self-Service ID checkbox.

8.8.8. Set a default user profile for a site

Set a default user profile for a site, to be used when no user profile is specified when adding a subscriber.

Tip: *Use the Action search to navigate Automate*

1. In the Admin Portal, go to **Defaults**.
2. Click the user profile to set as the default.
3. On the **General Defaults** tab, and from the **Default User Profile (for User Self Provisioning)** drop-down, choose the default user profile for the site.
4. Click **Save**.

8.9. Move Users

8.9.1. Push users to Cisco UCM

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

In Automate, user management involves a series of steps to integrate new users from the following sources:

- Synced from the LDAP directory
- Synced from UCM (Cisco Unified Communications Manager)
- Manual configuration within Automate

One step in this process is to push the user to the UCM assigned to the customer and site where the user was added.

You can push a user to the UCM from Automate in two ways:

Automatic Push	Enable **Auto Push to CUCM** on the **Sites** page.
Manual Push	Executed for individual users via **Quick Add User**

Automate offers various options for provisioning users with phones, lines, and other services and features. Depending on the option you choose, users can be automatically pushed to UCM.

Auto push to UCM is recommended if users are synced in from an LDAP server, or if users are manually configured on Automate and then provisioned with phones, lines, and other services, regardless of whether you configure users through the Admin Portal, bulk loaders, or the API.

Note: If users are initially configured on UCM and then synced into Automate, auto push to UCM is unnecessary as the users are already present on UCM.

Auto push users to Cisco UCM

Users are automatically pushed to a UCM under these conditions:

- When users are moved to a site (via filters, username, or usernames) and that site has a NDL (network device list) containing a UCM.
- When an NDL containing a UCM is added to a site after the site is created.
- When a UCM is added to an NDL that is linked to a site, then users on the site are pushed to the UCM.
- When a new user is created at a site, and that site has a NDL containing a UCM.

Enable auto push users to Cisco UCM

By default, auto push to UCM is disabled in Automate. To enable “auto push to UCM”:

1. Go to **Sites**.
2. Click on a site to open it’s settings.
3. In **Site Details**, select **Auto Push Users to CUCM**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manually add users to Cisco UCM

You can manually add users to UCM from hierarchy nodes between customer and site, inclusive.

To verify that users are available as users, with assigned phones, lines, and features, go to the **Users** page.

Related topics

- *Cisco Quick User*.

8.9.2. Automatically move users synced from Cisco UCM

This procedure automatically moves users that were synced from Cisco UCM, using previously defined move filters.

Tip: *Use the Action search to navigate Automate*

1. Go to the UCM **Servers** page.
2. Click the UCM server to modify.
3. Click the **Publisher** tab.
4. From the **User Move Mode** drop-down, choose **Automatic**.
5. Click **Save**.

   Users are automatically moved based on the previously defined move filters.

8.9.3. Move users

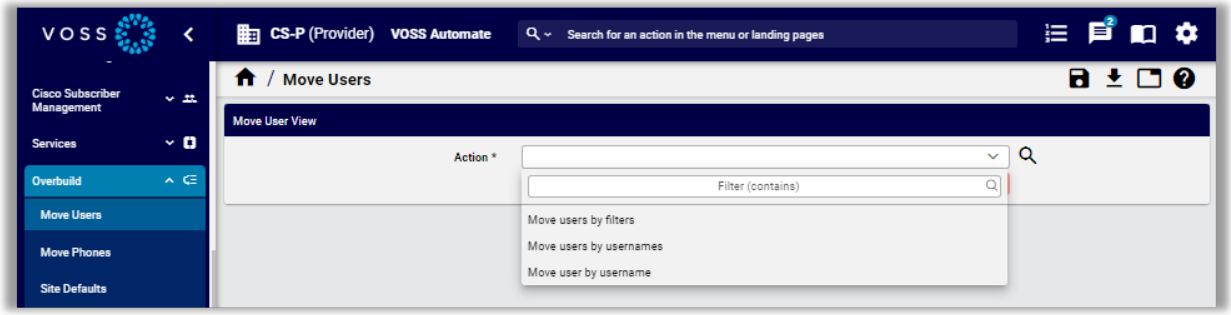
Tip: *Use the Action search to navigate Automate*

Overview

You can move users between any hierarchy nodes at or below the hierarchy node where the users were originally created or synced in. Typically, users synced in at a Customer hierarchy node are moved to various customer sites.

When moving a user, you will choose their role at the target hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.



You will need to consider the restrictions that apply when moving users:

Scenario	Description
Moving users pushed to UCM	• Cisco UCM users can only be moved down the hierarchy. For example, from Customer to Site. • A Network Device List (NDL) containing the same UCM the users were pushed to must be referenced at or below the target hierarchy node.
Moving users between sites	• (Enterprise and Provider) You can't move users between customers. • (Enterprise deployments) You can't move users from one site to another site as this will fail with dialplan errors. • (Provider deployments) You can only move users between sites that: – Reference the same NDL – Have the same type of site dial plan – Are associated with the same country

Note: When moving a user for SLC dialplan the lines associated to the agent line and the shared line show warnings in the form of logs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Create a Filter to Move Users in the Core Feature Guide
- Automatically move users synced from Cisco UCM in the Core Feature Guide

Move user from customer to site

This procedure moves users from a customer to a site.

Pre-requisites:

- Create relevant filters. See *Create a filter to move users*

To move a user from the customer level to a site:

1. In the Admin Portal, go to **Move Users & Services**.
2. From the **Action** drop-down, choose an option for moving the user/s:

Action	Description
Move users by filters	Moves users based on one or more user attributes, for example, City or Street. a. At **Move From Hierarchy**, select the hierarchy node from which you are moving the user. b. At **Filters**, choose one or more move filters from the **Available** list, and click the arrow to move the filters to the **Selected** list. Click the up/down arrows to change the order of the filters, which determines the order in which they are applied.
Move users by usernames	Moves multiple users at once, by their username (bulk move). a. At **Move From Hierarchy**, choose the hierarchy node from which you are moving the users. b. From the **Move To Hierarchy** drop-down, choose the target hierarchy node. c. From the **Set Default Role** drop-down, choose the default role for the moved users. This default role will be assigned to the moved users unless valid LDAP Custom Role Mappings have been configured, which take precedence over the default role. d. Click **Users +**, and from the drop-down, choose the user to move, repeat for each user you want to move. Alternatively select the **Move All Users** checkbox to select all the users.
Move user by username	Move a single user, by their username. a. At **User**, choose the user to move. b. At **Move To Hierarchy**, choose the target hierarchy node. c. From the **Set Default Role** drop-down, choose the default role to assign to the moved user. This default role will be assigned to the moved users unless valid LDAP Custom Role Mappings have been configured, which take precedence over the default role. The list of available roles will include those where the **Hierarchies Allowed** list of the role contains the target hierarchy selected in the **Move To Hierarchy** list.[1]

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Click **Save**. Users are moved.
4. Go to the **Users** page to verify that users were moved to the correct target hierarchy.

Related Topics

- For more details around moving one or more users by username, see *LDAP custom role mappings*

Move users from one site to another site

provider

As an administrator, you can move users from one site to another with their assigned devices and services intact.

Note: Certain conditions must be met for a site-to-site move to succeed. These conditions differ slightly for users in non-SLC dial plans and users in SLC dial plans.

Move users between sites with non-SLC dial plans

When moving a user with their devices and services between sites with a non-SLC dial plan configured, Automate checks the following conditions:

- Both sites must be configured with a SLC dial plan.
- Both sites must use the same NDL.
- Both sites are in the same country.
- The SyncTo hierarchy is a parent of both sites.
- The target site data/SiteDefaultsDoc contains the required default settings (that is, they are not empty nor null).
- The role is valid at the target site.

When moving a user from one (non-SLC) site to another (non-SLC) site, the following models and relations are moved with the user:

- `relation/User`
- `relation/Voicemail`
- `relation/Subscriber`
- `relation/SparkUser`
- `relation/LineRelation`
- `relation/HcsCucmCcTagREL`
- `data/InternalNumberInventory`

Various fields are updated for the target site (by the target site's site defaults) for the models that are moved. These fields include (but are not limited to), the following:

- Voicemail Pilot Numbers

[1] See: *Role Management*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- UCM Device Pool
- UCM Location
- UCM Region, and others

The following fields are updated for the `device/cucm/Line` model:

- Calling Search Space Name
- Route Partition Name
- Share Line Appearance Css Name

The following models are updated for `relation/Subscriber`:

- Device Profile
- Remote Destination Profile
- Phones

Each of these models contains a **Lines** field, which in turn can contain individual lines. In a site-to-site move, the E164 Mask and Route Partition Name fields are updated for each line contained in these models.

Additionally, the move updates some fields within these individual models:

- Remote Destination Profile
  - Device Pool Name
  - Route Partition Name within the Line Associations
- Phones
  - Device Pool Name
  - Location Name

You will need to update these values if you wish to use the overbuild with your existing Cisco UCM data in the future.

The following models trigger a warning message when you attempt to move them from one site to another. While Automate does not prevent you from moving these models, a system message describes the possible implications for moving them:

- E.164 associations
- Call pickup groups
- Hunt lists

Note: When using an API for a older version of Automate (prior to v11.5.1), the Move Users function has the previous behavior. Devices and services do not move with a user.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Move users between non-SLC sites with directory number routing configured

For moves between non-SLC sites with directory number routing (DNR) configured at *either* site, a system message is triggered to warn that any lines associated to the user being moved may not work correctly unless you take one of the recommended actions provided. See the Advanced Configuration Guide to perform the first recommended action.

Move users between sites with SLC dial plan configured

When moving users between sites with a SLC dial plan configured, the required conditions are the same as with non-SLC plans. The only difference is that no error is triggered when the system check detects an SLC dial plan configuration for the customer.

Note: When moving users from a dial plan site to a non-dial plan site, the users are set to a default CSS.

When moving users from one SLC site to another SLC site, the same models and relations are moved as for sites with non-SLC dial plans, with the following exceptions:

- When moving `relation/Subscriber` -> Lines:
  - Lines are disassociated from all phones and the relation.
  - Removing the line from **Phones** should remove the primary line from the relation.

These models are **not** handled when moving SLC dial plans, because the line does not move:

- Internal Number Inventory (INI)
- E.164 Association
- E164 Inventory
- Call Pickup Group
- Hunt List

The following models trigger a warning message when you attempt to move them from one site to another. While Automate does not prevent you from moving these models, a system message notifies you of the possible implications of moving them:

- Agent line associations
- Lines associated to a user's phones, device profile, or RDP
- Voicemail

Moving Microsoft users

Moving a Microsoft user manually (via **Move User**) also moves the following models:

- device/msgraph/MsolUser
- device/msteamsonline/CsOnlineUser
- device/msexchangeonline/UserMailbox

These models are moved regardless of the source and target hierarchies.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.9.4. Site-to-site user move transaction log errors

Transaction log errors occur with a site-to-site user move, if the following conditions are not met:

- Each site is not in the same country.
- (Provider deployment) Sites must have the same types of dial plans (SLC vs. Non-SLC).
- The target site *data/SiteDefaultsDoc* contains the needed default settings (that is, they are not empty or null).
- Move is not outside the *sync_to_hn*.
- Role is valid at move to site.
- UC applications resources are set to false.

Review the transaction log for error messages and actions to resolve the errors.

8.9.5. Manage duplicate usernames

Tip: *Use the Action search to navigate Automate*

Users are created in a sync with LDAP or Cisco Unified Communications Manager (Cisco UCM), or they're created manually in Automate.

Important: Usernames for admin and non-admin users must be unique within the hierarchy, both upwards and downwards. User emails must be unique system-wide.

All users are created according to these duplicate username guidelines:

- A user's username can't be updated if another user in the current hierarchy has the same username. This restriction includes above, below, or at the same level in the current hierarchy.
- You can't add a user with the same username as another user that is above, or was originally above before being moved, the current hierarchy.
- You can't manually add a user with the same username as another user at the same level or below in the current hierarchy.
- You can't convert a user to a provisioned user or Cisco UCM user if another user at the same level or below the UCM in the current hierarchy has the same username.
- A user may or may not be synced from LDAP or UCM if another user at the same level or below in the current hierarchy has the same username.

  This condition depends on the source of the existing user.

The following tables describe sync conditions for users created in a LDAP or UCM sync.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Users created in an LDAP sync:

Source of existing user	Action
LDAP	Simple user update, if the user is coming from the same LDAP server
UCM	Update user, update provisioning status with LDAP server and SyncTo info
Manually created	Update user, update provisioning status with LDAP server and SyncTo info

Users created in a Cisco UCM sync:

Source of existing user	Action
LDAP	User is not synced
UCM	Simple user update, if the user is coming from the same UCM server
Manually created	Update user, update provisioning status and SyncTo info with UCM server

Users created in Automate and auto pushed to Cisco UCM

The table refers to users created in Automate using:

- Users page
- Quick Add User
- Auto Push feature on Site

Quick Add User and User Management create Automate and non-Automate users, while Manage Users and the Auto Push to Cisco UCM feature convert existing users into provisioned users.

Source of existing user	Action
LDAP	Update user, update provisioning status with UCM server (keep SyncTo info the same)
UCM	No action or updates are necessary
Manually created	Update user, update provisioning status with UCM server and update SyncTo to the UCM hierarchy if the current SyncTo is below it

Note:

- If a user can't be created or updated during an LDAP or UCM sync, a log is created in **Log Messages**, and the sync succeeds.

  If a user can't be created or updated manually, an error message is generated.
- If the duplicate user check fails, the transaction fails and the user is not converted to a provisioned user.
- If a user's SyncTo value is updated, SSO User updates can result. The SSO User's IDP is set to the IDP configured at the new SyncTo hierarchy node. If no IDP is configured at the new SyncTo hierarchy node, the SSO User is deleted, if it existed. If an IDP is configured at the new SyncTo hierarchy node, but no SSO User exists, an SSO User is created at the user's hierarchy node.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- An update is blocked if two duplicate users are from the same source but originate from different servers.

8.10. Session Timeouts

8.10.1. Session timeout rules

The following rules apply to the idle session timeout and absolute session timeout values that can be applied to users via a credential policy:

- Setting the absolute session timeout to 0 disables it.
- The absolute session timeout takes priority over the idle session timeout. Therefore, setting the absolute session timeout to a value less than the idle session timeout effectively disables the idle session timeout.
- Credential policy session timeouts do not apply to SSO authenticated users. For SSO authenticated users, Automate honors the SessionNotOnOrAfter SAML 2.0 attribute, which is equivalent to an absolute session timeout, although controlled by the IDP.

Note: Timeout limits will initiate the display of timeout limit notifications in the Admin Portal - see: *Timeout limit notifications*.

8.10.2. Timeout limit notifications

Timeout limit notifications are displayed in accordance with the credential policy that is associated with a user. See: *Customized credential policy* and *Session timeout rules*.

From 60 seconds before the session limit, in other words before a session expires, a warning message "Session will expire in [n] seconds" will show in the Admin Portal and will count down.

If the idle session limit generated the message (and the idle session limit is set to less than the absolute session limit), the user has the option to click the **Stay Logged In** button to extend the session. If the absolute session timeout is about to be reached, the user has the option to click the **Log Out Now** button to return to the login screen or to click **OK** to dismiss the message and finalize work before logout. All transactions submitted after clicking **OK** will be processed.

If the user does not click a button on the warning message box, the user is logged out and the Admin Portal returns to the login screen.

SSO users see the following message:

"Your Single sign-on session will expire in [n] seconds. All transactions submitted after clicking **OK** will be processed. When the session expires, you will be automatically redirected to the log-in page."

For the Admin Portal theme modification of the notification, refer to the Advanced Configuration Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.11. User Accounts and Passwords

8.11.1. Manage passwords

Passwords can be set by default in various ways, and can be configured between LDAP, Automate, and other systems, such as Cisco UCM.

Managing your own account password

Locally authenticated logged in users and administrators can manage their own account passwords.

Note: Users authenticated via Single Sign On (SSO) or LDAP do not have access to the Change Password functionality as these passwords are not managed in Automate. However, a user with authentication method set to Local can change their password even if a SSO IdP server is in scope in the hierarchy.

Self-service user passwords

Self-service users can reset their passwords from the Self-service Login page. Provided the user updates their local user password first and then logs in to authenticate, the password reset also updates the Self-service user's UC app passwords, including Jabber devices, voice mail, and Webex passwords.

8.11.2. Passwords and manually added users

User added manually via Subscriber Management

A user added through Subscriber Management in Automate has the same password that was configured in VOSS Automate when the subscriber was provisioned.

User added manually via User Management

A user added through User Management has the local VOSS Automate password that was specified when the user was created. When this type of user is pushed to Cisco Unified Communications Manager (Unified CM), the password is not pushed. Instead the password can be configured in one of the following ways:

- Create a default password with Unified CM
- Set the password in the CUCM end user page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a default password with CUCM

1. Log in to Unified CM as an administrator.
2. Choose **User Management > User Settings > Credential Policy Default**.
3. Choose the line item that has the Credential User to 'End User' and Credential Type to 'Password'.
4. Enter the default password in the confirmation box and click **Save**.

Note: Ensure that the user has the correct role defined.

Set the password in the CUCM End User page

1. Log in to Unified CM as an administrator.
2. Choose **User Management > End User**.
3. Filter for the user you wish to modify.
4. Change password fields for the specified user.

8.11.3. Force a user to change their password

Tip: *Use the Action search to navigate Automate*

You can use a credential policy to force users to change their passwords on initial login. However, an administrator can manually force a user password change on the next login attempt.

To manually force a password change:

1. Log in as provider, reseller, or customer administrator.
2. Go to the **Users** page.
3. Click the user whose password you want to be changed on the next login attempt.
4. Click the **Account Information** tab.
5. Select the **Change Password on Next Login** check box.
6. Click **Save**.

   The next time the user attempts to log in, they are prompted to change their password. Once the password is changed the **Change Password on Next Login** check box is cleared.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.11.4. Force administrators to change their password

Tip: *Use the Action search to navigate Automate*

You can use a credential policy to force administrators to change their passwords on initial login. However, an administrator at a higher hierarchy level can manually force an administrator to change password on the next login attempt.

To manually force an administrator to change their password:

1. Log in as provider, reseller, or customer administrator.
2. Go to the **Admins** page.
3. Click the administrator whose password you want to be changed on the next login attempt.
4. Click the **Account Information** tab.
5. Select the **Change Password on Next Login** check box.
6. Click **Save**.

   The next time the administrator attempts to log in, they are prompted to change their password. Once the password is changed the **Change Password on Next Login** checkbox is cleared.

8.11.5. Change your own password

Locally authenticated users can change their own password.

Note: Locally authenticated users includes users where a SSO IdP is configured at higher levels of the hierarchy, but the user has Authentication Method set to Local.

1. Log in to the Automate Admin Portal.
2. Click the toolbar **Settings** icon (Cog), then select your profile name from the drop-down to open the **Account** page.
3. Click **Change Password**.
4. Fill out your current password and a new password, then click **Submit**.

   Note: Refer to *Customized credential policy* for more information about password length and password complexity requirements, if required.

   Your password is changed.

Copyright © 2025 VisionOSS Limited. All rights reserved.

8.11.6. Unlock a locked user account

Tip: *Use the Action search to navigate Automate*

This procedure unlocks a user's account, where the user is locked out on account of a credential policy violation.

1. Log in as provider, reseller, or customer admin.
2. Go to the **Users** page.
3. Click the user whose account you want to unlock.
4. On the **Account Information** tab, clear the **Locked** checkbox.
5. Click **Save**.

8.11.7. Unlock a locked admin account

Tip: *Use the Action search to navigate Automate*

This procedure unlocks an admin user's account, where the admin is locked out due to a credential policy violation

Prerequisites:

- You must be an administrator user at a hierarchy node above the hierarchy node of the locked out admin user.

1. Log in as provider, reseller, or customer admin, depending on the location of the locked out administrator.
2. Go to the **Admins** page.
3. Select the relevant admin user (the user with the locked account).
4. On the **Account Information** tab, clear the **Locked** checkbox.
5. Click **Save**.

8.11.8. Manually disable a user account

This procedure manually disables a user account. Typically, a user account is disabled when the password has expired. However, an administrator can manually disable a user account at any time.

Note: A user account is typically disabled when the password expires. However, an administrator can disable a user account at any time. Manually disabling a user is preferred to manually locking out a user as you can provide the reason for disabling.

Prerequisites:

- You must be an administrator to manually disable a user account.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer admin.
2. Go to the **Users** page.
3. Click the user whose account you want to disable.
4. On the **Account Information** tab, select the **Disabled** checkbox.
6. In the **Reason for Disabled** field, enter the reason the account is disabled. The reason is displayed to the user when their next login attempt fails.
7. Click **Save**.

8.11.9. Manually disable an admin account

Typically, an administrator account is disabled when the password has expired. However, an administrator at a higher hierarchy level can manually disable an administrator account at any time.

Note: Manually disabling an administrator is preferred to manually locking out an administrator as you can provide the reason for disabling.

Tip: *Use the Action search to navigate Automate*

1. Log in as provider, reseller, or customer admin.
2. Go to the **Admins** page.
3. Click the administrator whose account you want to disable.
4. Click the **Account Information** tab.
5. Select the **Disabled** checkbox.
6. Enter the reason the account is disabled in the **Reason for Disabled** field. This reason will be displayed to the administrator when the next login attempt fails.
7. Click **Save**.

8.12. Self-service

8.12.1. Introduction to Self-service

Using the VOSS Automate Self-service interface, users can configure their own phone settings, including voicemail, call forwarding, availability, and speed dials.

To access the Self-service interface, a user must be assigned a *selfservice* role in VOSS Automate. A user may get a *selfservice* role in one of the following ways:

- Automatically when synced from LDAP, if the LDAP sync has the user role configured to a *selfservice* role.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- By default when synced from Cisco Unified Communications Manager.
- Manually assigned by an administrator via **Users**.

Tip: *Use the Action search to navigate Automate*

To access the Self-service interface, the user enters the following in the browser URL field:

```
https://<Hostname>/selfservice/#/login?theme=[your_theme]
```

Note: Access to the Self-service interface and the VOSS Automate Admin Portal are mutually exclusive *unless* the administrator user is assigned *both* of:

- An Authorized Admin Hierarchy instance containing an associated admin role. For details on the Authorized Admin Hierarchy, see: *Authorized Admin Hierarchy Roles*.
- A *selfservice* role directly to the user.

Otherwise, if an administrator needs access to the Self-service interface, the administrator needs a second user configured in VOSS Automate with a *selfservice* role assigned to it.

If the theme value is set as `login?theme=cisco_selfservice` then the theme will revert to the Self-service theme that has been set as the default.

8.12.2. Self-service and user configuration

Overview

As an administrator, you can:

- Configure various aspects of the Self-service interface
- Provide user access to Self-service
- Configure services for the users as required

The table provides a summary of the configurable items for the Self-service interface.

Configurable items in the Self-service user interface

Tip: *Use the Action search to navigate Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Task or Item	Description
User access	A user can log in to the Self-service GUI if a 'System User' entry exists for the user. A 'System User' entry is created automatically when a user is added as a subscriber. You can grant a user access to Self-service by creating a user with a *selfservice* role directly in the system user interface. A user with this role is not able to view devices or any services associated with the devices. Manually added users also cannot view personal information such as first name, last name, address, department, etc. You can also provide an administrator with user access to the Self-service GUI by assigning an Authorized Admin Hierarchy instance to the admin that also includes an administrator role.
User Authentication	Self-service authentication is controlled by the administration interface using the same three authentication methods: **Automatic**, **LDAP**, and **SSO**.
GUI Themes and Branding	The Self-service GUI interface can be branded by configuring Cascading Style Sheets and images and logos. It uses the same theme upload and download interface used for the administrator GUI. The theme itself however, is different between the administrator and Self-service interface (based on the user role). The log in page theme is also loaded from the URL: https://<host>/selfservice/#/login?theme=mytheme
Personal Phones (Remote Destinations)	You can automatically assign a remote destination profile (RDP) to a user so that they can manage their own personal phones and simultaneous ring settings. Select the **User can enable Personal Phone Management (add Remote Destination Profile)** checkbox on the **Personal Phones** tab of **Self-service Feature Display Policy**. If no RDP is associated to the user, the Personal Phones management interface in Self-service is hidden. Multiple RDPs for each user are not supported. The Personal Phones management interface in Self-service is also hidden if a user has more than one RDP associated.

For more information, see:

- *Add a user*
- *Add admin user*
- *User authentication*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Task or Item	Description
Dual-Mode Phones - Mobile ID	If a user has a dual-mode device associated, they can manage the phone number and simultaneous ring settings for the device. If no dual-mode device is associated, the relevant settings are hidden in the Self-service interface.
Voicemail	Voicemail settings are only visible in the Self-service interface if the user has a voice mailbox. Click the **Voicemail** tab of **Self-service Feature Display Policy** to set voicemail settings, notification devices, and SMS Interfaces.
Passwords and PINS	Users can modify their own Passwords and PINs if the Self-service Feature Display Policy is set to 'Show' these items. Click the **My Information** tab of the **Self-service Feature Display Policy** page to change this setting.
Link to a WebEx server	Users have a link to their Webex server from the Self-service interface if this item is set to 'Show'. Click the **My Information** tab of the **Self-service Feature Display Policy** page to change this setting.
Hyperlinks to predetermined objects or items such as a support site or downloadable User Guide	As the administrator, you specify the hyperlinks that appear in the Self-service interface. Refer to the Automate "Self-service Guide".
Call Forwarding	Displays the call forwarding status of a user's phone lines. You can specify whether Basic or Advanced call forwarding is set to 'Show' in the Self-service interface. Click the **Call Forward** tab of the **Self-service Feature Display Policy** page to change this setting.

Related topics

- *Cisco phones*
- *Voicemail*

8.12.3. Create a Self-service link

Tip: *Use the Action search to navigate Automate*

1. Navigate to the required hierarchy.
2. Go to **Self Service Links**.
3. Click the Plus icon (+) to add a link.
4. Enter a name for the set of links.
5. Click the Plus icon at **Links** to create one or more links. For each link:
   - Provide a description (which will display on the Self-service GUI).
   - At the **Link** field, provide the URL, for example: `http://...`.
6. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

9. Call Groups

9.1. Microsoft Call Groups

9.1.1. Auto attendants

Tip: *Use the Action search to navigate Automate*

Overview

Automate allows you to add, update, and delete auto attendants for Microsoft Teams users from within the Automate GUI, and to have these changes update on the Microsoft Teams portal. Changes you make on the Microsoft Teams portal online also update the auto attendants in Automate.

Note: Auto attendants allow people who call in to your organization to self-navigate a menu so that they can be correctly routed to the required department, person, or operator. When setting up an auto attendant for your system, you can choose a greeting, set up menus, and choose how calls are redirected (to another user, team, or group).

Audio files for auto attendant

If you wish to use audio files for the auto attendant, to play a message or greeting for example, note the following:

- Automate supports the following file types: *.MP3*, *.WMA*, *.WAV*

  The format of *.WAV* files require the correct resolution and rates. Microsoft specifies these requirements:

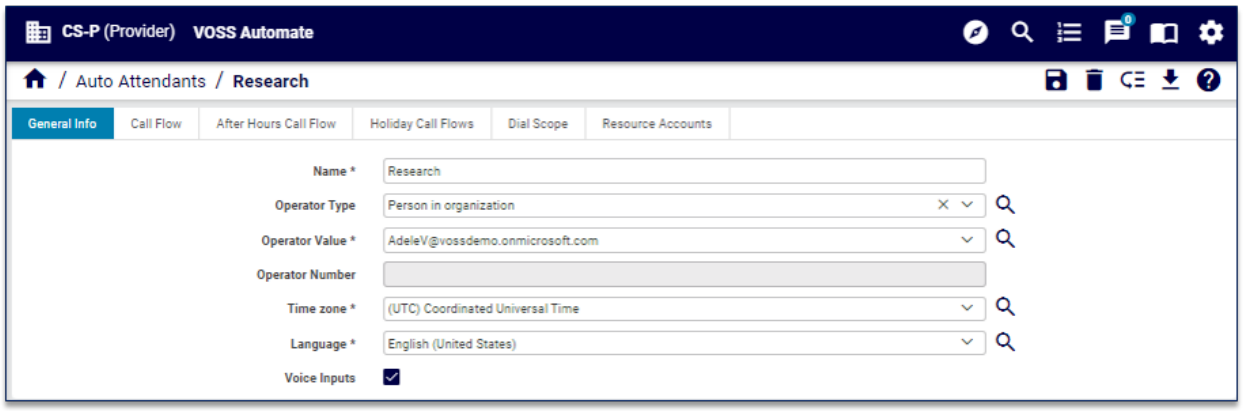
  - Uncompressed, linear Pulse-code modulation (PCM-encoded)
  - 8-bit, 16-bit, or 32-bit resolution
  - Mono or stereo channel
  - Sampling rate of 8 kHz or 16 kHz
  - Maximum audio file size 5 MB

.MP3 files are supported with commonly accepted bit rates and encoding.

Ensure that your audio files have the correct specifications. You can use an app such as *Audacity* to create correctly formatted audio files.

Auto attendants updated in Automate will copy the audio files to the Microsoft Admin Portal using SCP. This can be seen in the transaction logs.

- Audio files must be uploaded to Automate via the **File Management** page.



Related topics

- *Teams* in the Core Feature Guide
- *Groups* in the Core Feature Guide

View and manage auto attendants

You can view, add, or update Microsoft auto attendants via the **Microsoft Call Groups** dashboard:

- Click **View Auto Attendants** to see a list of auto attendants that exist for your organization, whether added in Automate or in the Microsoft Teams online portal.

  On this page, you can:

  - Click on an auto attendant in the list view to open its editing page, where you can view its details, or update it.
  - Select an auto attendant in the list to delete it.
  - Click the Plus icon (+) to add a new auto attendant.
- Click **Add Auto Attendants** to add a new auto attendant.

When adding or editing an auto attendant, settings are defined or updated via the following tabs/panels:

- *General Info*
- *Call Flow*
- *After Hours Call Flow*
- *Holiday Call Flows*
- *Dial Scope*
- *Resource Accounts*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *Authorized users*

Note:

- Voicemail options you choose are your MS Exchange service data synced in to the Microsoft tenant you have set up in Automate, from the Microsoft Teams online portal.
- Only users enabled for Enterprise Voice can be used as the answer or redirect options in call flows for auto attendant.

General Info

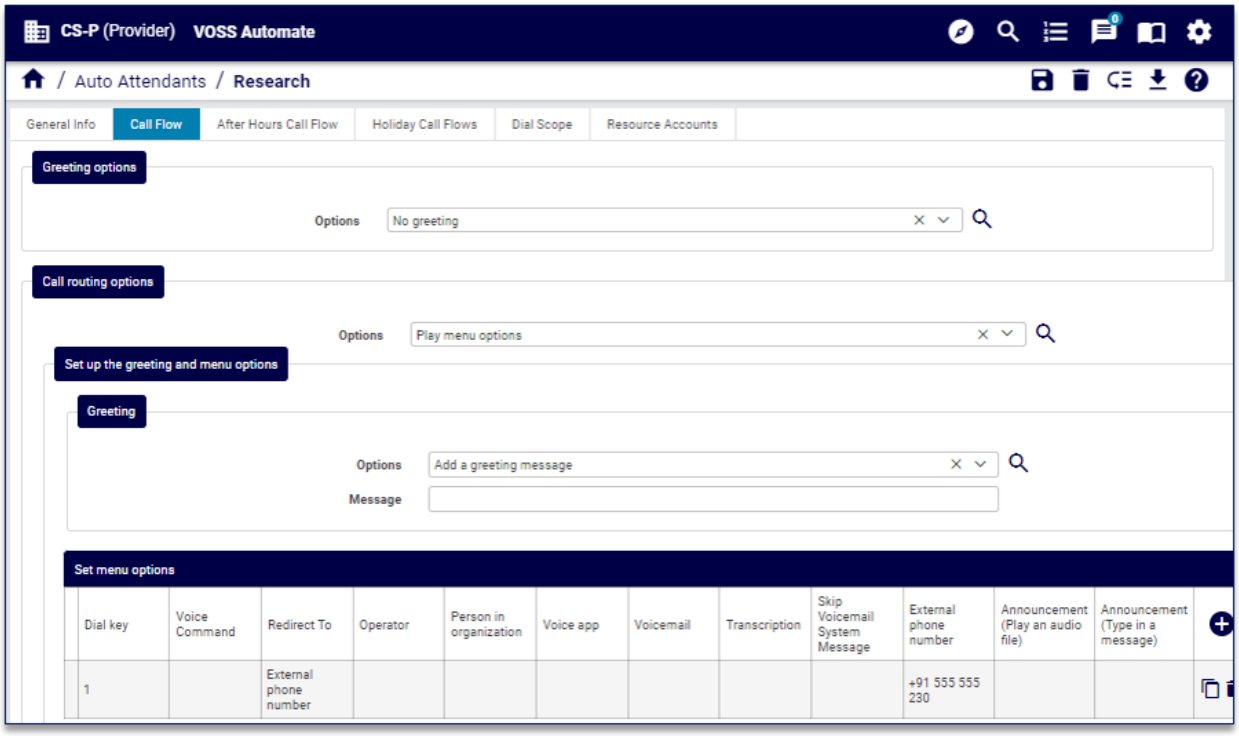
The table describes the fields on the General Info tab/panel:

Field	Description
Name	Mandatory. The name of the auto attendant.
Operator Type	Optional. Options are: • No operator • Person in organization • External phone number • Voice app
Operator Value	Mandatory. Field is hidden when operator type is *No operator*. When operator type is *Voice app*, operator values are call queues or auto attendant resource accounts.
Operator Number	Field is hidden when operator type is *No operator*.
Time zone	Mandatory.
Language	Mandatory.
Voice Inputs	Optional. Defines whether the auto attendant uses voice input.

Call Flow

The Call Flow tab/panel defines the call flow for the auto attendant. On this tab you can set up greeting and routing options, and menu options for call routing.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes the fields on the Call Flows tab:

Field	Description
Greeting options	Defines whether there is a greeting, and if so, choose the greeting, for example, play an audio file or add a greeting message.
Call routing options	Defines the system behavior for call flow, for example, play menu options, disconnect the call, or redirect the call. If you're choosing to redirect the call, you can choose either a person in the organization, voice app, resource account, external phone number, or voicemail. Depending on the option you select, additional options display, for example, to specify the person, phone number, resource account, or phone number.
Set up the greeting and menu options	Choose greeting options, a message, and set up the dial keys that define the behavior for how a call is routed via the menu, for example, to send a call to voicemail, or to a person in the organization, or play an announcement. Depending on the options you choose, you can define options for the redirect, for example, to choose a number for voicemail, or choose the voice app, or set up the external phone number to redirect the call.

Note:

- If you're adding a greeting message, **Message** is a mandatory field.
- If you're playing an audio file, **Audio File** is a mandatory field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

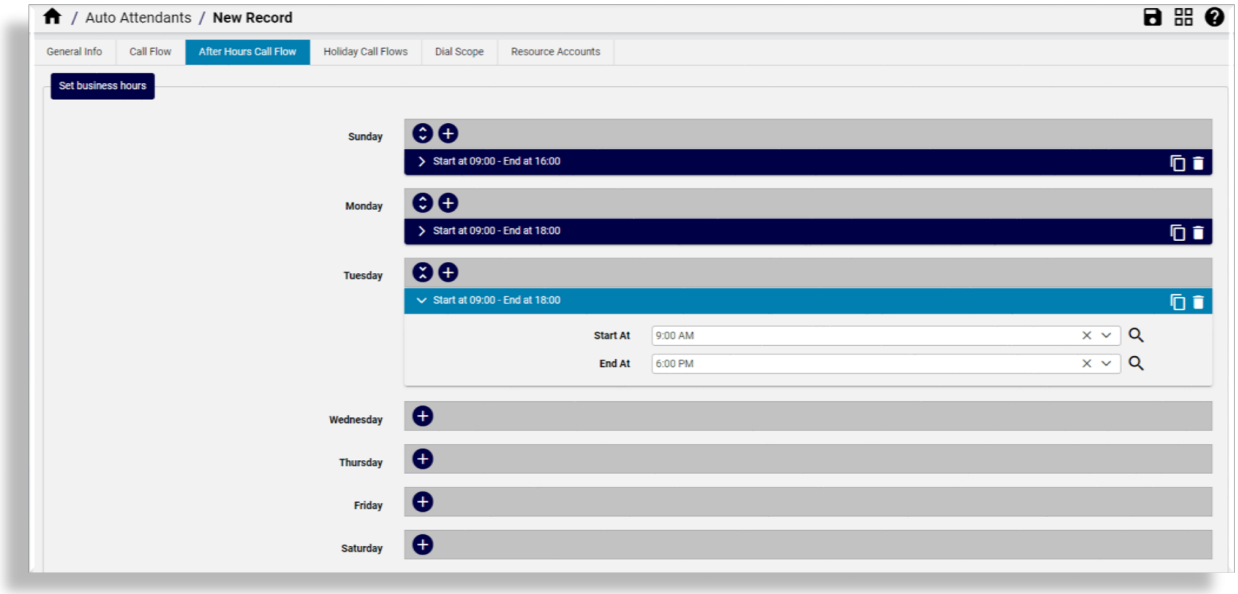
After Hours Call Flow

The After Hours Call Flow tab/panel defines the call flow for after hours calls for the auto attendant.

On this tab you define the business hours for your organization for each day of the week. You will need to choose a start time and an end time from a drop-down of hours and minutes (in 15 minute increments for a 24 hour period), and then define the system behavior for routing incoming calls outside of the predefined business hours, Monday through Sunday, for example, to set up greeting options and menu options, and define whether calls are disconnected or redirected (for example, to person in the organization, a resource account, an external phone number, voicemail, or voice app), and the options for the call flow in each instance.

To set the after hours period to a full day, choose a start time of *12:00 AM*. The system automatically sets the end time also to *12:00 AM*, representing a full day. Choose *None* to clear a start or end time.

Note: If you're adding a greeting message, **Message** is a mandatory field. If you're playing an audio file, **Audio File** is a mandatory field.



Holiday Call Flows

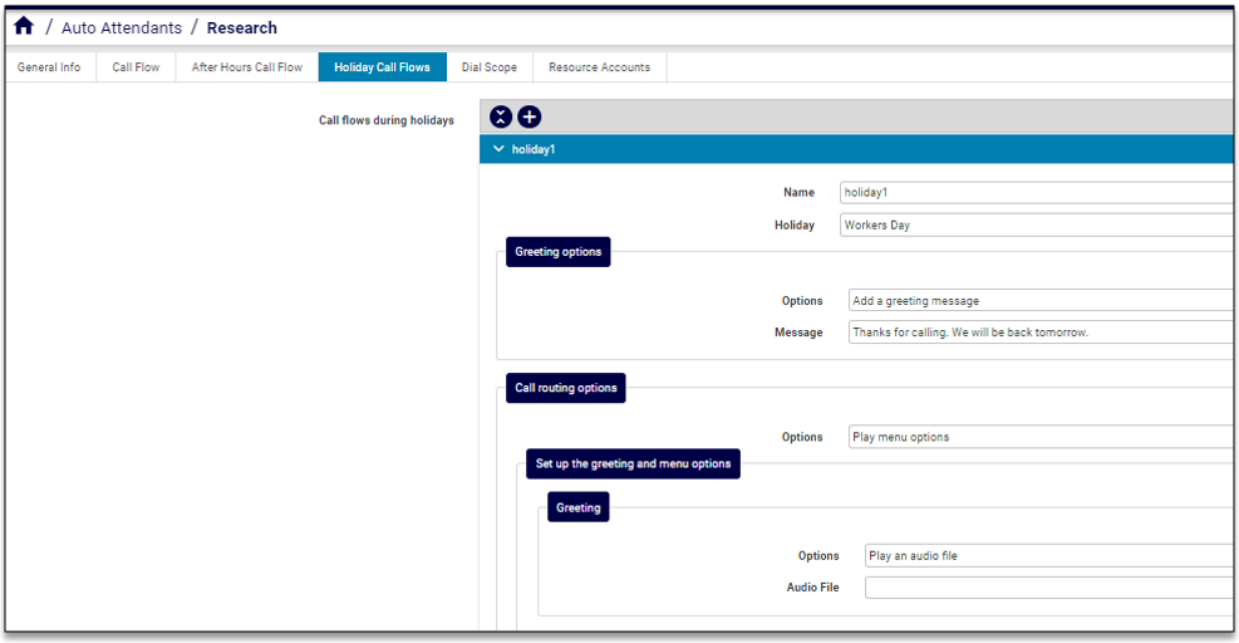
On the Holiday Call Flows tab/panel you can set up automated greetings and call routing options for days when your business is closed or operating at less than full capacity due to holidays in your region.

Note: If you're adding a greeting message, **Message** is a mandatory field. If you're playing an audio file, **Audio File** is a mandatory field.

Setting up holidays in your system allows you to automate how calls are answered when the business is closed or operating at less than full capacity. For example, you can choose to play a greeting or message on specific dates, and define how calls are routed. For example, the call may disconnect at the end of a message, or you can present menu options to redirect the call, for example, to voicemail, to an announcement, to a specific person in your organization, to a resource account, or to an external phone number.

Copyright © 2025 VisionOSS Limited. All rights reserved.

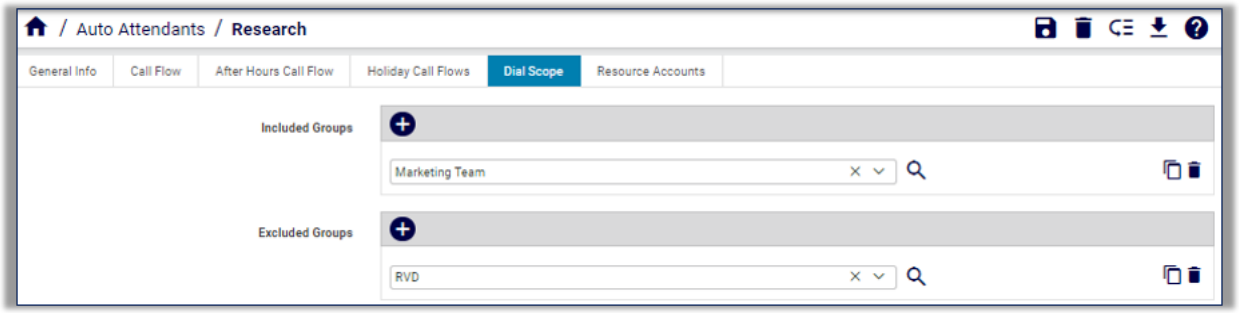
Important: If more than one call flow is added, a selected **Holiday** of each should *not* contain days that overlap with a Holiday selected in another call flow. Adding call flows with holidays containing overlapping days will result in a transaction error.



Dial Scope

Settings on the Dial Scope tab/panel configures dial scope for the auto attendant, allowing you to choose the Microsoft groups from Microsoft Entra ID (including Microsoft Exchange), to include or exclude from the dial scope.

Note: Microsoft changed the name of Azure Active Directory to Microsoft Entra ID in August 2023.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Resource Accounts

The Resource Accounts tab/panel adds and edits resource accounts for the auto attendant. When adding a resource account, you choose the resource account, and specify the resource account number.

In Automate, the application ID is the resource account type in the MS Teams online portal. There are two options for application ID/resource accounts:

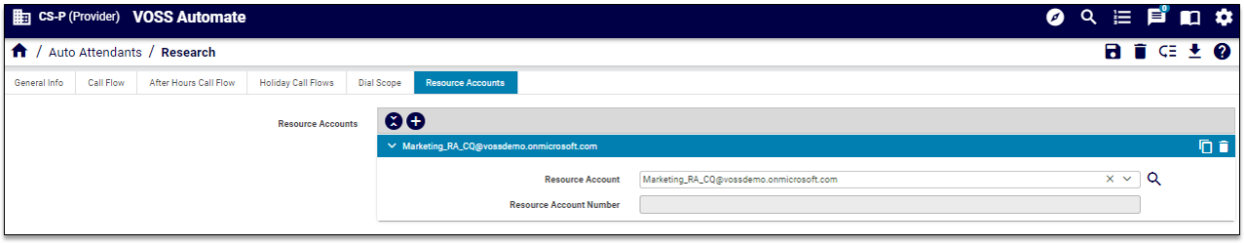
- Call queues
- Auto attendants

Note: MS Teams resource accounts are licensed, non-enabled user accounts, created to assign system resources to voice features such as call queues and auto attendants.

The **Resource Account** drop-down on this tab displays both licensed and unlicensed resource accounts. Choosing an unlicensed resource account triggers a warning and the transaction will fail in Automate. The resource account you choose must be Enterprise Voice enabled.

Each resource account has a display name, and is associated with a username, a phone number, and a device.

When resource accounts (resource users) are added to call queues and auto attendants, deleting a call queue or auto attendant triggers a system workflow that first disassociates any associated resource accounts, then deletes the call queue or auto attendant.



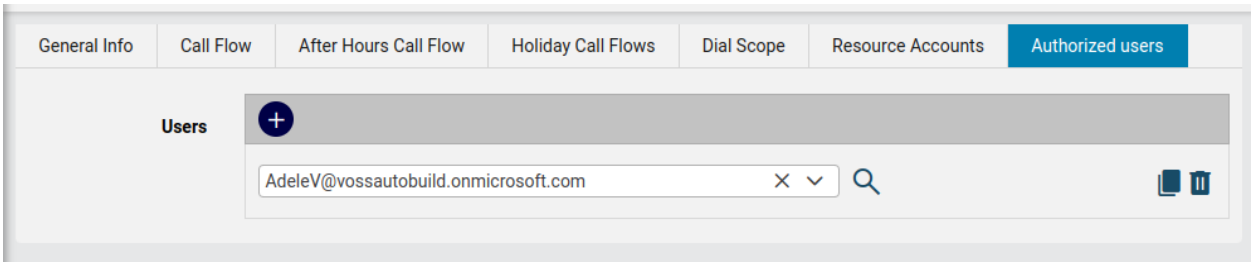
Authorized users

The Authorized users tab/panel adds and edits authorized users for the auto attendant. Authorized users are Teams users authorized by a Teams admin center administrator to make configuration changes to auto attendants and call queues. Authorized users don't need access to the Teams admin center portal or the assignment of any administrative roles. They can manage call queues and auto attendants settings using their Teams client or web portal, for example, Music on hold, voicemail greeting for call queues, or business hours greetings for auto attendants.

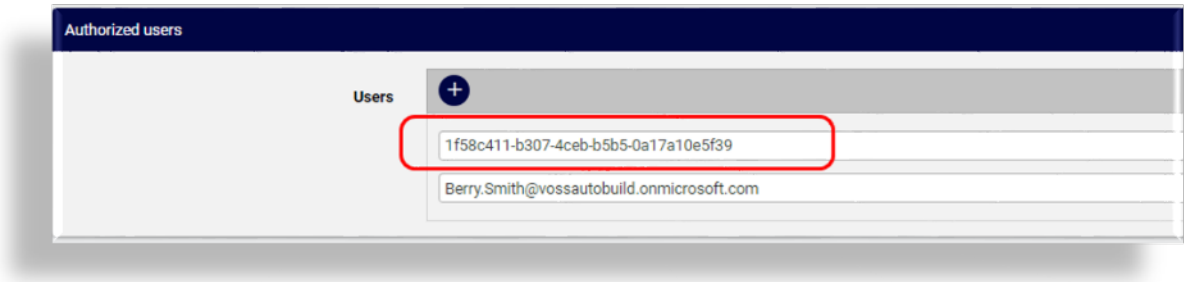
Users that can become authorized users must have a voice application policy assigned to them in Microsoft Teams. The drop-down of users available to be authorized users in Automate are for users with Enterprise Voice enabled.

When adding an authorized user, you choose the user from the drop-down list.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: If a user displays only with the PKID value, this occurs when the user has been deleted from the Microsoft portal (Microsoft Entra) but the user sync is not yet complete in Automate to remove the user from the cache.



9.1.2. Resource Accounts

Tip: *Use the Action search to navigate Automate*

Overview

MS Teams resource accounts are licensed, non-enabled user accounts that may be created to assign system resources to voice features such as call queues and auto attendants.

Changes you make to resource accounts in VOSS Automate are synced to the MS Teams portal. When adding or updating resource accounts in the MS Teams portal, these changes are also synced to VOSS Automate.

Note: From Automate 24.1, only Microsoft 365 Global Admins or User Admins will be able to create and manage resource accounts. The following roles will no longer have “user create” permissions on resource accounts:

- Teams Administrator
- Teams Communications Administrator
- Teams Telephony Administrator

Organizations using these Teams roles will require administrators with the “user create” permission, such as Microsoft 365 Global Admin or User Admin, in order to create and manage resource accounts.

Copyright © 2025 VisionOSS Limited. All rights reserved.

View, Modify, and Add Resource Accounts

This procedure displays, adds, and edits resource accounts from within the VOSS Automate Admin portal.

Note: Resource accounts can only be deleted using PowerShell. It is not possible to delete resource accounts from the VOSS Automate Admin portal or from the MS Teams cloud portal.

1. In the VOSS Automate Admin portal, go to **Resource Accounts** to open the **Resource Accounts** list view.
2. View details of existing resource accounts in the list view.

   Note: The list view displays resource accounts that have been added either in the MS Teams cloud portal or in VOSS Automate. Each resource account has a display name, and is associated with a username, and a device.

3. Choose an option:
   - To modify an existing resource account, click on a resource account in the list to open its the editing page. Update the resource account, and save your changes.

     Note: The following fields are editable: Application ID, Display Name

     Changes you make to resource accounts in VOSS Automate are synced to the MS Teams portal. When adding or updating resource accounts in the MS Teams portal, these changes are also synced to VOSS Automate.

   - To add a new resource account, click the Plus icon (+) to add a new record, then:
     - At **Application ID**, choose an option, either call queue or auto attendant.
     - At **Display Name**, fill out a user-friendly display name for the new resource account.
     - Mandatory. At **Username** fill out a username.
     - At **Domains**, choose a domain.

       Note: The value for **User Principal Name** (UPN) is auto-populated, and is a combination of the display name you specify, and the domain name you choose from the drop-down.

       Domain names are imported from Azure and are associated with your Microsoft tenant, which may have multiple domains.

       Once you save the resource account, the UPN is read-only.

4. Save your changes.

   Note: Adding a new resource account creates an Office 365 user in the MS Teams portal, which may be identified via their department name, *Microsoft Communications Application Instance*.

   Deleting this user account from Office 365 places the linked resource account in an *Inactive* state, although it remains associated with the auto attendant.

Copyright © 2025 VisionOSS Limited. All rights reserved.

When resource accounts (resource users) are added to call queues and auto attendants, deleting a call queue or auto attendant triggers a system workflow that first disassociates any associated resource accounts, then deletes the call queue or auto attendant.

Refresh your MS Teams portal account to view updates to resource accounts made from the VOSS Automate Admin portal.

9.1.3. Call Queues

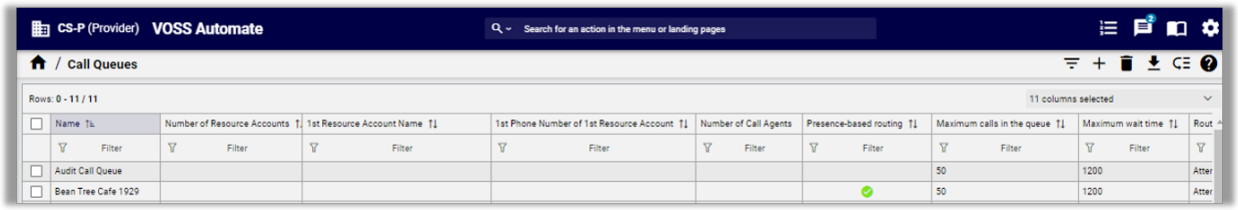
Tip: *Use the Action search to navigate Automate*

Overview

Microsoft Teams call queues allow you to manage incoming callers as they arrive in a call queue, and for the duration of their wait in the call queue, until they're connected to an agent. For example, you can set up a call queue to play a greeting message as a caller arrives in the queue, or play a music file while they're waiting to route to a call agent.

Note:

- If you're adding a greeting message, **Message** is a mandatory field.
- If you're playing an audio file, **Audio File** is a mandatory field.



Automate administrators may configure all call queue related configuration within the Automate Admin Portal without requiring additional configuration in the Microsoft Admin Portal.

You can set up a call queue to efficiently route callers out of the queue, to the first available agent, for example. If no agents are signed in or when all agents have opted out of the queue, you can also define, from within Automate or from the Microsoft Admin Portal, how new incoming calls are managed. In this case, you can choose to add new incoming calls to the queue, or disconnect, or redirect the call. Redirect options include redirect to a person in the organization, a voice app, a resource account, an external phone number, or a personal or shared voicemail.

Note: See the Microsoft documentation for more information around the recommended call queue configuration, including some options that you can set up in Automate (https://docs.microsoft.com/en-US/microsoftteams/create-a-phone-system-call-queue).

Microsoft's recommended settings for call queue are as follows:

- Enable *Conference mode* (Call answering tab in VOSS Automate)
- Set *Routing method* to *Round robin* or *Longest idle* (Agent selection tab in VOSS Automate)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Enable *Presence-based routing* (Agent selection tab in VOSS Automate)
- Set *Agent alert time* to a minimum of 20 seconds (Agent selection tab in VOSS Automate)

Changes you make to call queues from within VOSS Automate updates call queues in the Microsoft cloud portal, and changes made in the Microsoft cloud also syncs to the relevant call queues in VOSS Automate.

Supported audio file types for call queues

Call queues support the following audio file types: *.MP3*, *.WAV*, *.WMA*

The format of *.WAV* files require the correct resolution and rates. Microsoft specifies these requirements:

- Uncompressed, linear Pulse-code modulation (PCM-encoded)
- 8-bit, 16-bit, or 32-bit resolution
- Mono or stereo channel
- Sampling rate of 8 kHz or 16 kHz
- Maximum audio file size 5 MB

.MP3 files are supported with commonly accepted bit rates and encoding.

Ensure that your audio files have the correct specifications. You can use an app such as Audacity to create correctly formatted audio files.

Call queues updated in Automate will copy the audio files to the Microsoft Admin Portal using SCP. This can be seen in the transaction logs.

View and manage Microsoft Teams call queues

This procedure displays, edits, and deletes existing Microsoft Teams call queues, and adds new call queues, from within the Automate Admin Portal.

1. In the Automate Admin portal, go to **Call Queues** to display the **Call Queues** summary list view.
2. View existing call queues, which may have been added either from Automate or from the Microsoft Teams Admin Portal.

   Note: From the list view you can choose to update, delete, move, or export existing call queues, or add new call queues, and your changes will sync to the call queue details in the Microsoft Teams Admin Portal.

3. Choose an option:
   - **Update an existing call queue**:
     - Click on a call queue in the list view to open the **Call Queues** management page.
     - Click through the tabs on the page to update the configuration.
     - Save your changes. Updates are synced to the Microsoft Teams cloud portal.
   - **Add a new call queue**:
     - In the list view, click the toolbar Plus (+) icon.
     - Choose the customer or site hierarchy where you're adding a call queue.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- On the configuration page, click through the tabs to configure the call queue:
  - *General info*
  - *Greeting and music*
  - *Call answering*
  - *Agent selection*
  - *Call back*
  - *Call overflow handling*
  - *Call timeout handling*
  - *No agent handling*
  - *Authorized users*
- Save your changes.

A new call queue is added to the Microsoft Teams Admin Portal with the settings you configured. Any changes made to update an existing call queue are synced to the Microsoft Teams Admin Portal. Any changes you make to these settings on the Microsoft Teams Admin Portal sync to Automate to update the call queue in Automate.

Call queues settings

You can select the following tabs on the Call Queues configuration page (once you select a call queue in the summary list view):

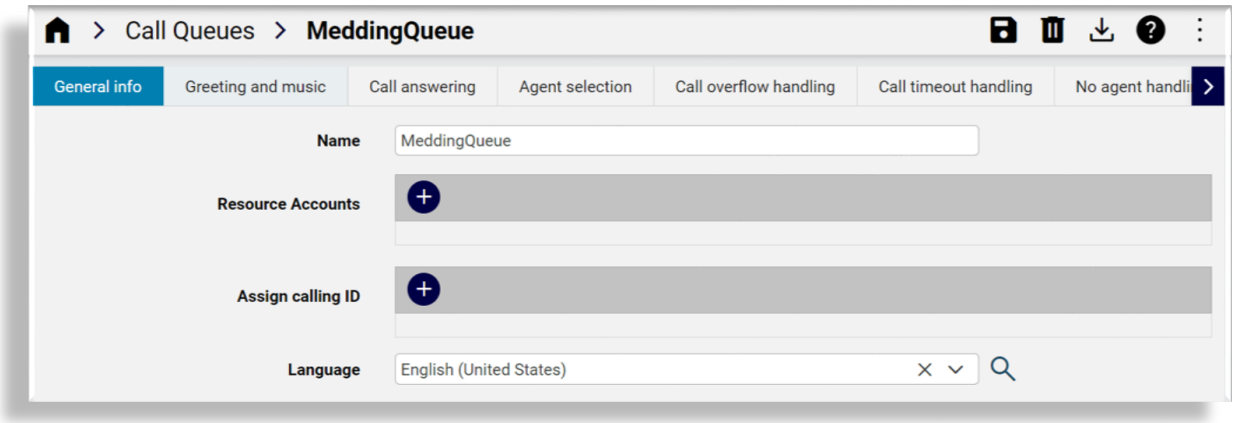
- *General info*
- *Greeting and music*
- *Call answering*
- *Agent selection*
- *Call back*
- *Call overflow handling*
- *Call timeout handling*
- *No agent handling*
- *Authorized users*

General info

This tab/panel configures the call queue name, adds resource accounts and calling IDs (optionally), and allows you to choose the language that will be used for transcribing voicemail messages and to play system prompts.

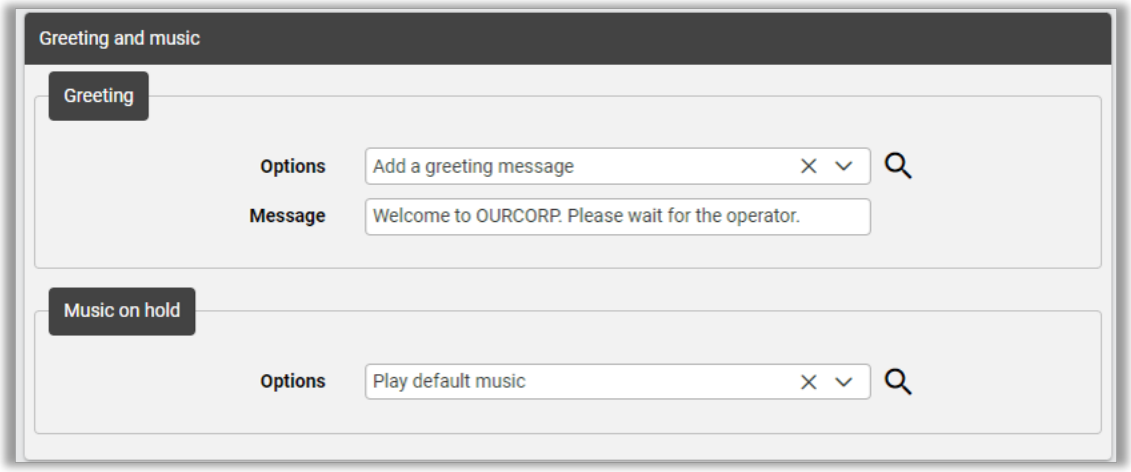
Note: When resource accounts (resource users) are added to call queues and auto attendants, deleting a call queue or auto attendant triggers a system workflow that first disassociates any associated resource accounts, then deletes the call queue or auto attendant.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Greeting and music

This tab/panel configures greeting and music on hold options.



The table describes configuration options on the tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Greeting > Options	Choose a greeting option, either of the following: • No greeting • Play an audio file Selecting this option displays the **Audio file** field, where you will need to (mandatory) choose the audio file to use. • Add a greeting message Selecting this option displays the **Message** field, where you will need to (mandatory) fill out the greeting message to use. The typed message will be converted to an audio message by MS text-to-speech.
Greeting > Music on hold	Choose an option for playing music while the caller is on hold. Options are: • Play default music • Play an audio file Selecting this option displays the **Audio file** field, where you will need to (mandatory) choose the audio file to use.

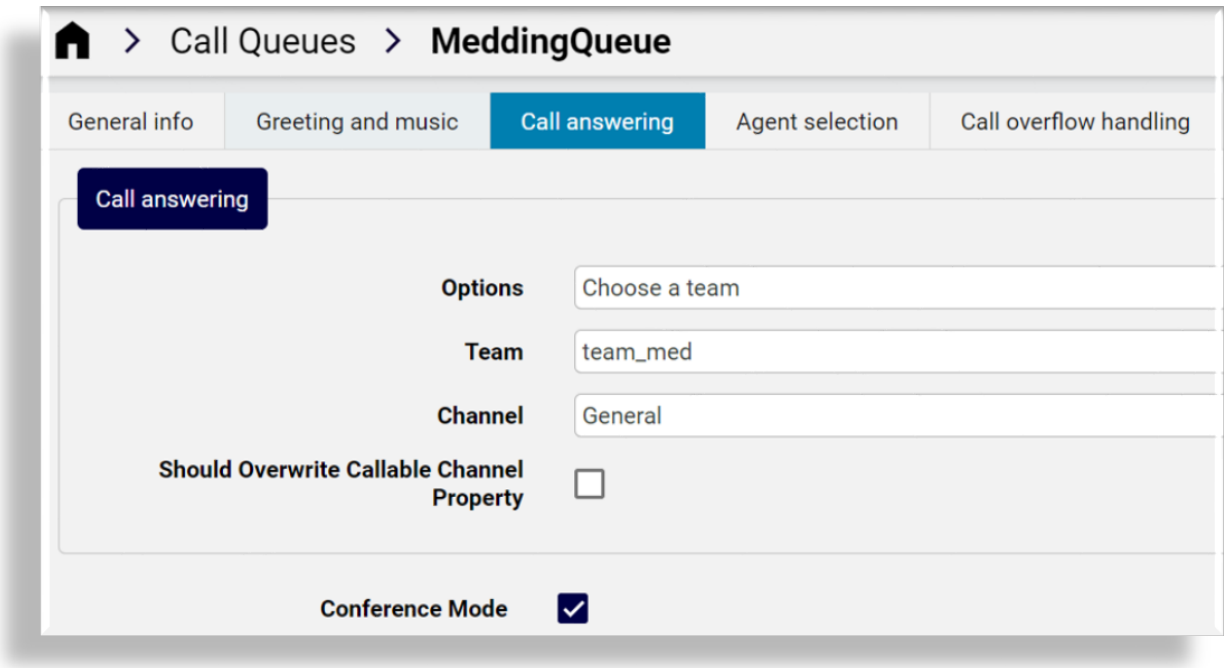
Note:

- VOSS Automate supports the following audio file formats for call queues: *.MP3*, *.WAV*, *.WMA*
- Microsoft Teams provides a default MOH file to play to callers while they're on hold in a queue. You can choose to play the default file, or choose a file you uploaded (custom files). Custom files are uploaded via File Management to the relevant sites in VOSS Automate.

Call answering

This tab/panel defines how incoming calls in the call queue are answered.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes configuration options on this tab/panel:

Field	Description
Options / Team / Channel	Defines whether to have a specific MS Team and channel answer calls in the queue or choose to assign specific call agents, distribution lists, and groups. The **Channels** drop-down displays only non-private channels. Assigning a MS team to call answering must be configured on the MS Teams portal and synced to VOSS Automate. The ability to set this up from within VOSS Automate is reserved for future development.
Should Overwrite Callable Channel Property	A Teams channel can only be linked to one call queue at a time. To force reassignment of the Teams channel to a new call queue, set this to value to True.
Conference Mode	Enables or disables conference mode. The recommended setting is *Enabled*. Enabling conference mode reduces the time it takes for the caller to connect with an agent. Conference mode enabled requires that the agent answering calls is using Microsoft Teams desktop client or a Microsoft phone.

Note: An edge case scenario exists where deleting a user or a group that is referenced by a call queue causes invalid data to display for the call queue. Typically, this is visible when opening the call queue in the Automate portal and the group or user ID is shown under call answer settings instead of a name.

This is due to MS Teams still including the deleted resource(s) in the call queue settings response that VOSS Automate retrieves. This case has the most impact if the group or user that was deleted is the only resource left in the call queue. The pkid of the resource (user or group) is seen instead of the proper name in the dropdown and if you save the call queue, it may error out as MS Teams will then yield an error for those

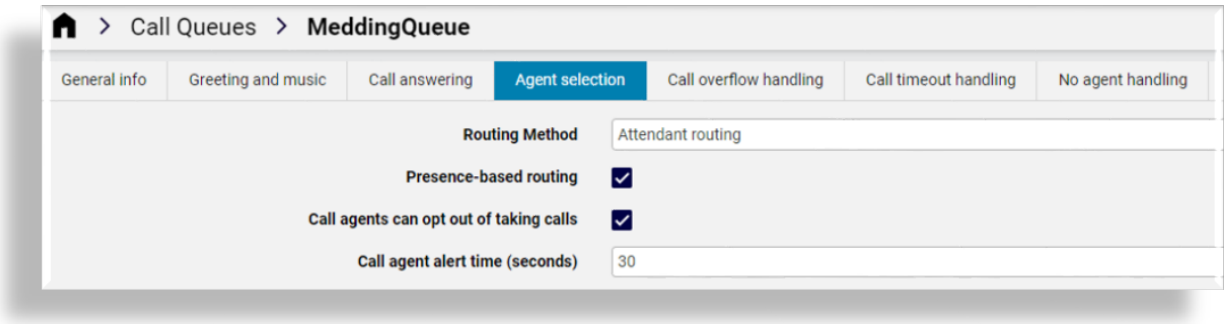
Copyright © 2025 VisionOSS Limited. All rights reserved.

resources being invalid.

As a workaround, you can remove the resource(s) that appear as pkids from the call queue before saving the call queue. This will ensure the call queue update that happens only includes valid data.

Agent selection

This tab/panel defines the agents available to answer calls, and how calls are distributed and routed to agents.



The table describes configuration options on the Agent selection tab/panel:

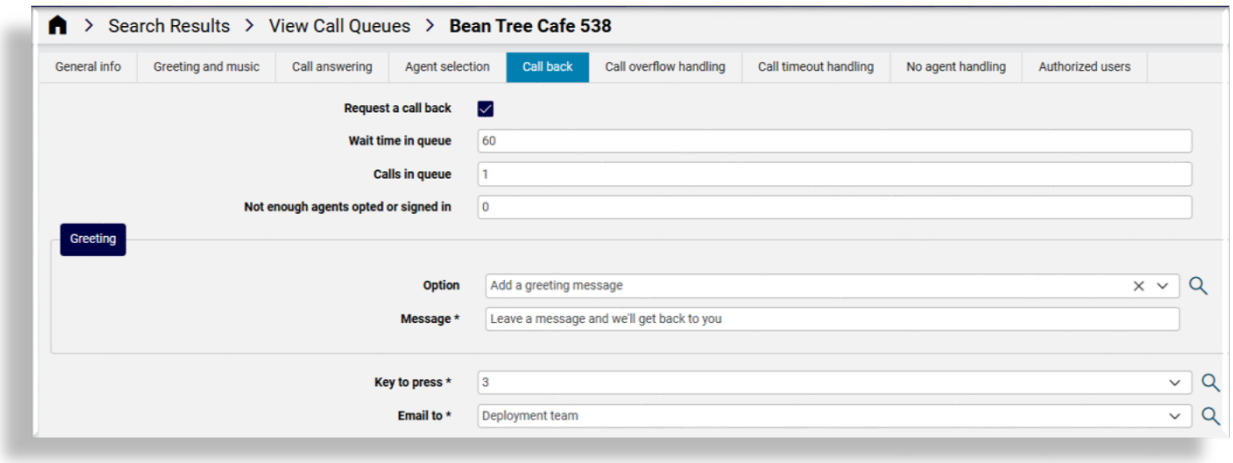
Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Routing method	Defines how calls are routed: Options are: • Attendant routing Rings all agents in the queue at the same time. The first agent to pick up the call takes the call. • Serial routing Rings call agents in the order they're listed in the call agents list. The call cycles through agents until one answers the call. • Round robin A recommended routing method, representing a balanced approach that sends the same number of calls from the queue to each agent. • Longest idle A recommended routing method that routes the next call to the agent who has been idle the longest. An agent is considered idle when their *presence* status is set to *Available*. Calls won't be routed to agents with their *presence* status set to *Unavailable*. You cannot enable *Presence-based routing* for this routing method.
Presence-based routing	Recommendation is *Enabled*. However, this setting can't be enabled for routing option *Longest idle*. Disable to send calls to agents who choose to receive calls, regardless of their presence status. Enable to send calls only to agents with their presence status set to *Available*.
Call agents can opt out of taking calls	Recommendation is *enabled*. Disable to ensure agents accept a call routed to them. Enable to allow agents to choose not to answer a call.
Call agent alert time	The time, in seconds, to wait before redirecting the call to the next agent. The recommendation is a minimum of 20 seconds. The minimum alert time is 15 seconds, and the maximum alert time is 180 seconds.

Call back

This tab/panel enables or disables courtesy call back functionality for call queues, and configures call back (when enabled).

Copyright © 2025 VisionOSS Limited. All rights reserved.



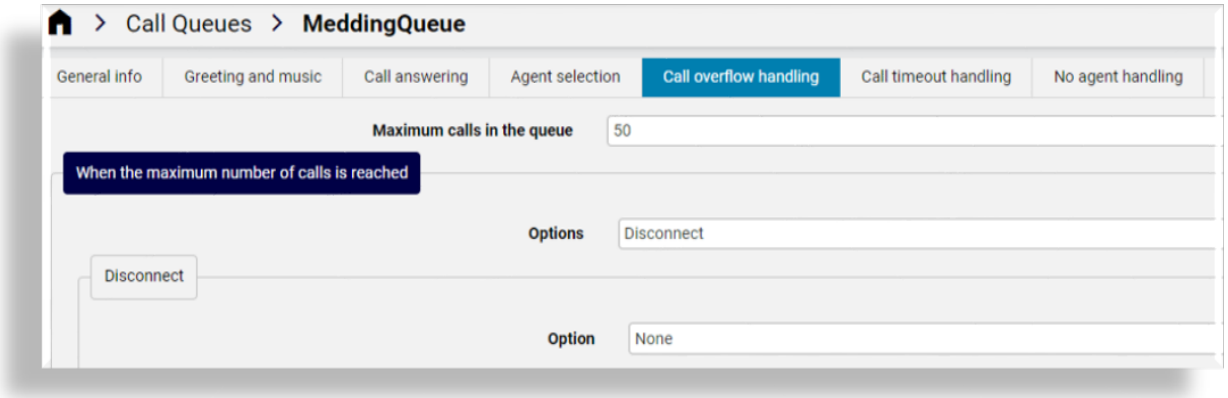
The table describes configuration options on the Call back tab/panel:

Field	Description
Request a call back	Defines whether call back functionality is enabled. Default is False. When set to True (checkbox selected), call back configuration options display and can be configured.
Wait time in queue	Defines the maximum period, in seconds, that the first call in the must wait before it is eligible for call back.
Calls in queue	The number of calls in queue before a call arriving at the queue becomes eligible for call back.
Not enough agents opted or signed in	The ratio of calls to agents that must be in queue before a call arriving at the queue becomes eligible for call back. Minimum value of one (1).
Option	Greeting option to use, either of the following: • Add a greeting message • Play an audio file
Message / Audio File	Mandatory. • A **Message** field displays when the greeting option selected is is **Add a greeting message**. You can fill out a greeting message to display. • An **Audio File** drop-down displays when the greeting option selected is **Play and audio file**. You can select an audio file already uploaded to Automate.
Key to press	Mandatory. The DTMF touch-tone key a caller will be told to press to select call back. Valid values are one (1) to nine (9), star (*), or pound (#).
Email to	Mandatory. The email address to send a notification to when call back cannot be completed.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call overflow handling

This tab/panel defines the maximum number of calls that may be in the queue, and how the system handles calls that exceed the maximum.



The table describes configuration options on the Call Overflow Handling tab/panel:

Field	Description
Maximum calls in the queue	Defines the maximum number of incoming calls you want to allow in the call queue. The default maximum number of incoming calls allowed in a call queue is 200 calls.
When the maximum number of calls is reached	This fieldset defines the system behavior once the number of incoming calls in the call queue reaches your defined maximum. Two options are available: • Disconnect Disconnects the call. In this case you can choose to disconnect and take no further action (None), or play an audio file (and select an audio file), or add a greeting message (and fill out a greeting message). • Redirect the call In this case, calls can be re-directed to another person, a voice app, a resource account, an external phone number, or to a shared or personal voicemail. For each redirect option you choose you can set up further configuration. For example, when redirecting to a shared voicemail, you'll choose the shared voicemail account, define whether to allow transcription, define whether to skip the voicemail system message, and configure a greeting with an audio file or greeting message.

Note:

- If you're adding a greeting message, **Message** is a mandatory field.
- If you're playing an audio file, **Audio File** is a mandatory field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Call timeout handling

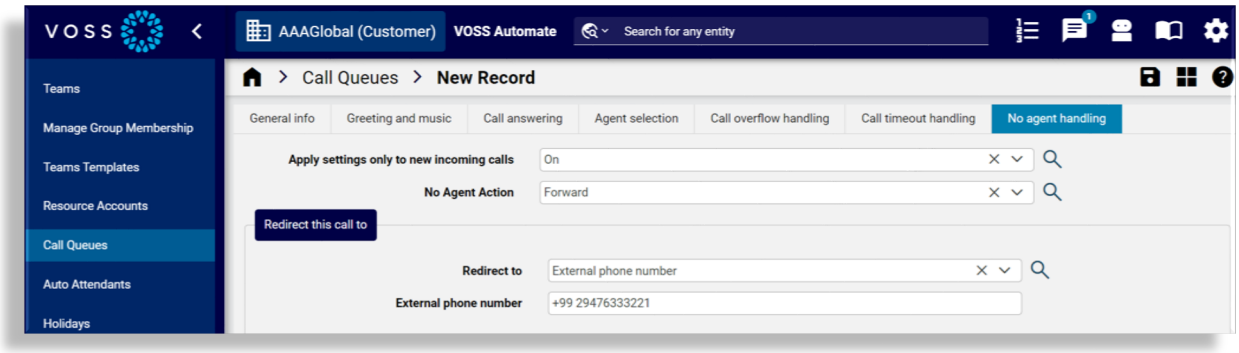
This tab/panel defines the maximum wait time (in seconds) that an incoming call can remain in the call queue. Once you've set up the maximum wait time, you can configure what happens to the call, that is, disconnect the call, or redirect it (and configure redirect options, such as redirect to a person in the organization, to a voice app, a resource account, an external phone number, or to shared or personal voicemail).

Note: The default maximum wait time is 2700 seconds (45 minutes). The call is dropped or redirected after the predefined wait time threshold is reached.

If you're adding a greeting message, **Message** is a mandatory field. If you're playing an audio file, **Audio File** is a mandatory field.

No agent handling

This tab/panel defines how to manage new incoming calls when no agents are signed in or when all agents have opted out of the queue.



The table describes configuration options on the tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Apply settings only to new incoming calls	Defines whether to apply the settings you're configuring to new calls coming in to the call queue. Either Yes or No. Default is No.
No Agent Action	Defines the action to take when no agents are signed in or opted in to handle new incoming calls. Options are: • Queue Call - The call is added to the call queue, with no further configuration options. • Disconnect - This option allows you to take no further action or to play an audio file (and choose an audio file) or to add a greeting message. • Forward - Allows you to redirect the call to: – Default. A person in the organization (and select the person) – A voice app (and select the voice app) – A resource account (and select the resource account) – An external phone number (and fill out the phone number) – A person in the organization (and select the person) – Voicemail (personal) (and select the voicemail) – Voicemail (shared) - in this case you select the shared voicemail, define whether to transcribe the message, define whether to skip the voicemail system message, and set up a greeting (add a greeting message or play an audio file) The following file formats are supported for audio files: MP3, WAV, and WMA. The maximum file size is 5 MB.

Note:

- If you're adding a greeting message, **Message** is a mandatory field.
- If you're playing an audio file, **Audio File** is a mandatory field.

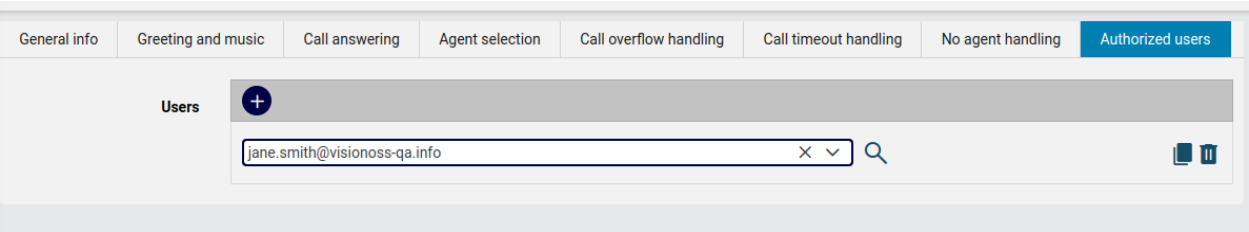
Authorized users

This tab adds and edits authorized users for the call queue. Authorized users are Teams users who have been authorized by a Teams admin center administrator to make configuration changes to Auto attendants and Call queues. This user does not require access to the Teams admin center portal or the assignment of any administrative roles. They can manage Call queues and Auto attendants settings using their Teams client or web portal, for example, Music on hold, Voicemail greeting for Call queues, or Business hours greetings for Auto attendants.

The users allowed to become authorized users must be have A Voice Application Policy assigned to them in MS Teams. However, this policy is not (currently) shown in VOSS Automate and therefore the dropdown of users available to be authorized users in Automate are for users with Enterprise Voice enabled.

When adding an authorized user, you choose the user from the drop-down list.

Copyright © 2025 VisionOSS Limited. All rights reserved.



9.2. Webex Call Groups

9.2.1. Automate - Call Groups - Webex Call Groups

Webex Call Group Settings

Counters

- Hunt Groups
- Call Pickup Groups
- Auto Attendants

Links

- **Call Group Settings**
  - View Hunt Groups
  - Add Hunt Group
  - View Call Pickup Groups
  - Add Call Pickup Group
  - View Webex Auto Attendant
  - Add Webex Auto Attendant
  - Webex Schedule

Charts

- **Pickup Groups by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Call Pickup
- **Auto Attendants by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Auto Attendants
- **Hunt Groups by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie

Copyright © 2025 VisionOSS Limited. All rights reserved.

– **Resource:** Webex Calling Hunt Group

9.3. Cisco Call Groups

9.3.1. Hunt groups

Tip: *Use the Action search to navigate Automate*

Overview

A hunt group is a combination a hunt pilot, hunt list, and line groups.

The table describes each of the elements of a hunt group:

Element	Description
Hunt Pilot	A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.
Hunt List	A hunt list displays a set of line groups in a specific order, and then associates with one or more hunt pilots, and determines the order in which those line groups are accessed. The order defines the progress of the search for available directory numbers for incoming calls. A hunt list comprises a collection of directory numbers as defined by line groups. A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.
Line Groups	Hunt groups provide a business context for the lines you choose as members of line groups. You will need to choose lines belonging to line groups, or any existing line groups that must be added to the hunt list members. A line group allows you to define the order in which directory numbers are chosen. CUCM distributes a call to idle or available members of a line group based on a call distribution algorithm and on the Ring No Answer (RNA) Reversion Timeout setting.

The hunt pilot, hunt list, and line group combination are automatically associated via unique identifiers for the following:

- The name of the hunt pilot and its hunt list is the same.
- The hunt list's line group members are set to the name of the associated line groups.

Searches can be performed on any of the details of the hunt pilot.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The site defaults auto-populates some values for hunt groups. To view or update the defaults, go to the **Defaults** page, choose a site to view its defaults, and locate the **Default CUCM Hunt Pilot Partition** field on the **General Defaults** tab. See *Site defaults*

Related topics

- *Add a hunt group*

Add a hunt group

This procedure adds a hunt group in Automate and Cisco Unified Communications Manager (CUCM).

Note: When adding a hunt group, you'll specify the parameters of the hunt pilot and the hunt list, and choose one or more new or existing line groups.

If your administrator has enabled number inventory, you can choose the hunt pilot pattern from a list of available numbers. If number inventory is disabled, you'll need to specify a hunt pilot pattern, or choose from a limited selection of available numbers.

To allow the successful use of call forwarding in a hunt pilot, clear the defaults for **Max Callers In Queue** (`32`) and the default for **Max Wait Time In Queue** (`900`). To use queuing instead of call forwarding, change the default values, for example, to 33 and 901.

To add a hunt group:

1. Log in as site administrator or higher.
2. Choose the hierarchy (if necessary) where you want to add the hunt group.

   Note: Hunt groups can be configured at the customer level or at site level.

3. Go to Cisco **Hunt Groups** to open the summary list of existing hunt groups.
4. On the **Hunt Groups** list view, click **Add**.
5. Customer level only. If you're adding the hunt group at the customer level, choose a network device list (NDL).

   Note:

   - Choose a NDL that identifies the CUCM where the hunt group is defined.
   - The system supports adding duplicate hunt groups (two hunt groups with the same hunt list name), provided multi-cluster CUCM is configured and you choose a different NDL. The second hunt group and hunt list are added to the second CUCM.

6. On the **Hunt Groups**/**New Record** page, fill out at least the required fields to configure the new hunt group.
7. Save your changes.

   Saving triggers a workflow to add the new hunt group. This workflow:

   - Adds a hunt list with the details you configured
   - Adds a hunt pilot with the details you configured

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Creates one or more line groups with the specified directory numbers as members

Related topics

- *Hunt group configuration*
- *Reserve numbers for a user*

Edit a hunt group

It is possible to edit hunt groups, for example, to add or delete line groups, or to add or delete line group members.

When modifying a hunt group, the following workflow is executed (depending on the changes you made):

- The line group details are modified.
- Any new line groups are added.

  A removed line group is deleted *only* if it is the last instance. If a shared line group is removed, it is deleted from the specified hunt group *only*, but is still included in other hunt groups that are also using it.

  If the hunt group uses existing line groups, the existing line groups are updated when the hunt group is modified.
- The hunt list is modified.
- The hunt pilot is modified.

Related Topics

- *Hunt group configuration*

Delete a hunt group

When deleting a hunt group, the following workflow is executed:

- The line groups that are members of the hunt list are deleted (if they are not used by any other hunt group in the system).

  If a shared line group is removed, it is deleted from the specified hunt group *only*, but is still included in other hunt groups that are also using it.
- The hunt pilot is deleted
- The hunt list is deleted

Copyright © 2025 VisionOSS Limited. All rights reserved.

Hunt group configuration

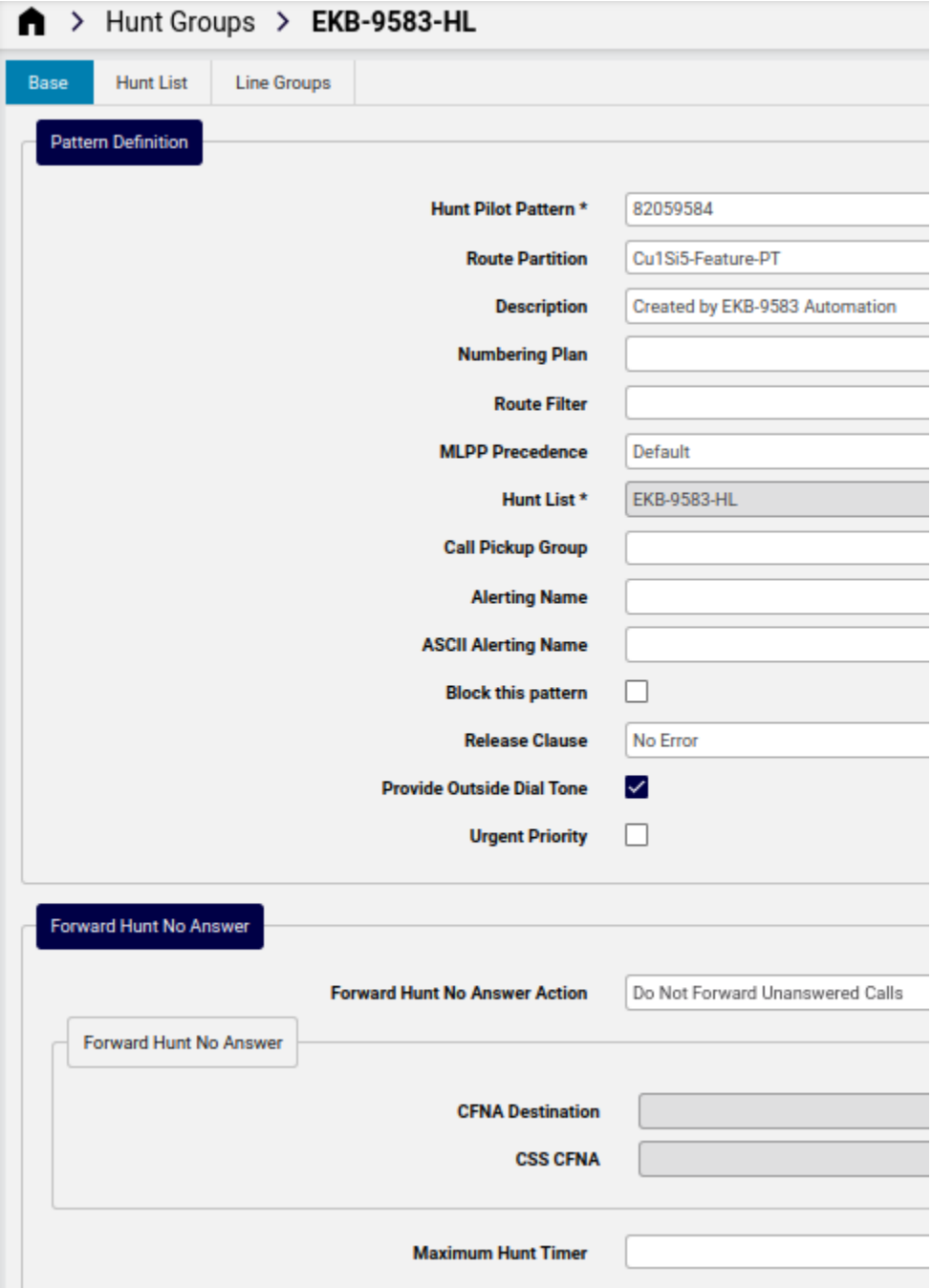
Details for hunt groups are added or updated on the **Hunt Groups**/**New Record [hunt group name]** page in Automate.

Note: You can toggle the layout on this page via a toolbar button that allows you to view the page content as either tabs or panels.

Content is added or updated in the following tabs/panels:

- **Base**
  - *Pattern Definition*
  - *Forward Hunt Busy*
  - *Forward Hunt No Answer*
  - *Queueing*
  - Park Monitoring
  - Calling Party Transformations
  - Connected Party Transformations
  - Called Party Transformations
  - AAR Group Settings
- *Hunt List*
- *Line groups*

Copyright © 2025 VisionOSS Limited. All rights reserved.



Pattern Definition

For hunt groups configured at the customer level, the **Pattern Definition** tab/panel defines a unique hunt pilot pattern.

The hunt pilot pattern is added to the customer-level DN inventory and is marked as in-use and unavailable.

The table describes the fields on the **Pattern Definition** tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Hunt Pilot Pattern	Mandatory. A hunt pilot pattern can include numbers and wildcards (no spaces). For example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. Valid characters include uppercase characters A, B, C, D, and + (representing the international escape character +). Ensure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique.
Route Partition	Choose a route partition from the list if you want to use a partition to restrict access to the hunt pilot, else, leave the field blank.
Route Filter	If your hunt pilot includes the '@' wildcard, choose a route filter from the drop-down. Route filters restrict some number patterns. The numbering plan you choose determines the route filters you can choose from.
Hunt List	Add the hunt list name to the **Name** field in the **Hunt List** section to auto-populate this field.
Call Pickup Group	The call pickup group to associate with this hunt group. Choose a call pickup group at the same hierarchy as this hunt group or if no call pickup groups are available at this hierarchy, choose a call pickup group at the hierarchy directly above. Call pickup group is the number that can be dialed to answer calls to this directory number (in the partition)
Alerting Name	Specify an alerting name for the hunt pilot in UNICODE format. This name is displayed on phones that the hunt pilot dials when it receives an incoming call, along with calling party information. Phone users can use this information to answer the call This name also displays on the calling phone. If you don't enter a name, the hunt pilot DN displays on the phones.
Provide Outside Dial Tone	Enable for each hunt pilot that routes the call off the local network and provides outside dial tone to the calling device. Disable if you want to route the call in the network.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Forward Hunt Busy

The table describes the hunt group configuration options on the **Forward Hunt Busy** tab/panel:

Field	Description
Forward Hunt Busy Action	The hunt call treatment action. Options: • Do Not Forward Busy Calls • Use Forward Settings of Device that Forwarded to Hunt Pilot Uses the call forwarding settings of the line group member. • Forward Busy Calls to Destination
CFB Destination	The directory number where calls are to be forwarded. Enabled only when the selected *Forward Hunt Busy Action* is *Forward Busy Calls to Destination*.
CSS CFB	The line CSS, which applies to all devices using this directory number. The default is the default line CSS of the site. Enabled only when the selected *Forward Hunt Busy Action* is *Forward Busy Calls to Destination*.

Forward Hunt No Answer

The table describes the hunt group configuration options on the **Forward Hunt No Answer** tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Forward Hunt No Answer Action	Options for hunt call treatment: • Do Not Forward Unanswered Calls • Use Forward Settings of Device that Forwarded to Hunt Pilot Choose this option to use the call forwarding settings of the line group member. • Forward Unanswered Calls to Destination
CFNA Destination	The directory number where calls are to be forwarded. Enabled only when the selected *Forward Hunt No Answer Action* is *Forward Unanswered Calls to Destination*.
CSS CFNA	The line CSS, which applies to all devices using this directory number. The default is the default line CSS of the site. Enabled only when the selected *Forward Hunt No Answer Action* is *Forward Unanswered Calls to Destination*.
Maximum Hunt Timer	The maximum time for hunting without queueing. Do not use the same value for this field and for the **RNA Reversion Timeout** field in the associated line group.

Queueing

The Queueing tab/panel defines whether to queue calls.

Note: *Forward Hunt No Answer* settings and *Forward Hunt Busy* settings define how calls are moved through the route list. On the other hand, *Queuing* settings are used to hold callers in a route list. Thus:

- If queuing is enabled, both *Forward Hunt No Answer* and *Forward Hunt Busy* are automatically disabled.
- If *Forward Hunt No Answer* or *Forward Hunt Busy* are enabled, queuing is automatically disabled.

The table describes the hunt group configuration options on the **Queueing** tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Queue Calls	Select this checkbox to enable call queueing for hunt groups. Enabling call queueing disables *Forward Hunt Groups*, and enables additional queueing configuration fields on the tab/panel.
Network Hold MOH Source & Announcements	The Music On Hold (MoH) source that will be used to play announcements and to provide queue hold treatments. If nothing is selected (default), the default Network Hold MoH/MoH Source and Announcements configured on service parameter is used. The MoH source can be configured as unicast or multicast. Caller side's MRGL takes precedence for multicast or unicast. The MoH source announcement locale is used to determine the language used for the announcement. Only one type of language announcement can be played per hunt pilot. When any of the MoH settings are changed, the existing callers in queue are not affected. All future queued callers will listen to MoH and announcements as per the updated settings.
Maximum Number of Callers Allowed in Queue	Auto-populated with default value, 32. Range value is from 1 to 100. When the maximum number of callers in the queue is reached, and if subsequent calls need to be disconnected, select "Disconnect the call". When the maximum number of callers in the queue is reached, and if subsequent calls need to be routed to a secondary destination, select the "Route the call to this destination" radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the "Full Queue Calling Search Space" from the drop-down (optional).
Maximum Wait Time in Queue	Auto-populated with default value,``900``.
Queue Full Destination	Where to route calls when the maximum number of callers in the queue is reached. If you don't configure this secondary destination then calls are disconnected if the queue is full.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Hunt List

Field	Description
Name	Maximum of 50 alphanumeric characters, and can contain combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each hunt list name is unique to the route plan. it is recommended that you use short, descriptive names for your hunt lists. The CompanynameLocationCalltype format provides enough detail and is short enough so you can easily identify a hunt list.
Cisco Unified Communications Manager Group	Choose a CUCM group from the list. The hunt list registers to the first node in the CUCM group. Choosing a CUCM with only one node configured triggers a system warning, so choose a group with more than one node.
Enable this Hunt List	Defines whether to enable your hunt list as soon as you save. No system reset is required.
For Voice Mail Usage	Define whether to use this hunt list for voicemail. Enabling this setting allows the route list control process to keep a count of the setups that are being served to the hunt list, and will not allow more setups than the number of available devices. As a result, each device in the hunt list is treated as if it has a Busy Trigger and related Maximum Number of Calls of one.

Line groups

It is recommended that you configure at least one line group member (directory number) for every line group you add. Before configuring the line group, you will need to add one or more directory numbers.

Note: Although it is possible to configure an empty line group (no members), CUCM does not support empty line groups for routing calls. If the line group has no members the hunt list stops hunting when the call is routed to the empty line group.

Note: For hunt groups configured at the customer-level, include lines defined at the customer level, and at any site within the customer.

The **Line Groups** tab/panel displays the line groups configured for the hunt group, with the following detail available for each line group:

- Line Group Name
- RNA Reversion Timeout
- Distribution Algorithm
- Automatically Logout Hunt Member on No Answer

Copyright © 2025 VisionOSS Limited. All rights reserved.

The Line Group Configuration dialog allows you to add details for a new line group or to update an existing line group. Click on a line group in the table, or click the Plus (+) icon to open the Line Group configuration dialog to add the new record.

The table describes the line group configuration options:

Field	Description
Line Group Name	The drop-down displays all line groups available at the site. You can choose a line group from the list or enter a name for the line group in the field. Names you add can be up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan. It is recommended that you use a short, descriptive name for your line groups. The CompanynameLocationGroup format usually provides a sufficient level of detail, and is short enough to be easily identified.
RNA Reversion Timeout	Specify a time, in seconds, after which CUCM will distribute a call to the next available or idle member of this line group or to the next line group if the call is not answered, and if the following option is chosen for Hunt Options No Answer: *Try next number; then try next group in Hunt List* The RNA Reversion Timeout applies at the line-group level to all members.
Distribution Algorithm	Applies at line group level, either top-down, circular, longest time, or broadcast.
Hunt Options No Answer	Choose a hunt option for CUCM to use if a call is distributed to a member of a line group that does not answer. This option is applied at the member level.
Automatically Logout Hunt Member on No Answer	Defines whether line members are automatically logged off the hunt list. Line members can log back in using the “HLOG” softkey or PLK.
Hunt Options Busy	Choose a hunt option for CUCM to use if a call is distributed to a member of a line group that is busy.
Hunt Options Not Available	Choose a hunt option for CUCM to use if a call is distributed to an unavailable line group member. The *Not Available* condition occurs when none of the phones that are associated with the DN in question is registered. Not Available also occurs when extension mobility is in use and the DN/user is not logged in.
Member	Line group members. For each member, choose a directory number, a partition, and specify a position.

Copyright © 2025 VisionOSS Limited. All rights reserved.

9.3.2. Call Pickup Groups

Tip: *Use the Action search to navigate Automate*

Overview

Certain default values for call pickup groups are populated via a site's **Site Defaults**, which you can view and edit (depending on your log in level).

Automate's *call pickup group* functionality provides the following:

- A single interface for adding call pickup groups, and for choosing one or more lines as members of a pickup group.
- Add CUCM call pickup groups and modify the call forward and call pickup settings of each CUCM directory number for membership to a newly added call pickup group.

  When adding a call pickup group, if your administrator has enabled the number inventory functionality, the pattern can be selected from a drop-down list of available numbers.

  If the feature is disabled, the **Pattern** field is a free text field or a drop-down containing only selected available numbers.
- Add lines to an existing call pickup group by selecting the pattern (directory number).

  When adding a member line, if your administrator has enabled the number inventory functionality, the pattern can be selected from a drop-down list of available numbers.

  If number inventory functionality is disabled, the **Pattern** field is a free text field or a drop-down containing only selected available numbers.

  The **Route Partition Name** field is populated automatically based on the selected pattern.
- Delete existing call pickup groups, and delete one or more lines from an existing call pickup group.

The first member of the associated pickup group name is set the newly created pickup group, and associated pickup groups can be added as part of the workflow.

Related topics

- *Reserve numbers for a user*

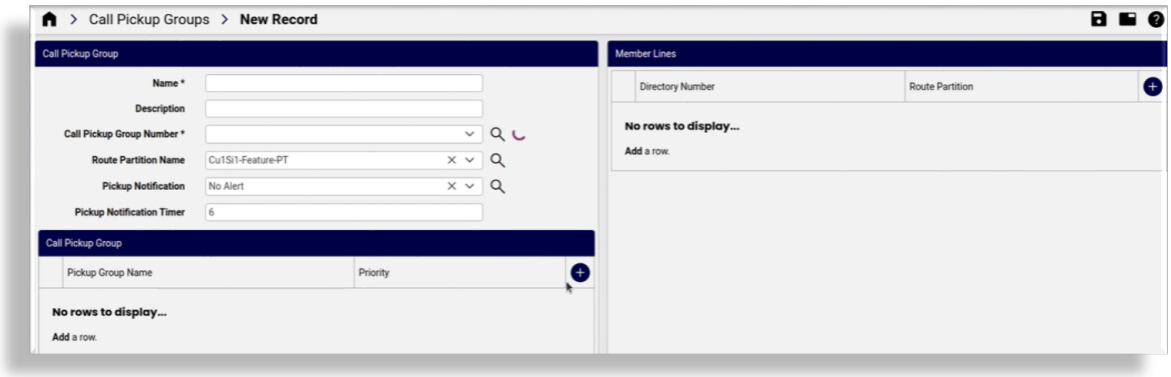
Add a call pickup group

This procedure adds a call pickup group in Automate.

1. Log in as Provider, Reseller, Customer, or Site administrator.
2. Set the hierarchy to the Customer or Site level.
3. If you've set the hierarchy level to Customer, choose the Network Device List. This step is not required if your hierarchy level is set to Site.
4. Go to **Add Call Pickup Group**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. Click the Plus icon (+) to open a new record.



6. On the **Call Pickup Group Details** tab/panel, configure the following:
   - Fill out a name (mandatory) and a description.
   - Mandatory. At **Call Pickup Group Number**, choose the pickup group pilot number.
   - At **Route Partition Name**, choose the required route partition.
   - At **Pickup Notification**, choose the method, one of the following:
     - No Alert
     - Audio Alert
     - Visual Alert
     - Audio and Visual Alert
   - At **Pickup Notification Timer**, enter the required period, as a number of seconds.
   - If the call pickup group is associated with other pickup groups, click the Plus icon (+) at **Call Pickup Groups** to add an entry. Choose a pickup group name, and set a priority.

     Note: This allows users to pick up incoming calls in a group that is associated with their own group. Note that the first member is automatically added, so there is no need to specify the first member as itself in an Add request.

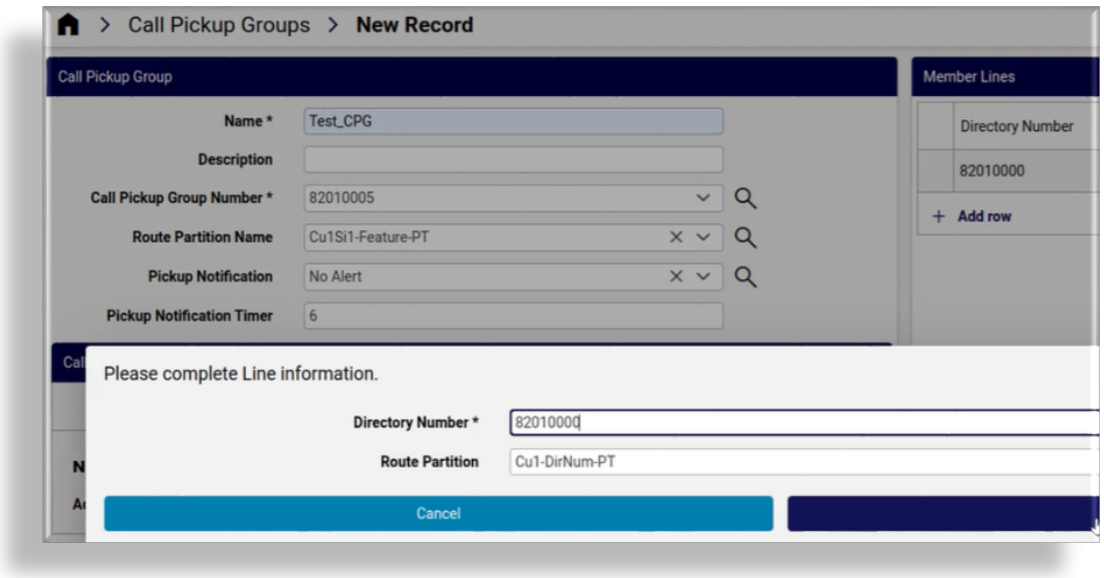
     For included pickup group names, ensure that the priority always starts at 1. When more than one included group exists, the group with Priority 1 has the highest the priority of answering calls for the associated group. Integer values are added in order of priority.

     The associated Directory Name and Partition is automatically selected, based on the Call Pickup Group Name. Set any required Pickup Notification settings.

7. On the **Membership** tab/panel, add lines, one or more:
   - Click the Plus icon (+) at **Directory Number** to open a dialog where you can select a directory number.
   - Select a directory number, then click **OK**.

     Note: The **Route Partition** field in this dialog is auto-populated when you select a directory number. You can select a different route partition, if required. Call pickup group members will only be successfully added if their directory number/s exist in a valid route partition. Directory numbers in a 'null' route partition appear as selectable members, but saving them results in an error.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- To add another line, click the Plus icon (+) again, choose another line, and click **OK**.

  Repeat this step to add more lines to the call pickup group, if required.

8. Click **Save** to add the call pickup group.

Note: If you're using partitions with the call pickup numbers, ensure that the directory numbers that are assigned to the call pickup group have a calling search space (CSS) that includes the appropriate partitions. The recommendation is to use `CU{macro}-PreISR-PT` partition for the call pickup groups added at the customer hierarchy.

The selected Call Pickup Groups drop-down lists the call pickup groups created at the customer level and the site level. Select the required call pickup group from both the customer and the site level.

Adding a call pickup group at customer level with members across child sites, succeeds without error, and the configuration is pushed to the associated Unified CM (CUCM). However, when viewing the call pickup group configuration after it was added, the added members will not be seen. Added members are only seen if the call pickup group and its members are at the same hierarchy level

To verify the individual member line association with the call pickup groups, you can go to the **Lines** page. The call pickup group under **Lines** displays the associated call pickup group

Edit or delete a call pickup group

This procedure updates or deletes a call pickup group in Automate.

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy to the Customer or Site level.
3. Go to **View Call Pickup Groups**. Choose an option:
   - To edit a call pickup group, click on the call pickup group in the list to open it's settings, make your changes, and save.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To delete a call pickup group, select the checkbox adjacent to the call pickup group in the list, then click the toolbar **Delete** icon.

Copyright © 2025 VisionOSS Limited. All rights reserved.

10. Security Management

10.1. Microsoft Defender setup, sync and overbuild

Microsoft

Automate provides a consolidated view and management of the Microsoft Defender suite, including the partitioning of and role-based access to MS tenant data.

To enable and use MS Defender in Automate, the following steps and activities are available:

10.1.1. Setup

1. Enable MS Defender for Office and/or Endpoint in the Global Settings.

   See Global Settings in the Core Feature Guide

   This will also by default enable a new **Microsoft Defender** administrator menu item containing links to related dashboards - to easily manage the enabled items. For details, see the *MS Defender management* topic below.

2. Configure a Microsoft tenant in Automate.

   This configuration will sync MS Defender data to Automate. Refer to the collection and and sync details below.

   See Microsoft tenant setup in the Core Feature Guide

10.1.2. Data collection and sync

When a tenant configuration for MS Defender is saved, Automate will:

- Create a data collection instance in Automate that is then synced from the tenant.

  For the data collection, if a MS Defender for Endpoint instance is added to the model called `data/DataCollection`, its name is of the format: **Defender for Endpoint Data Collection <hierarchy name>** and collects all instances from the tenant for the following models in a batch:

  - `device/msgraphsecurity/SecureScore`
  - `device/msgraphsecurity/Alert`
  - `device/msgraphsecurity/Incident`

  - `device/mssecurity/Machine`
  - `device/mssecurity/MachineAction`
  - `device/mssecurity/ExposureScoreByMachineGroups`

- Sync MS Defender collection data to Automate and create sync schedules.

  MS Defender data is synced to the tenant hierarchy.

  For the schedules, these are created (according to Global Settings enabled MS Defender suite items) and by default run every 30 minutes. The schedules can sync data according to the relevant created collection and a batch sync of data takes place.

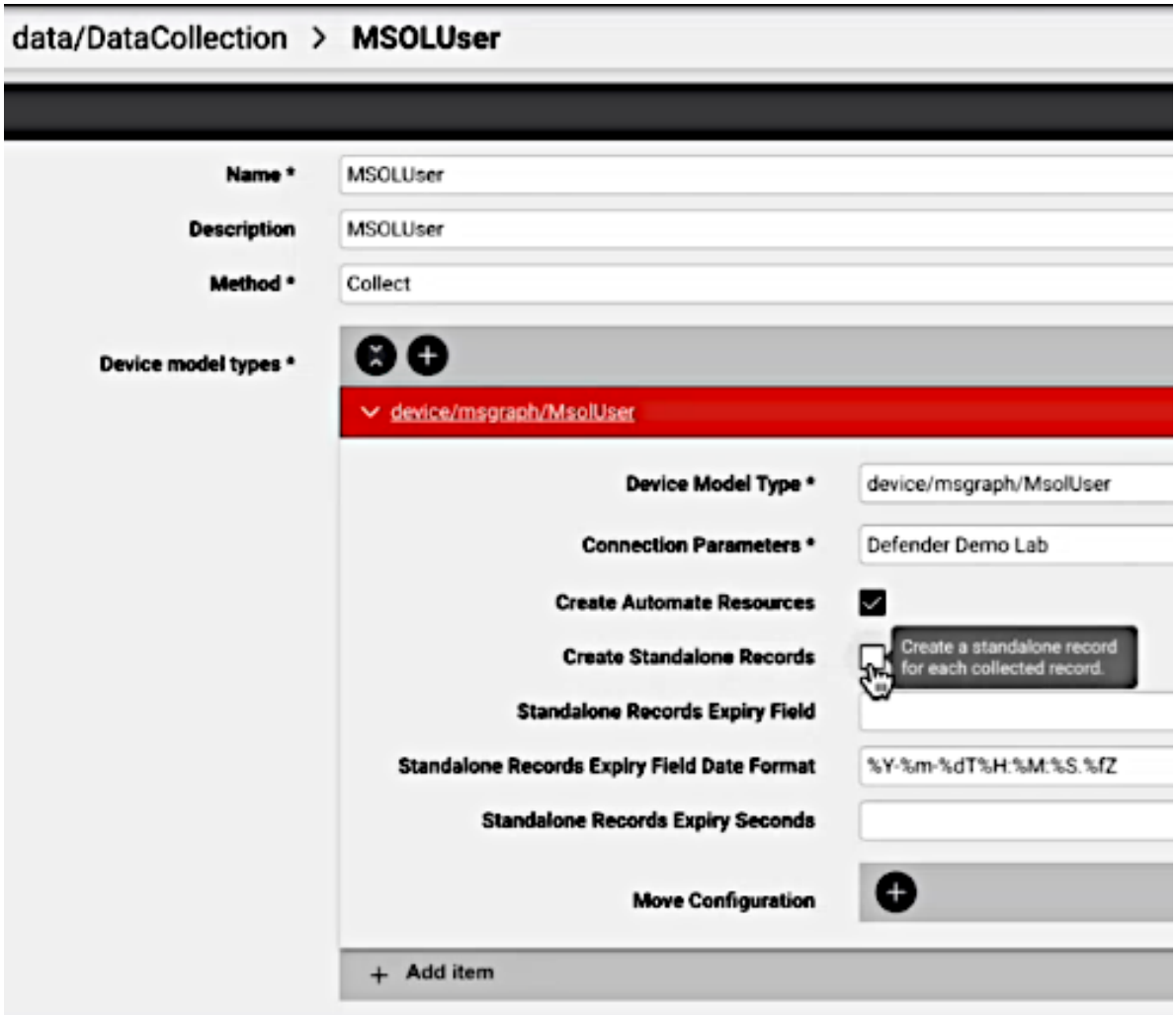
  For the schedule instance, the **Resource Type** of the created schedule is `data/DataCollection`, while the selected **Resource** naming format is:

  - **Defender for Endpoint Data Collection <hierarchy name>**
  - **Defender for Office Data Collection <hierarchy name>**

  The collected data at the tenant hierarchy is then also available when Overbuild for Microsoft is run to partition and move the data to the relevant sites in Automate.

Note: The default **MSOLUser** data collection does not apply the setting: **Create Standalone Records**, since this collection is used only for the Insights database in order to provide time series data for trends and charting.

Copyright © 2025 VisionOSS Limited. All rights reserved.



See Overbuild for Microsoft in the Core Feature Guide

10.1.3. Overbuild

Automate's Overbuild for Microsoft allows for the partitioning of the synced MS Defender data to relevant sites in Automate.

In particular, this includes: incident alerts, quarantine messages and MS Defender policies. The data partitioning is done according to the **Model Filter Criteria** (MFC) created during tenant setup.

For details on Microsoft Defender for Office and Endpoint overbuild, see: *Overbuild with Microsoft Defender - by Model Filter Criteria*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

10.1.4. MS Defender management

MS Defender data is the can be viewed and accessed in Automate from dashboards, allowing for further analysis as well as management from policy, incident and alert management interfaces.

See:

- *Microsoft Defender for Office security management and policies*
- *Microsoft Defender for Endpoint security management and policies*

10.2. Microsoft Defender for Office security management and policies

Microsoft

10.2.1. Overview

Automate provides support for Microsoft Defender for Office that addresses email security threats.

In particular, Automate supports:

- the rapid data sync of a large volume of quarantine messages
- hierarchy-specific data management
- the management of email quarantine messages, Safe Attachment Policies, Safe Link Policies
- *request staging areas* for quarantine email messages and for requests to create and update of policies

  Requests can then have the **State** that can be managed during the request cycle:
  - **PENDING**
  - **REJECTED**
  - **APPROVED**
  - **COMPLETED**
- the management of policy configuration templates, allowing for customization

---

Note:

- The following entry under **Global settings**, **Enabled Services** needs to be enabled: **Enable Defender for Office** - see: *Global settings*.
- For further setup and configuration, see: *Microsoft Defender setup, sync and overbuild*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

10.2.2. Dashboards

The administrator interface provides dashboards for the view and management of data:

Security Management - Defender for Office Overview Security Management - Defender for Office Actions

- By default:
  - The **Defender for Office Overview** dashboard provides the administrator with counters, charts and tables showing information on quarantine messages that are visible from the administrator's hierarchy, for example the total number of messages and breakdowns by site, time and type, including message senders, recipients and release requests.
  - The **Defender for Office Actions** dashboard also provides the administrator with counters on quarantined and released emails, as well as safelink and attachment policies. In addition, quick links are provided to manage quarantined emails, safe link policies and safe attachment policies.

To customize your dashboards:

- See: *Introduction to Automate dashboards*.
- Resources have been added and are available to widgets on a dashboard where **Data Source** is **Automate Analyzed**.

  For example:

  - Quarantine Messages, Shows diagnostic information about the Microsoft Quarantined messages, `device/msexchangeonline/QuarantineMessage`
  - Quarantine Message Staging, Shows diagnostic information about the Microsoft Quarantined Staging messages, `data/MicrosoftDefenderQuarantineMessageStaging`

10.2.3. Quarantine Email Actions

When synchronizing and overbuild on existing items that are in quarantine, these are moved to the relevant hierarchy node associated with the user.

Automate will sync a high volume quarantine messages using the data collection capability. The `data/DataModel` called: "DataCollection" provides this lightweight collection of data from external sources.

Administrators can carry out a number or list and request actions:

- View Quarantined Emails and Request Release
- View Released Emails
- View Release Requests

View Quarantined Emails and Request Release

A list view of quarantined email messages visible from the current hierarchy can be inspected and instances can be selected to request the message release.

Automate provides a *staging area* for requests (maintained in the data model: `data/MicrosoftDefenderQuarantineMessageStaging`).

Copyright © 2025 VisionOSS Limited. All rights reserved.

View Quarantined Emails and Request Release

Rows: 0 - 200 / Get Total

13 columns selected

First Recipient Address	Sender Address	Subject	Release Status	Received Time	Policy Name
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:04:57	QuarantineWh
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:04:59	QuarantineWh
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:04:51	QuarantineWh
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:04:49	QuarantineWh
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:04:34	QuarantineWh
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:04:47	QuarantineWh
aanderson@demo.vosslab.net	enter@olutions.com	Payment Details	NOTRELEASED	2025-08-25 17:05:04	QuarantineWh

An instance from this list can be selected, inspected and managed:

View Quarantined Emails and Request Release > aanderson@demo.vosslab.net

Microsoft Defender Quarantine Message Staging

Quarantine Message Release Request

Justification: Please supply a justification for the release of Quarantine Message...

Identity: 37ecbf3b-9778-4508-fcc5-08dde3e8c162\1c2c88ed-5199-5a63-3ba0-a1e392952227

First Recipient Address: aanderson@demo.vosslab.net

Message Id: <c5edf0fb45851f06913b44e944e08fce@voss-solutions.com>

Policy Name: QuarantineWhenSubjectContainsSpam

Policy Type: ExchangeTransportRule

Quarantine Types: TransportRule

Received Time: 2025-08-25 17:04:57

Recipient Address: aanderson@demo.vosslab.net

Released: ☐

Release Status: NOTRELEASED

Sender Address: nter@olutions.com

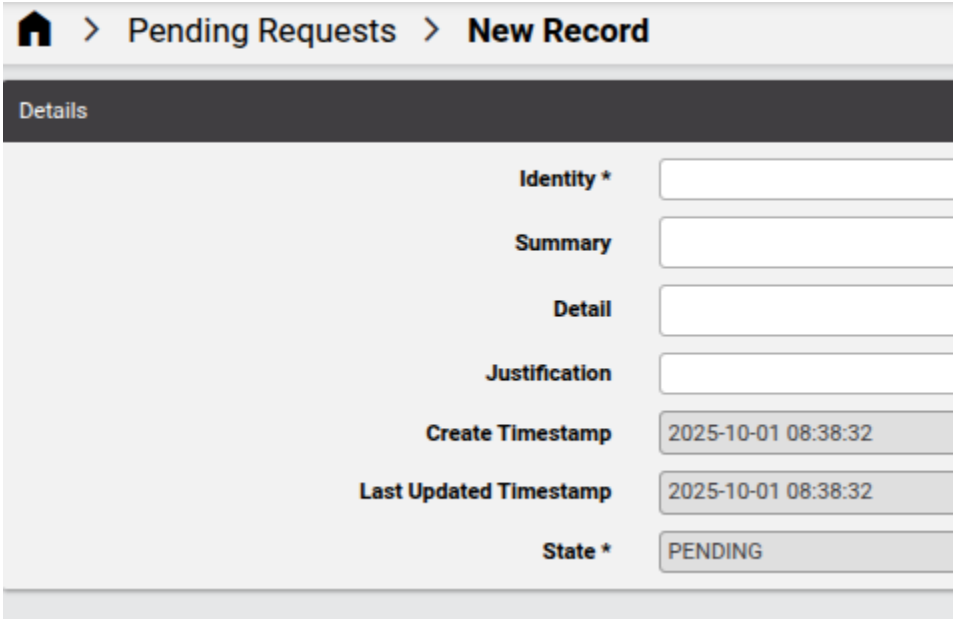
Size: 39741

Subject: Payment Details

System Released: ☐

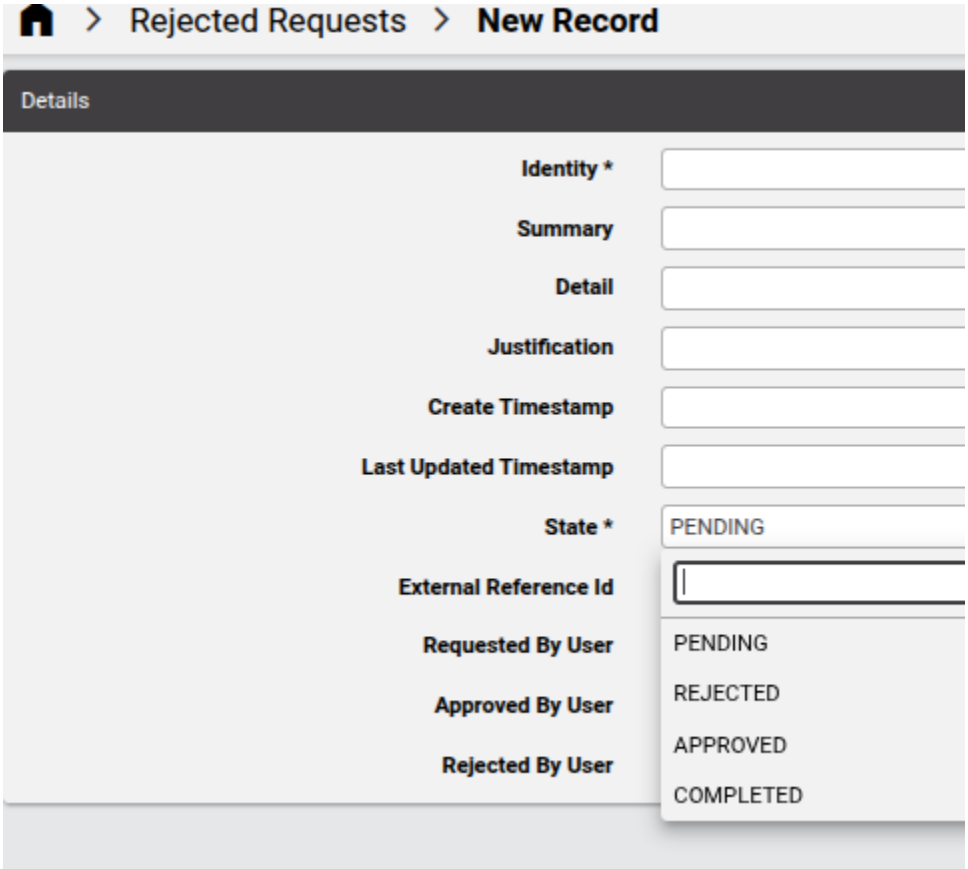
Copyright © 2025 VisionOSS Limited. All rights reserved.

For example, administrators can select a message from this list and request the release of the quarantined email message so that it will have a **State** as **PENDING**:



Similarly rejected requests can be managed:

Copyright © 2025 VisionOSS Limited. All rights reserved.

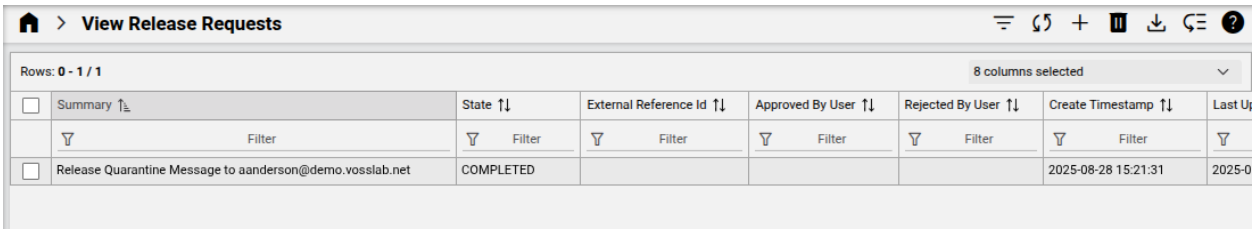


View Released Emails

By default, a separate list view is available to inspect all messages that have been released from quarantine.

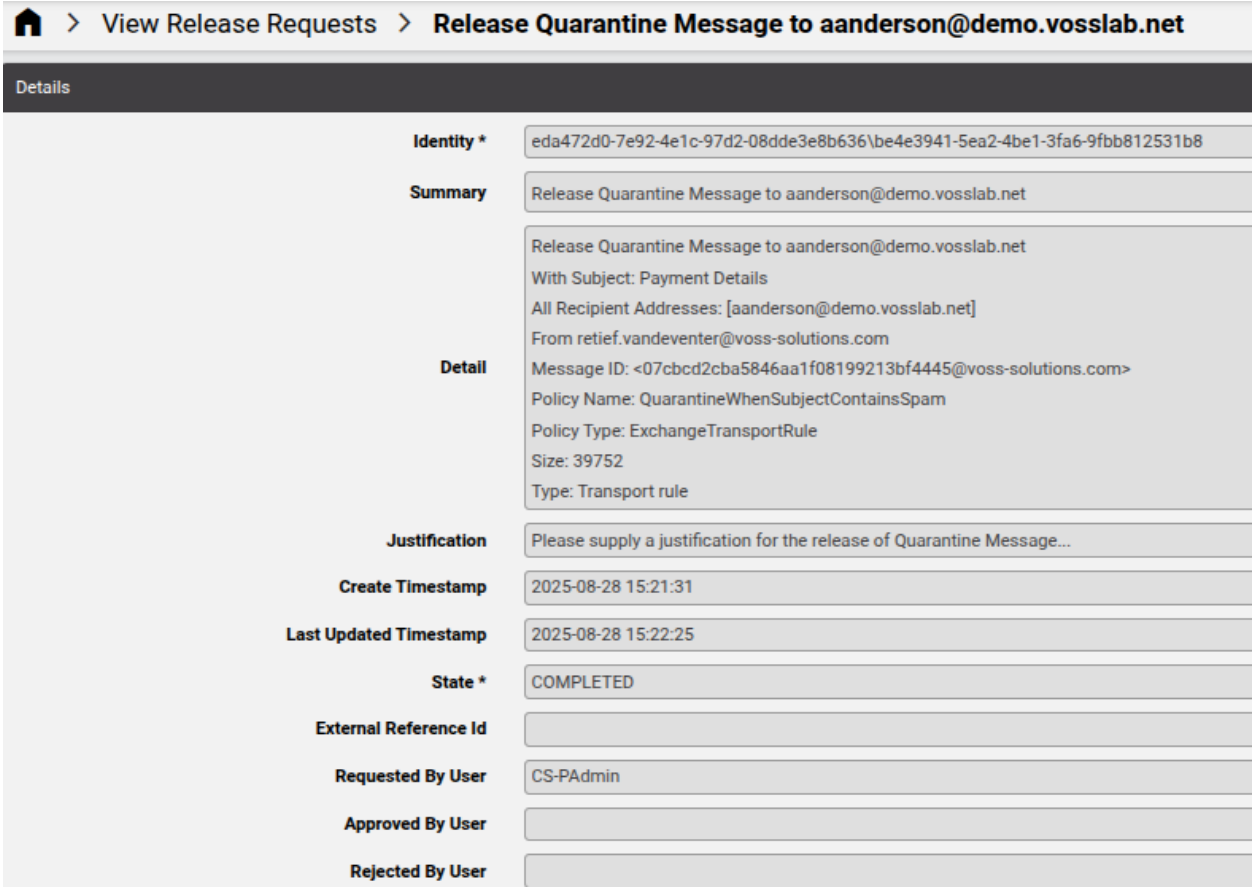
View Release Requests

Following on requesting the release of quarantined messages, the requests can be listed.



Release request instances can be inspected.

Copyright © 2025 VisionOSS Limited. All rights reserved.



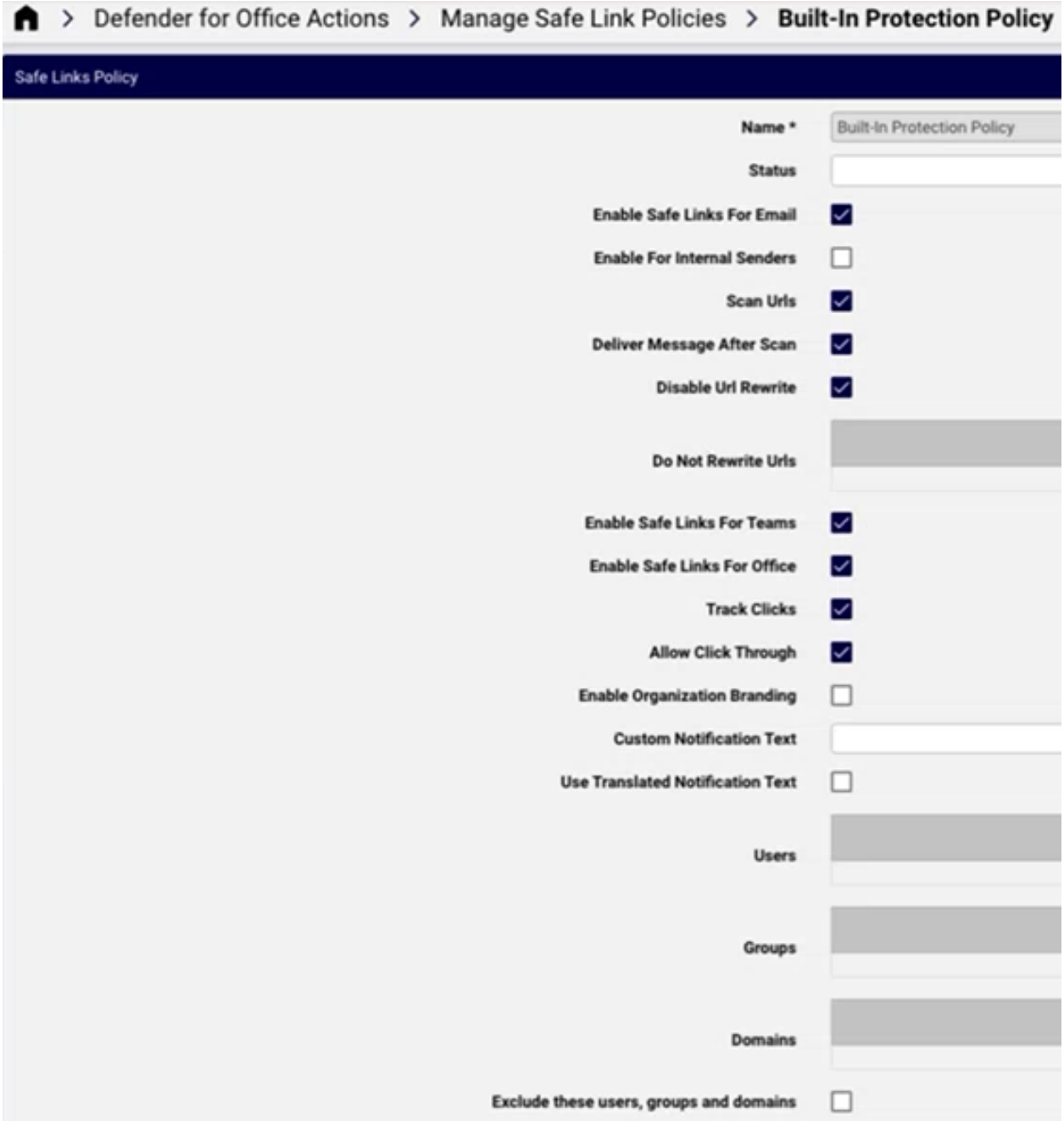
10.2.4. Safe Link Policies

Manage Safe Link Policies

Related device model: `device/msexchangeonline/SafeLinksPolicy`

Administrators can view and manage Safe Link policies in Automate. This includes the creation and configuration of policies.

Copyright © 2025 VisionOSS Limited. All rights reserved.

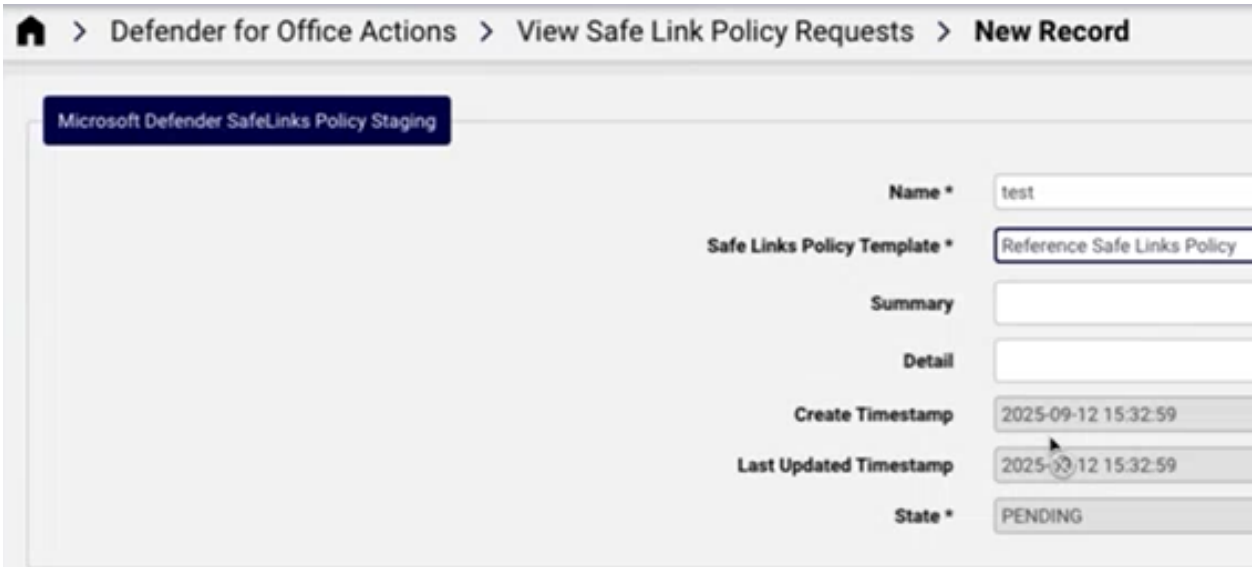


Request New Safe Link Policy

Automate provides a *staging area* for requests (maintained in the data model: `data/MicrosoftDefenderSafeLinksPolicyStaging`). Administrators can therefore submit requests for Safe Link policies, according to:

- a selected **Safe Links Policy Template**
- with **State** set as **PENDING**

Copyright © 2025 VisionOSS Limited. All rights reserved.



View Safe Link Policy Requests

By default, a separate list view is available to inspect all Safe Link policy requests that have been made, and to select a request for management.

Safe Link Policy Templates

Automate provides a reference configuration template for `device/msexchangeonline/SafeLinksPolicy`, called: `Reference Safe Links Policy`, but administrators can clone and manage these templates according to their needs when submitting policy requests.

10.2.5. Safe Attachment Policies

Manage Safe Attachment Policies

Related device model: `device/msexchangeonline/SafeAttachmentPolicy`

Safe Attachments in Microsoft Defender for Office opens attachments in a virtual environment before the messages are delivered.

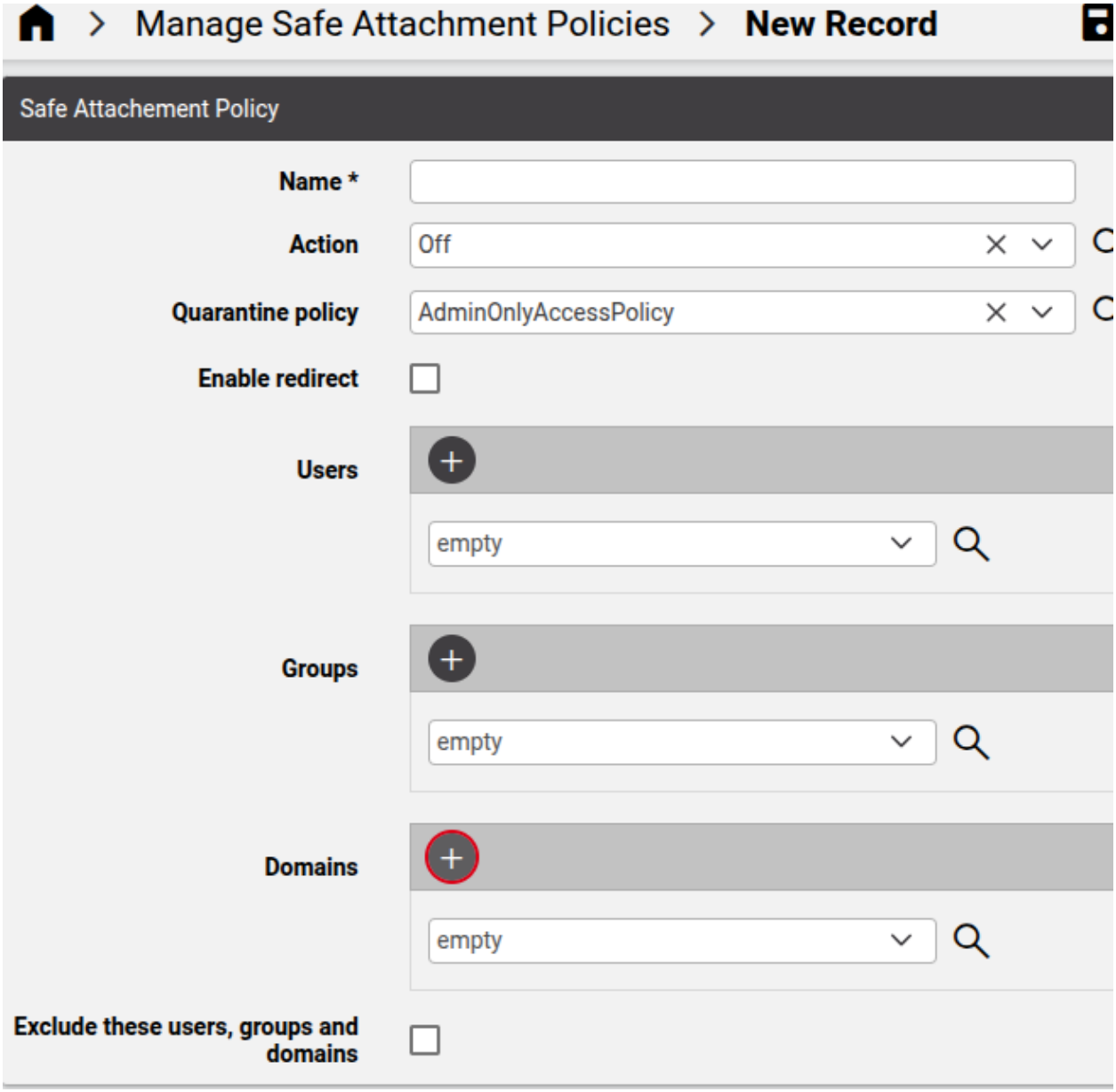
Safe Attachments policies can apply to specific users, groups, or domains and can be managed in Automate.

The **Quarantine policy** selected when managing a safe attachement policy in Automate is managed on the Microsoft Defender portal.

The default Microsoft Defender quarantine policies are:

- AdminOnlyAccessPolicy
- DefaultFullAccessPolicy
- DefaultFullAccessWithNotificationPolicy
- NotificationEnabledPolicy (in some organizations)

Copyright © 2025 VisionOSS Limited. All rights reserved.



Request New Safe Attachment Policy

Automate provides a *staging area* for requests (maintained in the data model: `data/MicrosoftDefenderSafeAttachmentPolicyStaging`).

Copyright © 2025 VisionOSS Limited. All rights reserved.

View Safe Attachment Policy Requests

By default, a separate list view is available to inspect all Safe Attachement policy requests that have been made, and to select a request for management.

Safe Attachment Policy Templates

Automate provides a reference configuration template for `device/msexchangeonline/SafeAttachmentPolicy`, called: `Reference Safe Attachment Policy`, but administrators can clone and manage these templates according to their needs.

Related Topics

- *Microsoft Defender for Endpoint security management and policies*
- *Model filter criteria* for Microsoft Defender Overbuild usage

10.3. Microsoft Defender for Endpoint security management and policies

Microsoft

10.3.1. Overview

Automate provides support for Microsoft Defender for Endpoint, that addresses user devices (laptops, phones, tablets, PCs) and network devices (access points, routers, firewalls).

Note:

- The following entry under **Global settings**, **Enabled Services** needs to be enabled: **Enable Defender for Endpoint** - see: *Global settings*.
- For further setup and configuration, see: *Microsoft Defender setup, sync and overbuild*.

10.3.2. Dashboards

The administrator interface provides dashboards for the view and management of data:

Dashboards:

Security Management - Defender for Endpoint Overview Security Management - Defender for Endpoint Actions

- By default:

Copyright © 2025 VisionOSS Limited. All rights reserved.

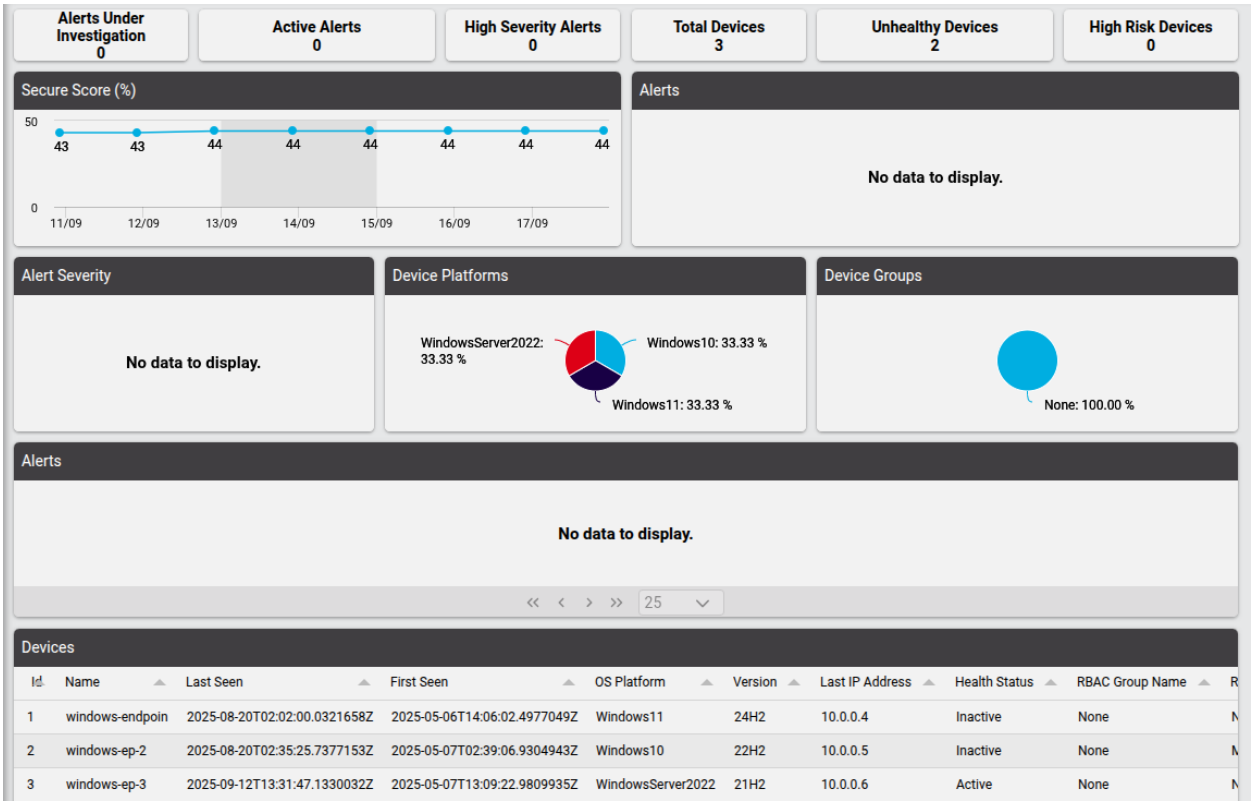
- The **Defender for Endpoint Overview** dashboard provides the administrator with counters, charts and tables showing information on alerts and devices that are visible from the administrator's hierarchy, for example the total number of alerts and status breakdowns by site, as well as an overview of device types and platforms.
- The **Defender for Endpoint Actions** dashboard also provides the administrator with counters on alerts and devices, as well as quick links to view and manage incident, alert and device actions.

To customize your dashboards:

- See: *Introduction to Automate dashboards*.
- Resources have been added and are available to widgets on a dashboard where **Data Source** is **Automate Analyzed**.

  For example:

  - Defender Actions, Shows Microsoft Defender actions, `device/mssecurity/MachineAction`
  - Defender Alerts,Shows Microsoft Defender alerts, `device/msgraphsecurity/Alert`
  - Defender Devices,Shows onboarded Microsoft Defender devices, `device/mssecurity/Machine`
  - Defender Exposure Score by Device Group,Shows Microsoft Defender exposure score by device group, `device/mssecurity/ExposureScoreByMachineGroups`
  - Defender Incidents,Shows Microsoft Defender incidents, `device/msgraphsecurity/Incident`
  - Defender Secure Score,Shows Microsoft Defender Secure Score, `device/msgraphsecurity/SecureScore`



Copyright © 2025 VisionOSS Limited. All rights reserved.

10.3.3. Incident and Alert Actions

Incidents

Related device model: `device/msgraphsecurity/Incident`

Automate provides an **Incidents** list view showing such headings as the incident **Status** and **Severity** at a hierarchy (**Located At**), and allows for the examination of the **Details** of an incident, including for example the **Incident Web URL** at `security.microsoft.com`.

- Details example in JSON:

```
{
    "id": "5",
    "tenantId": "f372af60-59d5-4e03-a849-9e46a432aac0",
    "status": "redirected",
    "incidentWebUrl": "https://security.microsoft.com/incident2/5/overview?tid=...",
    "redirectIncidentId": "1",
    "displayName": "[Test Alert] Suspicious Powershell commandline",
    "createdDateTime": "2025-05-07T13:12:59.9233333Z",
    "lastUpdateDateTime": "2025-05-07T13:13:12.24Z",
    "classification": "unknown",
    "determination": "unknown",
    "severity": "informational",
    "customTags": [],
    "systemTags": [],
    "lastModifiedBy": "Microsoft 365 Defender-AlertCorrelation",
    "comments": []
}
```

Alerts

Related device model: `device/msgraphsecurity/Alerts`

Automate provides an **Alerts** list view showing such headings as the incident **Title**, **Status**, **Severity**, **Description** and **Device** at a hierarchy (**Located At**), and allows for the **Details** of an instance to be viewed and managed.

Managing an alert

Administrators can manage the following alert properties:

- **Status**
- **Classification**
- **Determination**
- **Assigned To**
- Details snippet in JSON:

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
"category": "Execution",
"status": "resolved",
"severity": "informational",
"classification": "falsePositive",
"determination": "malware",
"serviceSource": "microsoftDefenderForEndpoint",
"detectionSource": "microsoftDefenderForEndpoint",
"createdDateTime": "2025-05-06T14:13:19.0633333Z",
"lastUpdateDateTime": "2025-08-21T02:47:29.24Z",
"resolvedDateTime": "2025-08-21T02:47:29.17Z",
"firstActivityDateTime": "2025-05-06T14:06:51.7300174Z",
"lastActivityDateTime": "2025-05-06T21:45:13.6345713Z",
"deviceEvidence": {
...
},
"userEvidence": {
...
},
"productName": "Microsoft Defender for Endpoint",
"deviceDnsName": "windows-endpoint",
"deviceTags": [
...
],
"userAccountName": "defender-admin",
"userSid": "..."
```


10.3.4. Device Actions

View Devices

Related device model: `device/mssecurity/Machine`

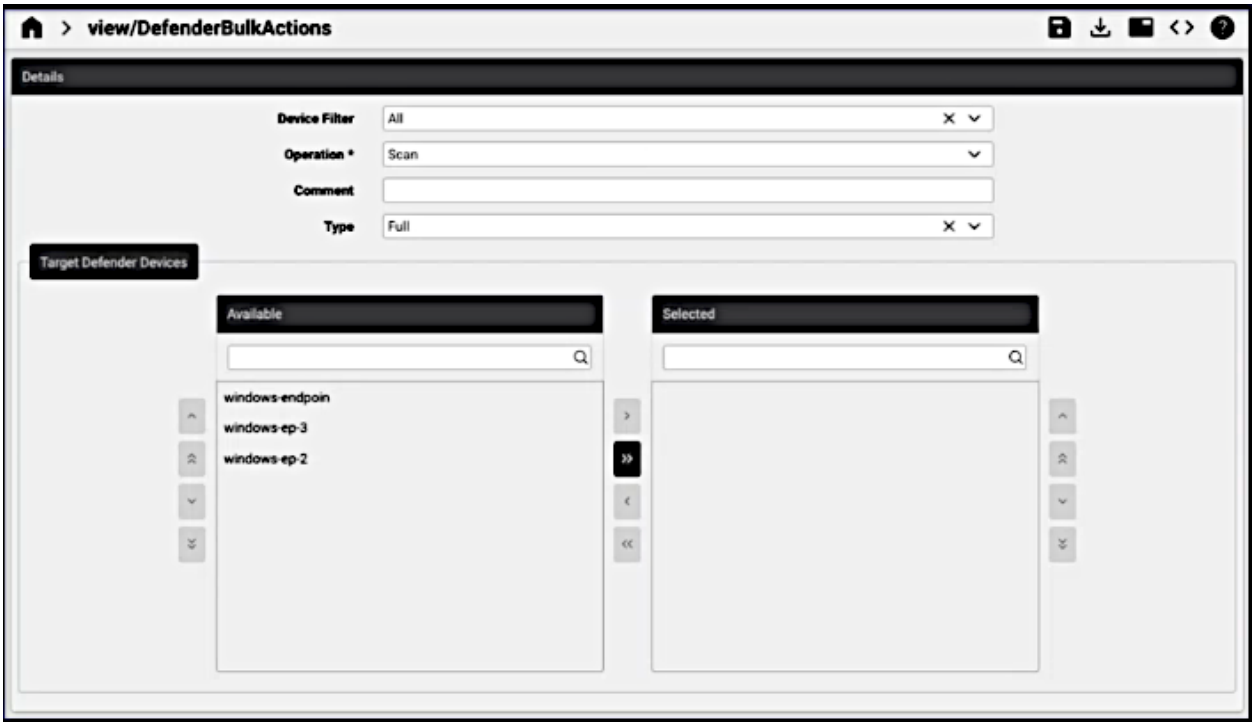
Automate provides an **View Devices** list view showing such headings as the **Last IP Address**, **Health Status**, **Exposure Level** and **Device** at a hierarchy (**Located At**), and allows for the examination of the **Details** of a device.

Bulk Actions

Automate provides an interface to carry out bulk actions on devices. For **Target Defender Devices**, the **Available** and **Selected** transfer boxes are available to select devices accessible from a hierarchy to carry out operations in bulk:

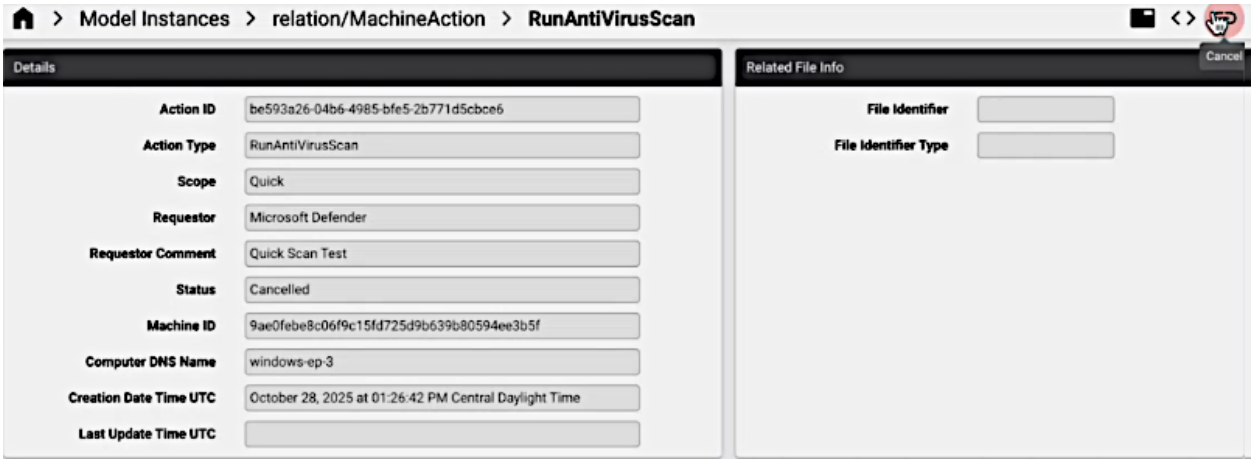
- **Device Filter**: by operating system - all, Windows, macOS, Linux, Android, IOS
- **Operation**: Scan, isolate, un-isolate, offboard, restrict code execution, unrestrict code execution
- **Type**: full, quick

Copyright © 2025 VisionOSS Limited. All rights reserved.



Machine Action

The `relation/MachineAction` model is available to allow for the execution of *Cancel* action. (This action sends a request to `device/mssecurity/MachineActionCancel`.)



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related Topics

- *Microsoft Defender setup, sync and overbuild*
- *Microsoft Defender for Office security management and policies*

Copyright © 2025 VisionOSS Limited. All rights reserved.

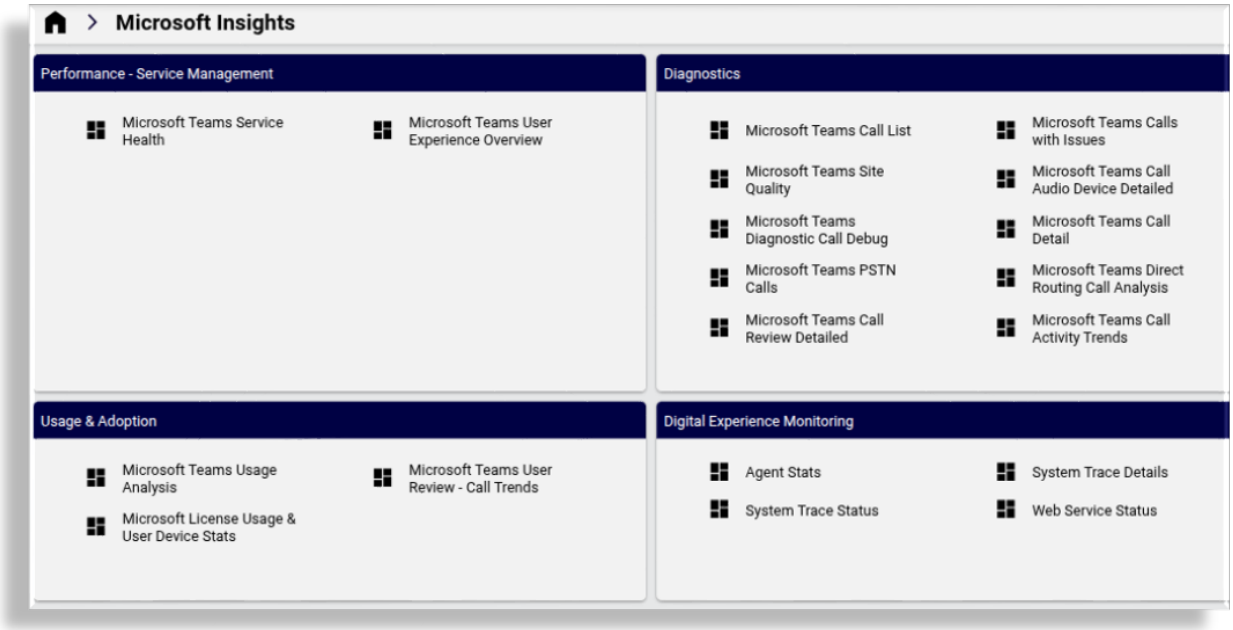
11. Insights Dashboards

11.1. Introduction to Microsoft Insights

11.1.1. Overview

The **Microsoft Insights** menu provides a single entry point dashboard to access a range of Microsoft performance, diagnostics and usage data presented in individual dashboards.

It includes Digital Experience Monitoring analytics that allows users to deploy and manage Insights agents and testing profiles to obtain a view on the health of such digital services as Microsoft Teams or Cisco Webex.



The sections below

- indicate the requirements to view and use these dashboards
- provide references to additional details
- include details on the Digital Experience Monitoring dashboards and setup.

11.1.2. Requirements

The **Microsoft Insights** menu is by default available to administrators on Automate where the following requirements are set:

- The **Global Settings**, **Enabled Services** shows **Enable Microsoft** as true. See: *Global settings*
- The system is licensed for **Insights Collaboration Assurance**. This allows for access to the **assurance** data source used in dashboards. See: **Licensed Applications** under *Manage your Automate product license*

11.1.3. Performance - Service Management

- *Insights Microsoft Teams Service Health*
- *Insights Microsoft Teams User Experience Overview*

11.1.4. Diagnostics

- *Insights Microsoft Teams Call List*
- *Insights Microsoft Teams Calls with Issues*
- *Insights Microsoft Teams Site Quality*
- *Insights Microsoft Teams Call Review Detailed*
- *Insights Microsoft Teams Diagnostic Call Debug*
- *Insights Microsoft Teams Call Detail*
- *Insights Microsoft Teams PSTN Calls*
- *Insights Microsoft Teams Direct Routing Call Analysis*
- *Insights Microsoft Teams Call Review Detailed*
- *Insights Microsoft Teams Call Activity Trends*

11.1.5. Usage & Adoption

- *Insights Microsoft Teams Usage Analysis*
- *Insights Microsoft Teams User Review - Call Trends*
- *Insights Microsoft License & User Device Stats*

Copyright © 2025 VisionOSS Limited. All rights reserved.

11.1.6. Digital Experience Monitoring (DEM)

Overview and setup

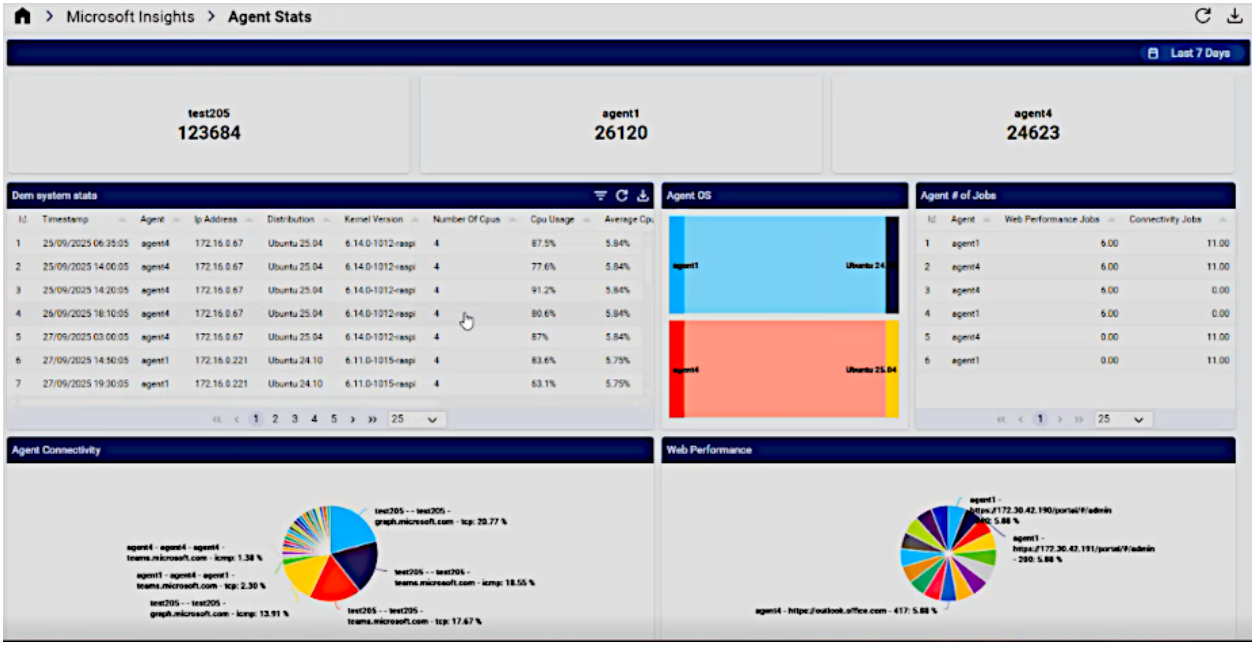
The following configuration requirements need to be completed in order to use the DEM dashboards:

- During arbitrator setup (see *Arbitrators*, Microsoft Tenant users are synced in to the Arbitrator hierarchy by using the **Sync in Microsoft Tenants** menu.
- DEM Agent installation and configuration

  See the Digital Experience Monitoring (DEM) Agent Installation topic in the Core Feature Guide

DEM Agent Stats

Provides an at-a-glance view of agent connectivity, web performance, and system statistics to monitor and optimize digital experience.



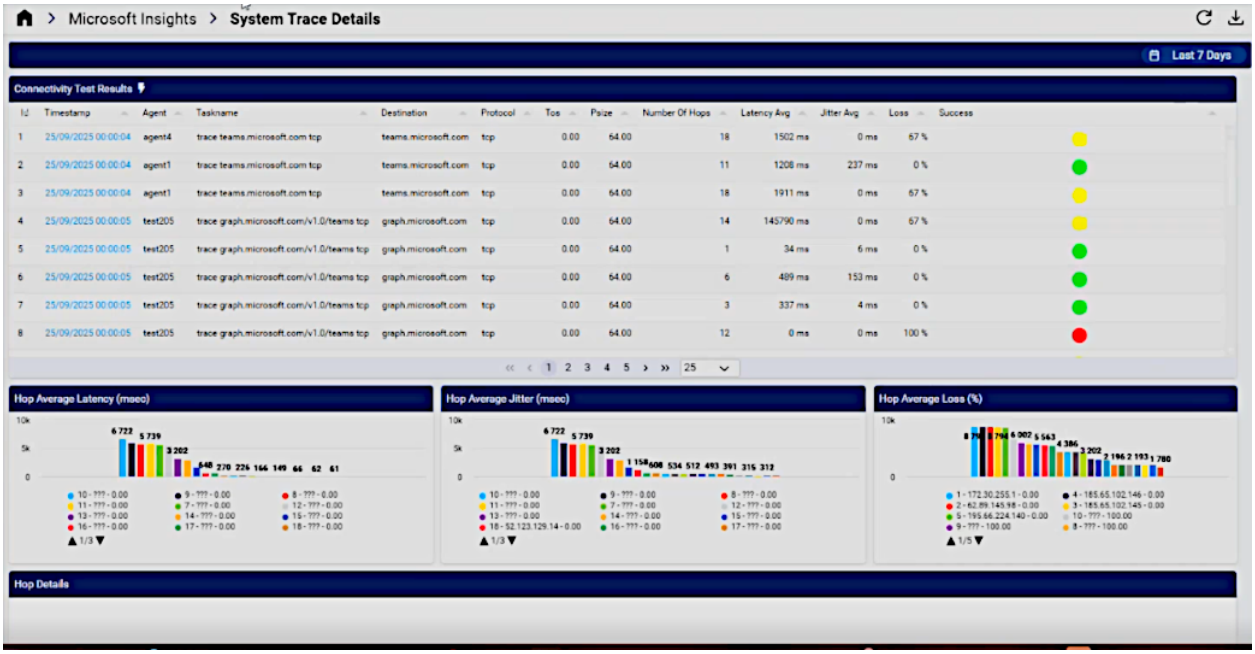
For further details, see: *DEM Agent Stats*

DEM System Trace Details

Provides detailed metrics on system connectivity, including ASN and hop-based insights into latency, jitter, packet loss, and trace details for performance monitoring.

An example dashboard is shown below:

Copyright © 2025 VisionOSS Limited. All rights reserved.

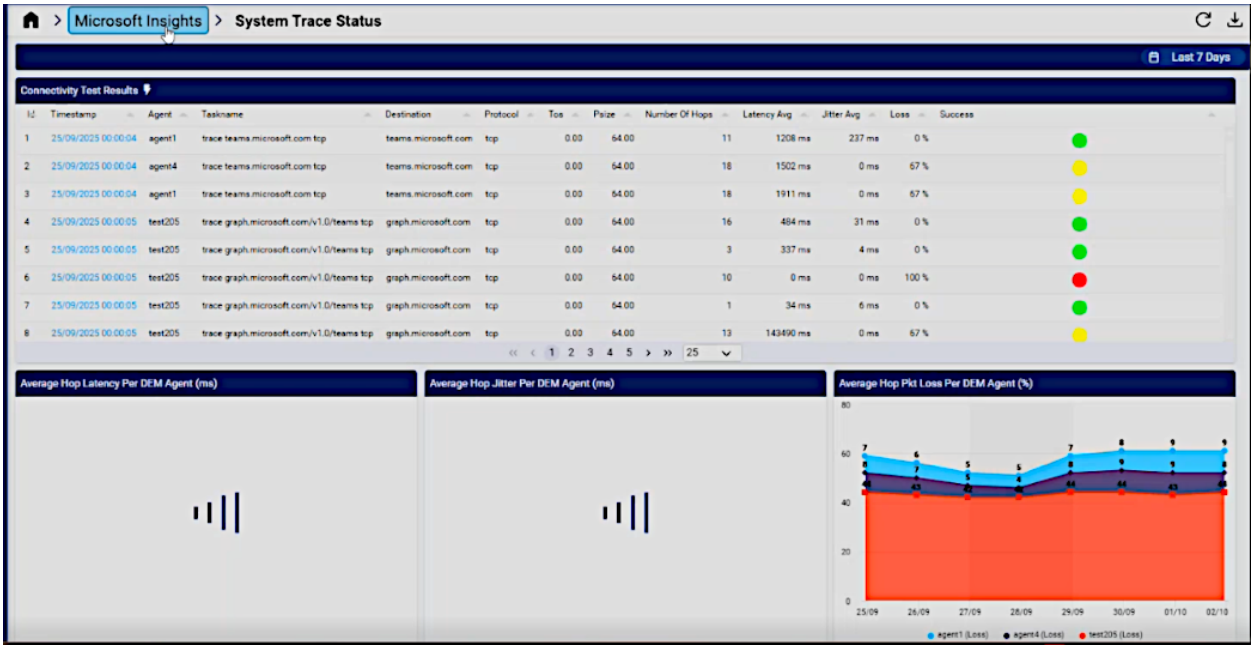


For further details, see: *DEM System Trace Details*

DEM System Trace Status

Offers a detailed view of system trace performance, highlighting top ASNs and destinations with the highest latency, jitter, and packet loss, alongside connectivity test results for comprehensive monitoring.

An example dashboard is shown below:



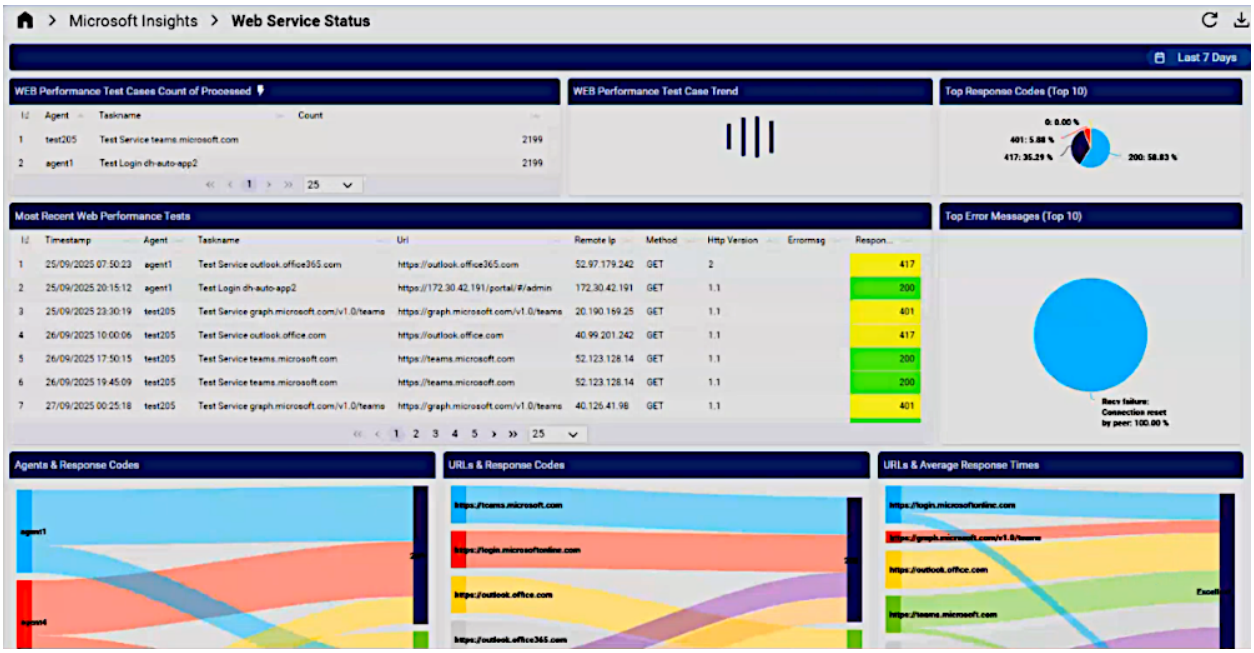
For further details, see: *DEM System Trace Status*

Copyright © 2025 VisionOSS Limited. All rights reserved.

DEM Web Service Status

Provides insights into web service performance metrics such as response times, connection times, and error messages, with trends and detailed test results for enhanced monitoring and optimization.

An example dashboard is shown below:



For further details, see: *DEM Web Service Status*

11.2. Digital Experience Monitoring (DEM) Agent Installation

11.2.1. Digital Experience Monitoring (DEM) Agent Installation Architecture and Requirements

Deployment Architecture

VOSS Insights provides for the installation and configuration of Digital Experience Monitoring (DEM) Agents.

The VOSS Insights Forwarder is an agent that collects statistics such as latency and response times on various cloud endpoints, along with system CPU statistics, which is sent by means of the API back to the Arbitrator.

The purpose of the agents are to monitor network experience, in particular for Microsoft Graph API, Teams, Web login and Exchange.

Measuring and widgets are available to:

- Measure hops
- Measure latency
- Measure web performance
- Provide alarms on for example: too many hops, latency, bad response

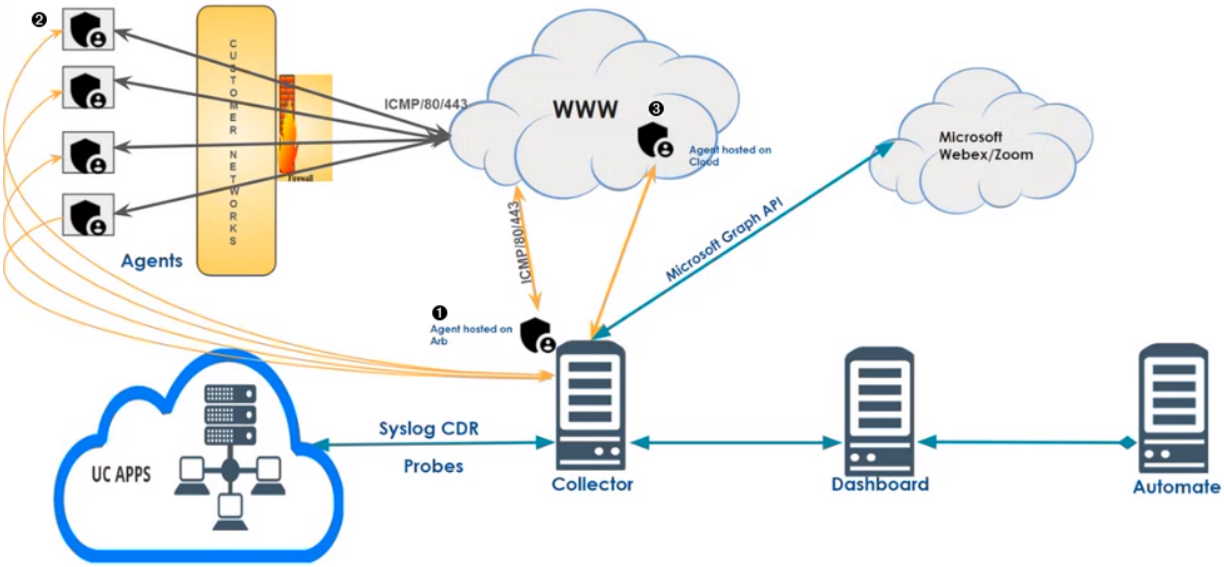
Copyright © 2025 VisionOSS Limited. All rights reserved.

A number of installation deployment options are available:

❶ One agent built into a single Collector

❷ Multiple agents within a customer network

❸ Agent hosted in the cloud



Hardware/OS requirements

The agent requires the deployment of a platform for it to run on - the agent itself is installed on that platform.

No specific hardware specification in terms of RAM, CPU, and so on is available: since this is a very lightweight agent, it can run on many hardware platforms.

However, some basic considerations are:

- Location - you want the device to be as close to the end user environment as possible - e.g “on the floor” with the users, not part of the data center (DC) infrastructure. For instance, part of the office wifi if that is the primary means of connectivity, or cabled into the local LAN if that is the primary.
- Connectivity - think of the different user connectivity options you want to test the experience over - LAN, wifi, guest wifi, etc.
- Small form factors typically work best, for example Intel NUC, Raspberry Pi, an old laptop, and so on.
- OS requirements are: Debian Linux OS. The agent installs via a Debian package install process.

The DEM agent does not currently support multiple network interfaces as part of the test suite - so if multiple interfaces are present, it will use the OS default routing. It is therefore currently best to just have a single network interface per device to ensure you know the interface being used.

Copyright © 2025 VisionOSS Limited. All rights reserved.

11.2.2. Connectivity

This section outlines the connectivity required to and from the agent.

VOSS Insights platform connectivity

The agent needs to communicate with the Arbitrator - whether that is in the same environment or in the VOSS Cloud.

Destination	Protocol/Port/Type	Purpose
Arbitrator	HTTPS 443 TCP ICMP	Registration and sending test results

Testing Connectivity

DNS - for resolving hostnames as part of the testing.

The recommended tests require the following connectivity if you intend to use them. Additional/alternate connectivity may be required if other tests are intended to be used.

The current schedule of test runs is every 5 minutes.

Destination	Protocol/Port/Type	Purpose
https://graph.microsoft.com	HTTPS 443 TCP	Graph API connectivity
https://graph.microsoft.com	ICMP	Reachability stats for graph
https://teams.microsoft.com	HTTPS 443 TCP	Access to Teams front-end
https://teams.microsoft.com	ICMP	Reachability stats for Teams
https://login.microsoftonline.com	HTTPS 443 TCP	Web Testing example - microsoft login front-end
https://outlook.office.com	HTTPS 443 TCP	Web Testing example - Microsoft exchange web
https://outlook.Office365.com	HTTPS 443 TCP	Web Testing example - Microsoft exchange web

Copyright © 2025 VisionOSS Limited. All rights reserved.

11.2.3. Agent Installation

When installing the Voss-Forwarder package to the agent host, a number of failsafe options built in to assist you with the correct installation. These are also highlighted below.

The first step is to move the installation file to the host. (Use SCP, Filezilla, etc.)

The current file is named: `voss-insights-forwarder-1.0.deb`

1. At the host prompt, run: `sudo apt install ./voss-insights-forwarder-1.0.deb`

```
sysadmin@DH-Agent-002:~$ cd /root
sysadmin@DH-Agent-002:/root$ sudo apt install ./voss-insights-forwarder-1.0.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'voss-insights-forwarder' instead of './voss-insights-forwarder-1.0.deb'
The following NEW packages will be installed:
  voss-insights-forwarder
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/12.9 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /root/voss-insights-forwarder-1.0.deb voss-insights-forwarder all 1.0 [12.9 kB]
Selecting previously unselected package voss-insights-forwarder.
(Reading database ... 47642 files and directories currently installed.)
Preparing to unpack .../voss-insights-forwarder-1.0.deb ...
Unpacking voss-insights-forwarder (1.0) ...
Setting up voss-insights-forwarder (1.0) ...
Info: Voss-Insights-Forwarder installing
mkdir: cannot create directory '/var/log/voss': File exists
Info: Voss-Insights-Forwarder installed

Info: ####### Voss-Insights-Forwarder Configuration #####################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50

Progress: [ 60%] [#############################################################.................
```

2. Enter the IP Address or FQDN of the Arbitrator that the agent is to report to then press Enter. The agent will now do a connectivity check via ICMP (Ping) to the Arbitrator.
   - If connectivity is good, move on to the next step.
   - If there is no connectivity after 4 attempts, the package will exit.

```
Info: ####### Voss-Insights-Forwarder Configuration #####################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):

Progress: [ 60%] [#############################################################.....................
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Enter the username (if you created a new API user) or keep the default user and press Enter.

```
Info: ####### Voss-Insights-Forwarder Configuration #######################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):
Please Enter Arbitrator Password:

Progress: [ 60%] [#############################################################.............
```

4. Enter the password (set on the Arbitrator). This will then check the credentials are valid.
   - If credentials are valid, you move on to the next step.
   - If credentials are invalid after 4 attempts, the package will exit.

```
Info: ####### Voss-Insights-Forwarder Configuration #######################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):
Please Enter Arbitrator Password:
Info: API Credentials are valid.
Info: Updated /etc/voss/configs/voss_insights_remote.config with API Credentials.
Please Enter Customer Name: ANY-TEXT
Progress: [ 60%] [#############################################################..........
```

5. Enter a customer name (data is required to continue) and press Enter.

```
Info: ####### Voss-Insights-Forwarder Configuration #######################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):
Please Enter Arbitrator Password:
Info: API Credentials are valid.
Info: Updated /etc/voss/configs/voss_insights_remote.config with API Credentials.
Please Enter Customer Name: ANY-TEXT
Info: Updated '/etc/voss/configs/voss_insights_remote.config' with Customer ANY-TEXT
Please Enter Forwarder Name: DH-Agent-1-site
Progress: [ 60%] [#############################################################............
```

6. Enter the Forwarder name (this should for example be a descriptive location). Press Enter.

```
Info: Updated '/etc/voss/configs/voss_insights_remote.config' with Customer ANY-TEXT
Please Enter Forwarder Name: DH-Agent-1-site
Updated '/etc/voss/configs/voss_insights_remote.config' with Forwarder Name 'DH-Agent-1-site'

Info: ########### Voss-Insights-Forwarder Configuration Complete! ###############

##############################################################################
```

This completes the configuration.

Copyright © 2025 VisionOSS Limited. All rights reserved.

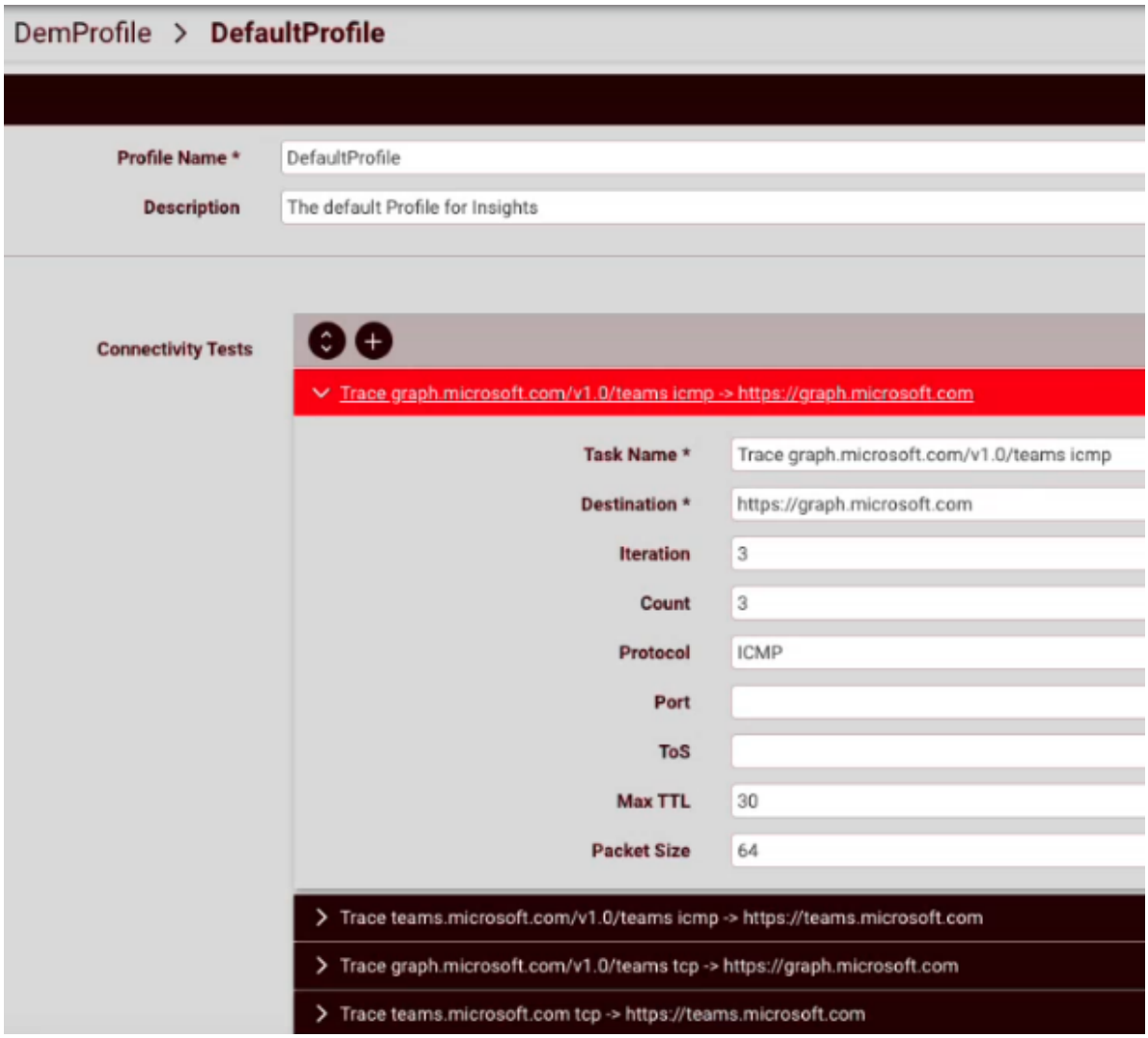
11.2.4. Digital Experience Monitoring Agents and profiles

Following the installation of Digital Experience Monitoring Agents, their configuration can be carried out in Automate.

Automate provides access to configuration interfaces for:

- **Digital Experience Monitoring Profiles** (`device/arbitrator/DemProfile`)

  Test configurations can be managed for connectivity and performance tests. This configuration can then be assigned to an agent as a **Profile**.



Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Digital Experience Monitoring Agents** (`device/arbitrator/DemAgent`)

  A profile can be managed and then be associated with an agent when managing the agent by selecting it from the **Profile** dropdown list. In addition, an agent can be also be enabled or disabled from the **Enable** dropdown options.

Copyright © 2025 VisionOSS Limited. All rights reserved.

12. System Configuration

12.1. Customizations

12.1.1. Introduction to customizations

The system allows a provider administrator (or higher) to customize the Admin portal user interface.

This customization includes:

- Theme selection
- Menu Layout customization and associated Field Display Policies
- Dashboard customization
- Field Display Policies
- Configuration Templates

12.1.2. Model filter criteria

Tip: *Use the Action search to navigate Automate*

Overview

Model filter criteria defines how users (for example, Microsoft Active Directory or MS Entra MSOL user) are matched to corresponding data in Automate to move users and related data to the correct system levels (Customer or Site) on import (in a sync or overbuild), based on one or attributes defined for the model type.

Note: Model filter criteria for LDAP sources is only compatible with Microsoft Active Directory (that is, Microsoft LDAP, not OpenLDAP).

Administrator users with access to the `data/ModelFilterCriteria` model can manage instances of this model so that these are available for selection in the Site Defaults Doc (SDD) of a site.

The SDD provides options to choose a predefined model filter criteria (depending on the user type). Options are:

- MS 365 User Model Filter Criteria

- Microsoft Active Directory (Microsoft LDAP) User Model Filter Criteria
- CUCM User Model Filter Criteria

In addition, model filter criteria can also be executed directly, in other words outside of the import (sync or overbuild) process. By default, the administrator's default access profile (for the Automate - Admin role) has the **Permitted Operation** called **Execute** enabled for model filter criteria. This allows for model filter criteria execution to match and move data from the source hierarchy to the specified target hierarchy.

Related topics

- Flow through provisioning (FTP) in the Core Feature Guide.

Create model filter criteria

Pre-requisites:

- To allow move to work using model filter criteria defined at the Site level, an admin user must enable the following on the **Flow Through Provisioning** tab in the **Global Settings**:
  - Enable Move & Flow Through Provisioning
  - Enable Move & Provisioning after Add Sync

Perform these steps:

1. Identify the source and target model and field that will be used in the filter.
2. Go to **Model Filter Criteria**.
3. Click **Add** to add a new record, or clone an existing model filter criteria and update it to create a new model filter.
4. Provide a **Name**, **Description**, and **Usage** for the filter.

   For **Usage**:

   - The model filter criteria with usage set to **Move User** is used to move the user.
   - Model filter criteria with usage set to **Flow Through Provisioning** is used to provision the user. The flow through provisioning usage does not move a user, and will run only if the user is at a site.
   - If set to **Overbuild**:
     - the **Target Hierarchy** drop down is shown, listing the available nodes below the current hierarchy. (For bulk load sheets, enter the full hierarchy path, starting from `sys`.)
     - the **Automated Overbuild** check box is available to enable so that only MFCs set to **Automated Overbuild** will then be executed.
5. From the **Type** (model type) drop-down, select the source model, for example `device/msgraph/MsolUser` (MS Entra MSOL users) or `device/ldap/user` (Microsoft Active Directory users). For Microsoft Defender overbuild, select the relevant device model, for example `device/msexchangeonline/QuarantineMessage` - see: *Microsoft Defender for Office security management and policies*.

   Note: The model type defines the available attributes you can use in the model filter criteria.

6. Click the Plus sign (+) in the **Criteria** group to add one or more criteria.

   Each criteria is defined by the following:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Unary Operator	None, or NOT: to operate on the match **Condition** with the target value
Attribute	The field from the source model, for example `City` from `device/msgraph/MsolUser`.
Condition	Options are exact and non-exact types of contains and equals, as well as a regex search option.
Value	The target value that identifies the site in VOSS Automate. The value can also be a named macro, for example, `{{ macro.OVERBUILD_SITE_CITY_NAME }}`.
Conditional Operator	AND or OR: only needed and used to indicate the type of Boolean combination with the following criteria instance, if an additional instance is added.

7. Save the model filter criteria.

   You will be able to choose this new model filter criteria in the site's SDD, and it will be, for example, applied in the Microsoft overbuild if **Include Site for Overbuild** and **Microsoft Users** is enabled.

   When running the overbuild, the system loops through the site defaults to identify sites with **Include Site for Overbuild** enabled, and moves related user data to the site based on the chosen model filter criteria rule.

   In this example, all `device/msgraph/MsolUser` instances synced in will be moved to the site matching `{{ macro.OVERBUILD_SITE_CITY_NAME }}` if their `City` value matches.

8. If required, use the **Execute** button to run the model filter criteria in order to move matched data.

Microsoft Entra ID groups in model filter criteria

For model filter criteria of **Type** `device/msgraph/MsolUser`, the **Attribute** called `Groups.displayName` can be used to create a filter for syncing in and automatically onboarding - move and provision users - based on their Microsoft Entra ID group membership.

Important: Consider the following when creating filters using `Groups.displayName`:

- The **Value** of the `Groups.displayName` attribute should be an exact *case-sensitive* match of the Microsoft Entra ID group name.

  For example, a **Value** of `Northwood` will match `Northwood`, but will not match `northwood`, `Northwoodly`, `WestNorthwood` or `Westnorthwood`.

- The **Condition** should be `Equals Exactly`.
- Multiple conditions using the `Groups.displayName` attribute are supported, but require the use of `AND` as the **Conditional Operator**. All conditions in the filter should therefore be true for the filter to apply; in other words, the user needs to belong to *all* the groups matching the **Value** field.

  Note:

  – If a *single* matching filter condition is added whereas a user belongs to more than one Microsoft Entra ID group, the user is matched if the filter matches.

  – If an `OR` conditional operator is used, this will be interpreted as an `AND` operator.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The `Groups.displayName` attribute cannot be combined with other attributes in a filter: other attributes will be ignored.
- Verify that these caveats are taken into consideration, since model filter criteria can be saved in the system without their consideration.

Additional available model filter criteria for device/msgraph/MsolUser

From release 25.1 onwards, the model filter criteria of **Type** `device/msgraph/MsolUser` offers additional **Attribute** values:

```
City
CompanyName
Country
Department
EmployeeType
extensionAttribute1
extensionAttribute10
extensionAttribute11
extensionAttribute12
extensionAttribute13
extensionAttribute14
extensionAttribute15
extensionAttribute2
extensionAttribute3
extensionAttribute4
extensionAttribute5
extensionAttribute6
extensionAttribute7
extensionAttribute8
extensionAttribute9
IsLicensed
Licenses.SkuId
Office
UserPrincipalName
UserType
```

The use of these attributes in model instance filters allow for the optimization of sync performance and timing, as well as additional filtering functionality in the list view of `device/msgraph/MsolUser`.

Note: By default, model filter criteria with attribute *UserType* and value *Member* is automatically applied to filter the `device/msgraph/MsolUser` model sync into Automate from the Microsoft tenant. The default filter then allows only import of real users; that is, members only, and not external/guest accounts (where *UserType* is *Guest*). While the default filter syncs is only *Member* user types, you can adjust the model filter criteria to sync in *Guest* user types from the tenant, if required.

Automatic filtering on member users ships with Automate 25.1. Post-upgrade syncs on existing tenants where external/guest users have previously been synced in won't trigger workflow changes and updates to the existing users.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Microsoft Defender criteria for overbuild

If Microsoft Defender for Office is enabled as a service in global settings, additional model filter criteria are added to allow for the move of MS Defender policies, incidents and alerts.

See:

- Microsoft Defender setup, sync and overbuild in the Core Feature Guide
- Overbuild for Microsoft in the Core Feature Guide

Related Topics

- Microsoft Overview in the Core Feature Guide
- Sync to Site with with Flow Through in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide

12.1.3. Macros

Tip: *Use the Action search to navigate Automate*

Macros are used to return data from the system in various formats, to test for conditions, map data from Admin Portal or bulk loader input to various elements in the system (in conjunction with configuration ltemplates) and to access data in workflow steps.

Note: You can view existing macros and add new macros via the **Macros** page. For details on creating macros, see the Advanced Configuration Guide.

Various macro functions are available. These serve as boolean operators or can be used to carry out various numeric functions, string manipulation functions, list functions, time functions, and hierarchy related functions.

Note: The following macro functions are only available to administrators with an Access Profile set to **Full Access**:

- `fn.request_get`
- `fn.perform_http_get`

Macros can be created for re-use, named and stored as an instance of the Macro data model. When re-used, the reference prefix syntax is of the format: *macro.<macroname>*.

Named macros and macro functions can be nested within other macros.

Refer to the Macro Reference topics.

Copyright © 2025 VisionOSS Limited. All rights reserved.

12.1.4. Drop-down filters

Tip: *Use the Action search to navigate Automate*

Overview

Administrators with access to the **Dropdown Filters** page can manage the items available in drop-down lists on input forms. A filter would typically be used to define a shorter drop-down list.

Filters can be added, removed, modified and two existing filters can also be merged to define a new filter.

The Dropdown Filter list macro name that is generated starts with `DDF__` and is of the format (dots and slashes replaced by underscores):

```
DDF__<target model type> _<target model name>_<target field>
```

This is also the name shown in the **Dropdown Filters** list view at the hierarchy at which is was created.

Add a drop-down filter

1. Navigate to the required hierarchy.
2. Go to the **Dropdown Filters** page, then click the Plus icon (+) to add a new record.
3. At **Select a Dropdown Filter action**, select **Create a Dropdown Filter**.
4. Select a target model name and target field name to which the filter is to be applied.

   This is the drop-down field on an input form on the Admin Portal. Click **Help** on the input form to see the names.
5. Identify the associated **Model Type** and **Dropdown Field** of the **Dropdown Filter specifications**.

   Note: This can differ from the form names. Click **Help** on the input form to verify.

6. Set up the **Filter Fields**. Compare a **Filter Field** to a **Filter Field Value**:
   - contained in or not contained in
   - equal or not equal

   Note:
   - The **Filter Field** can differ from the **Target Field**, that is, the drop-down list can be filtered according a filter applied to *another* field that belongs to the **Model Type**.
   - The **Filter Field value** can also take the *name* of a named macro that resolves to a value, for example: `macro.SITENAME`.
   - If the same **Filter Field** is used more than once, these filters will be merged, that is, the *combined* filters on the field apply.

7. Add **Additional Parameters** to the filter:
   - direction:hierarchy direction for search: [up|down|local|parent|below|above] (`below` and `above` exclude current hierarchy)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- device: device name
- ndl: network device list that the device belongs to
- limit: number of results
- skip: start number of results - can be used for paging
- title: character or regular expression: only return values matching its value

For details and examples, refer to the topics on macro syntax in the Advanced Configuration Guide.

8. Click **Save**. A drop-down filter is created.

   This filter is a named list macro that will be added to the GUI Rule which is in place at the selected hierarchy for the **Target Field** on the Admin Portal input form of the selected **Target Model Name**.

   When opening a drop-down filter, the macro is shown in the **Macro** field at the bottom of the form. Users who have menu access to the list of named macros can also see the drop-down filter macros by filtering the list by name starting with `DDF__`.

Drop-down filter example

Consider the filter:

- **Target Model Name**: `relation/LineRelation`
- **Target Field**: `callForwardAll.callingSearchSpaceName`
- **Model Type**: `device/cucm/Css`
- **Dropdown Field**: `name`
- **Filter Field**: `name`
- **Filter Condition**: `Contains`
- **Filter Field Value**: `Cu2`
- **Additional Parameter**: **Parameter Title**: `Direction`
- **Additional Parameter**: **Parameter value**: `up`

The list macro that is created applies to the GUI rule for the input field `callForwardAll.callingSearchSpaceName` of the input form for `relation/LineRelation` at the selected hierarchy. The list macro would then be:

```
{# device/cucm/Css | name /Cu2/i | direction: up #}
```

If you have access to the Macro Evaluator, you can test this macro. Also refer to the topic on Macro Syntax in the Advanced Configuration Guide for more details.

In the **Dropdown Filters** list view at the hierarchy, the **Filter Name** shows as:

`DDF__relation_LineRelationTarget_callForwardAll_callingSearchSpaceName`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Merged drop-down filters

Two existing drop-down filters can be merged to create a new dropdown filter. The merged filter is a drop-down list that uniquely combines the lists from the two drop-down filters.

Merge drop-down filters

1. Navigate to the required hierarchy.
2. Go to the **Dropdown Filters** page.

   Check that the two drop-down filters that you want to merge are showing in the list view at the hierarchy. Otherwise, add the drop-down filters.
3. Choose **Merge Existing Dropdown Filters** from the **Select a Dropdown Filter Action** drop-down list.
4. Choose the **Target Model** and **Target Field** names to which the filter is to be applied.
5. Choose the two drop-down filters from the **Dropdown Filters to merge** form.
6. Click **Save**. A merged drop-down filter is created.

Note: Only two filters can be merged. To merge more than two drop-down filters, first create a merged filter of each filter pair and select it to be merged.

When a created merged drop-down filter is opened, the macro is shown in the **Macro** field at the bottom of the form. The macro uses the `fn.list_extend_no_dup` macro function to uniquely merge the two drop-down filter lists. The macro syntax is of the format

```
{{ fn.list_extend_no_dup macro.DDF__<filter name 1>, macro.DDF__<filter name 2> }}
```

Refer to the topic on Macro Syntax and List Functions in the Advanced Configuration Guide for more details.

12.1.5. Quick Add Groups

Tip: *Use the Action search to navigate Automate*

Overview

A Quick Add Group (QAG) is a collection of configuration templates (CFTs) and features for onboarding users. This grouping allows admins to quickly and easily configure users.

Note: If you need to view or modify a CFT in a QAG, you can easily go directly to a CFT selected in a drop-down on a QAG form via an automatically generated URI link that will display next to that drop-down, provided you have appropriate access permissions to that CFT. See *Navigate to related entities from drop-downs*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Configuration templates in the Core Feature Guide
- Create a configuration template in the Advanced Configuration Guide
- Quick Add Group customization in the Advanced Configuration Guide
- *Onboard user (Microsoft)*
- *Introduction to Microsoft Teams policies* in the Core Feature Guide
- *Navigate to related entities from drop-downs*

Example: Using CFTs and QAGs to add users

Example 1 - Two user groups with different phones and services

In this example we're adding a group of 100 back office users, and a group of 50 sales users. Each group will be assigned a specific phone type, and either has or does not have specific services:

User group?	Using which phones?	And which services?
Back office users	All using 7965 phone with SCCP protocol	No services
Sales users	All using 8865 phone with SCCP protocol	Single number reach service (SNR)

To configure the *Example 1* scenario:

1. Create two configuration templates (CFTs):
   - For the back office users, create a CFT for the 7965 phone, with no services.
   - For the sales users, create a CFT for the 8865 phone, with SNR service
2. Create two Quick Add Groups:
   - For the back office users, create a QAG that references the CFT you created for the back office users.
   - For the sales users, create a QAG that references the CFT you created for the sales users.

Example 2 - Users with phone type 6911 and SCCP protocol

In this example we're adding back office users with a 6911 phone type using SCCP protocol and a voice account.

User group?	Using which phones?	And which services?
Back office users	Phone type 6911 using SCCP protocol	Voice account

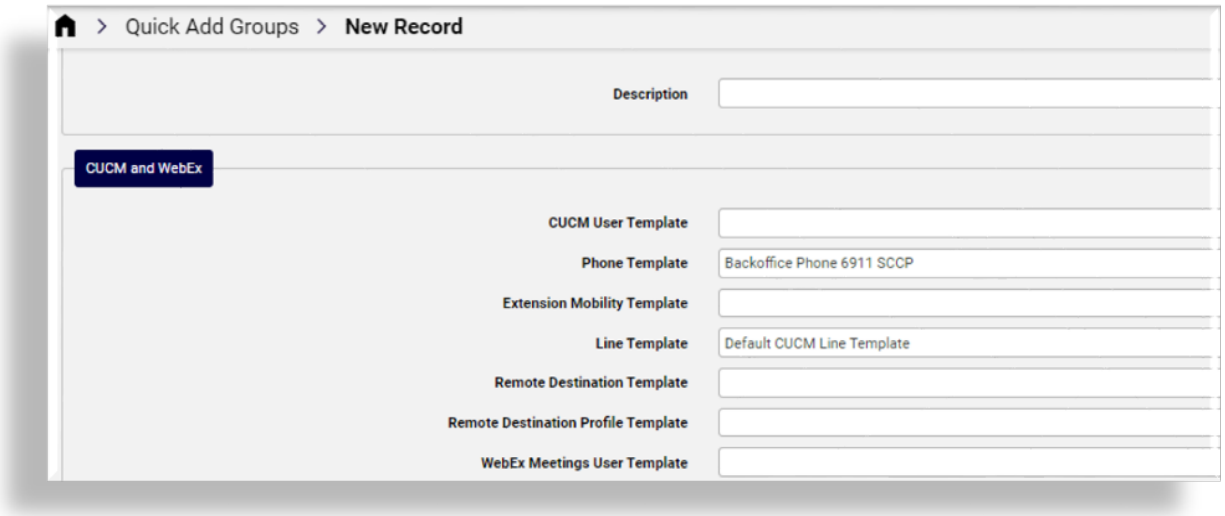
To configure the *Example 2* scenario, add the Quick Add Group, and choose these configuration templates from the Cisco UCM and Webex template group on the form:

- **Phone Template** - select the **Backoffice Phone 6911 SCCP** CFT from the drop-down of available CFTs

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Line Template** - select the **Default UCM Line Template** CFT from the drop-down of available CFTs (this CFT associates a line with the phone)

Note: You can also use customized CFTs to assign to a Quick Add Group. The custom CFT can be at the same level in the hierarchy as the Quick Add Group, or higher.



Naming convention for Quick Add Groups

The best practice naming convention recommendation for Quick Add Groups may use the following pattern:

<friendly hierarchy name>-QAG-<user type>-<phone-template-name>-[description]

For example, `GeoLogic-QAG_BasicUser - 69XX SIP - CallWaiting`

Quick Add Groups named macros for Quick User

When using Quick User (for Microsoft, Cisco, Webex Teams, or Hybrid users) you'll choose a Quick Add Group that assigns services and sets up the user.

Quick Add Groups contain one or more configuration templates that defines how the user is assigned services. Named macros are used in the configuration templates. A default named macro is associated with each of the following *Quick User* scenarios:

Where used?	Named Macro
Cisco Quick User	`macro.Default_Quick_Add_Group_Cisco_Subscriber`
Microsoft Only Quick User	`macro.Default_Quick_Add_Group_Microsoft_Subscriber`
Webex Teams Calling Only Quick User	`macro.Default_Quick_Add_Group_Webex_Subscriber`
Hybrid Quick User	`macro.Default_Quick_Add_Group_Hybrid`

By default, the values of these macros are set to be the first Quick Add Group found up in the hierarchy:

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
{{ fn.one data.QuickAddGroups.group_name | | direction:up }}
```

However, these named macros can be cloned to a hierarchy and modified in order to provide a reference to a specific default Quick Add Group to apply, as required.

Note: See the *Advanced Configuration Guide* for further details on macros.

When adding users, choose the appropriate Quick Add Group for the user you're provisioning.

All user services use configuration templates that belong to a Quick Add Group.

Related topics

- Named Macros Overview in the Advanced Configuration Guide
- Quick Add Group Functions in the Advanced Configuration Guide

Configuration templates for Microsoft in a Quick Add Group

A group of configuration templates are available for Microsoft in the Quick Add Group form.

Note: You can show or hide fields on a Quick Add Group form via a field display policy (FDP).

The image displays a Quick Add Group used for offboarding, where the **Subscriber Offboarding** checkbox is configured via a FDP to display on this form, and the setting is enabled, which means that this Quick Add Group is available for selection when running *Offboard user (Microsoft or Webex)*.

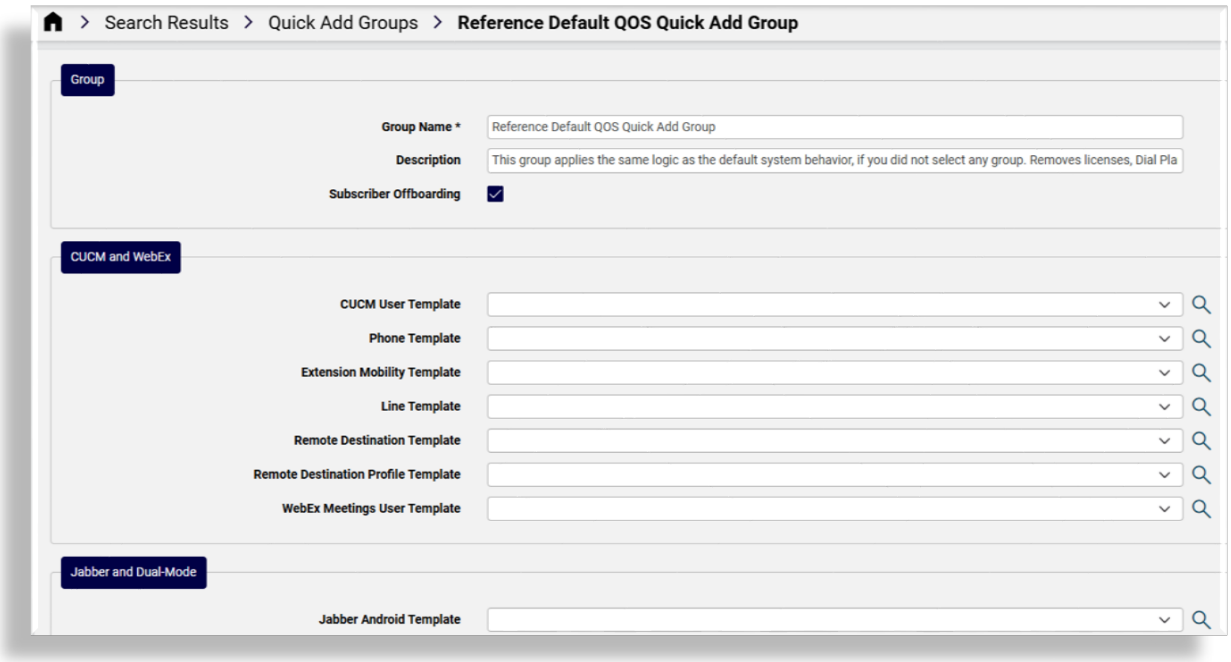
The flag acts as a filter so that only Quick Add Groups with this flag enabled display on the *Offboard User* page. By default the **Subscriber Offboarding** checkbox is clear (set to False).

Quick Add Groups designed for user offboarding function in a similar way to how configuration templates are configured to drive onboarding. For offboarding however, an admin configures the CFTs to drive offboarding. For example, defining CSOL CFTs to reset policies to some default, to clear Enterprise Voice or to clear the LineUri.

Only QAG's flagged for subscriber offboarding display in the **Offboarding Quick Add Group** drop-down. However, these QAGs are still valid as options on normal Quick User forms, so it is recommended that clear and descriptive names are used to identify the purpose of the QAG.

For more information around the system behavior for offboarding Microsoft users, see *Offboarding (Microsoft)*.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes configuration template options for Microsoft on Quick Add Group forms:

Note: Automate ships with reference and system configuration CFTs that you can clone and customize, if required. The CFTs available for selection in the template fields on Quick Add groups may be defaults or custom CFTs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CFT Template Type	Description
MS 365 User Template	.
MS Teams User Template	CFTs for **MS Teams User Template** can define the Microsoft Teams policies to be included.
MS Groups Add Template	CFTs available for **MS Groups Add Template** and **MS Groups Remove Template** can be selected to assign or unassign MS 365 group membership to a user when a Quick Add Group with this CFT selected is used during Microsoft Quick User. This functionality allows for group licensing, typically used in large enterprises.
MS Groups Remove Template	CFTs available for **MS Groups Add Template** and **MS Groups Remove Template** can be selected to assign or unassign MS 365 group membership to a user when a Quick Add Group with this CFT selected is used during Microsoft Quick User. This functionality allows for group licensing, typically used in large enterprises.
MS Exchange Online User Mailbox Template	These CFTs are used to set default values and import of the MS Exchange user mailbox. The selected CFT then applies to the Microsoft Quick User and **User Profile**. Automate also ships with a default CFT called **Reference MS Exchange Online User Mailbox Template**.
MS Exchange Online Convert Mailbox Template	The CFT you choose for **MS Exchange Online Convert Mailbox Template** is used when the Quick Add Group settings are applied, for example during the Quick Offboard User process if mailbox conversion to a shared mailbox is required. In the default reference CFT for this template type (**Reference MS Exchange Online Convert Mailbox Template**), the **Convert to Type** field also allows the conversion of a mailbox to a regular mailbox.

Note: You can also use the **Update Group Membership** multi-vendor quick action to manage a user's group membership. See *Multi vendor users* and *Enable multi vendor users*.

Related topics

- *Microsoft Licenses* in the Core Feature Guide
- *Microsoft Quick User*
- *Onboard user (Cisco)*
- *Offboarding (Microsoft)*
- *Offboard user (Webex or Microsoft)*
- *Introduction to Microsoft Teams policies* in the Core Feature Guide
- *Onboard user (Microsoft)*
- *Configuration templates* in the Core Feature Guide
- *Field display policies* in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Add a Quick Add Group

This procedure adds a Quick Add Group (QAG).

Note: You can also create a new Quick Add Group by cloning (copying) an existing one, then customizing it for your requirements.

1. Log in as Provider, Reseller, Customer, or Site administrator.
2. Go to **Quick Add Groups**.
3. Click **Add**, then fill out details for the new Quick Add Group.
   - (Mandatory) At **Group Name**, fill out a name for the new Quick Add Group.
   - Fill out a description.
   - Choose the required configuration templates to use in this Quick Add Group.

     Note: Configuration templates (CFTs) available for selection are grouped per vendor scenario. You can choose one or more CFTs for:

     - Cisco UCM and Webex
     - Jabber and Dual-mode
     - CUC (Unity)
     - Webex App
     - Pexip Conference
     - Microsoft
     - Additional services

     If you wish to use the Quick Add Group for user offboarding, select the **Subscriber Offboarding** checkbox so that this Quick Add Group is available for selection when running offboard. Also ensure that the offboarding configuration template is configured to offboard and de-provision as required, and associate the CFT with this Quick Add Group. See *Offboard user (Webex or Microsoft)*
4. Save your changes.

Related topics

- *Onboard user (Microsoft)*
- *Offboard user (Webex or Microsoft)*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Delete a Quick Add Group

The default Quick Add Group resides at the *sys* (system-level) hierarchy node.

Note: A Quick Add Group is required for the Quick User function to work.

1. Go to **Quick Add Groups**.
2. Select the checkbox at the Quick Add Group you want to delete.
3. Click **Delete**, then click **Yes** to confirm.

Quick Add Groups, default model

Default group model for Quick User and Add User Wizard functions:

Title	Field Name	Configuration Template Name
Group		
Group Name*	group_name	N/A
UCM and Webex		
UCM User Template*	default_cucm_user_template	Default UCM User Template Also used for vendor filtering.[1]
Phone Template	default_cucm_phone_template	Default UCM Phone Template
Extension Mobility Template	default_cucm_device_profile_template	Default UCM Extension Mobility Template
Line Template	default_cucm_line_template	Default UCM Line Template
Remote Destination Template	default_cucm_rd_template	Default UCM Remote Destination Template
Remote Destination Profile Template	default_cucm_rdp_template	Default UCM Remote Destination Profile Template
Webex User Template	default_webex_user_template	Default Webex User Template
Jabber and Dual-Mode		
Jabber Android Template	default_cucm_jabber_android_template	Default UCM Jabber Android Template
Jabber CSF Template	default_cucm_jabber_csf_template	Default UCM Jabber CS Template
Jabber iPad Template	default_cucm_jabber_ipad_template	Default UCM Jabber iPad Template
Jabber iPhone Template	default_cucm_jabber_iphone_template	Default UCM Jabber iPhone Template
Carrier Integrated Mobile Device Template	default_cucm_jabber_cim_template	Default Carrier Integrated Mobile Device Template
CTI Remote Device Template	default_cucm_jabber_ctird_template	Default CTI Remote Device Template
CUC(Unity)		

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

Title	Field Name	Configuration Template Name
CUC User Template	default_cuc_user_template	Default CUC User Template
CUC User Password Template	default_cuc_user_password_template	Default CUC User Password Template. Quick User applies this template and overrides CUC user template settings on CUC.
CUC User PIN Template	default_cuc_user_pin_template	Default CUC User PIN Template. Quick User applies this template and overrides CUC user template settings on CUC.
Webex App		
Default Webex App User Template	default_spark_user_template	Default Webex App User Template
Default Webex App Calling Template	default_spark_calling_template	Default Webex Teams Calling Settings Template Also used for vendor filtering.[Page 1394, 1]
Default Webex App User CTI Device Template	default_spark_user_cti_device_template	Default Webex App User CTI Device Template
Default Webex App User iPhone Device Template	default_spark_user_iphone_device_temp	Default Webex App User iPhone Template
Default Webex App User Android Device Template	default_spark_user_android_device_tem	Default Webex App User Android Template
Default Webex App User Tablet Device Template	default_spark_user_tablet_device_templ	Default Webex App User iPad Template
Default Webex App User CSF Device Template	default_spark_user_csf_device_template	Default Webex App User CSF Template
Default Webex App Wholesale for wholesale user	default_webex_app_wholesale_template	E.g. Default Webex Wholesale user - webex_calling for Webex calling package. Any package can be set and only wholesale package templates are available to be set. A template must be set for wholesale customers.
Pexip Conference		
Pexip Conference Template	default_pexip_conference_template	Reference Pexip Conference Template
Microsoft		
MS 0365 User Template		Also used for vendor filtering.[Page 1394, 1]
MS Teams User Template		Also used for vendor filtering.[Page 1394, 1]
MS Groups Add Template		Add one or more entries to the Group list to provide group membership to a user.[2]

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

Title	Field Name	Configuration Template Name
MS Groups Remove Template		Add one or more entries to the Group list to remove group membership from a user.[Page 1394, 2]
MS Exchange Online User Mailbox Template		Used for default MS Exchange user mailbox settings.
Additional Services		
Phone User Template		

Fields marked with * are mandatory.

Quick Add Groups and vendor filtering

Quick Add Group selection in the Automate portal takes place for Quick User management. In these cases, the list of available Quick Add Groups to select will be filtered in accordance with populated entries in the Quick Add Groups themselves.

The following list shows the corresponding Quick Add Groups fields to allow filtering for each activity:

- Cisco Quick User: **UCM User Template**
- WebexApp Quick User: **Default Webex App Calling Template**
- Microsoft Quick User: **MS 365 User Template** and **MS Teams User Template**

12.1.6. User profiles

Tip: *Use the Action search to navigate Automate*

Overview

User profiles allow you to group a number of services and resources into a profile that you can assign to a user via Quick Add Group (QAG) templates. The user profile can then for example be added to the QAG along with other configuration settings.

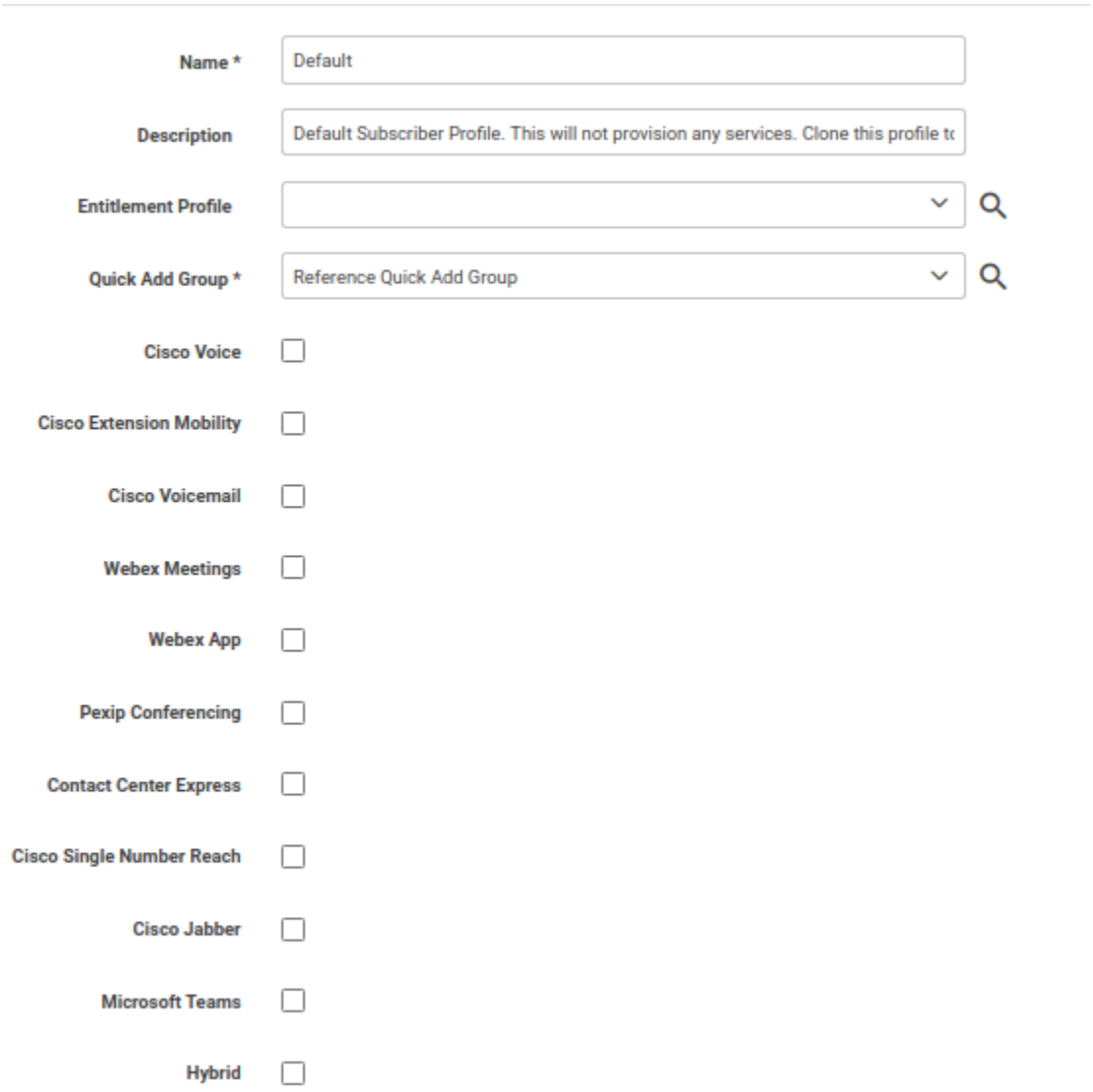
User profiles are used in the Admin Portal.

Flow through provisioning uses the user profiles to assign services to users once they're synced in and moved to the sites. This is useful where you need to assign different sets of services to different categories of users, depending on their job role, for example IT or Sales.

Important: A *Default* user profile is created at system (`sys`) level. Only a system level administrator may delete the system-level default profile. To add a new user profile, it is recommended that you clone (create a copy) of an existing user profile and create the new profile based on a valid (working) Quick Add Group.

[1] See: *Quick Add Groups and vendor filtering*.
[2] See: *Licensing Users for MS Teams and Teams Phone by Group Membership*.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Configure user profile

This procedure adds, edits, or deletes a user profile.

1. Go to the **User Profiles** page.
2. Choose an option:
   - To update an existing user profile, click on a profile in the list view. Go to step 3.
   - To delete an existing user profile, select the profile in the list view, and click **Delete**.
   - To add a new user profile, click **Add**. Go to step 3.
3. To add or update a user profile settings, configure fields on the form, then save your changes.

   The table describes options for configuring user profiles:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Entitlement profile	Select an entitlement profile to define the resources and services that may be assigned to a user.
Quick Add Group	The quick add group (QAG) defines the configuration templates to be used during service provisioning. QAGs are also used for Quick Add User (Cisco UCM and Microsoft).[1] Where the selected QAG contains details of MS Groups templates, flow-through provisioning will also assign or remove any MS licenses accordingly.[2]
Cisco Voice	Assigns voice services. When enabled, a desk phone is created. The phone template in the QAG defines the phone type.
Cisco Extension Mobility	The template in the QAG defines settings for extension mobility. The extension mobility template defines the device types available in the drop-down, and the selected device types define the available configuration settings. The default for **Line** is the first user line. User details define the values in **Line Label** and **Line Display**. Only one device profile can be added for extension mobility in VOSS Automate. If a user is associated with two or more extension mobility profiles on the Cisco UCM, and you sync with Automate, only the first extension mobility profile displays on the **Users** list view in Automate.
Cisco Voicemail	Assigns voicemail service for the profile. When enabled, and the service is added, the user can be added as a voicemail user.
Webex Meetings	Allows Webex service.

Field	Description
Webex App	A Webex App user profile may be chosen for the profile. In this case, the user profile defines the Webex App service that will be provisioned. When Webex App is enabled for the user profile, the user can be added as a Webex App user when the service is added.
Contact Center Express	When enabled, an agent profile may be chosen for the profile. In this case, you also need to choose the device type to use as the agent's controlled device. When adding the service, the user default extension displays, as well as (depending on the selected controlled device type - phone or extension mobility), the user's phone or device profile.

[1] The list of available Quick Add Groups are filtered by vendor (see *Quick Add Groups and vendor filtering*). The list of available Quick Add Groups (and user profiles) are restricted to those available at a selected hierarchy, based on the option selected for **Quick Add Group & User Profile lookup level** in the General Settings of the Global Settings. See *Global settings*.

[2] See *Microsoft licenses* in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Cisco Single Number Reach	Choose whether to include single number reach (SNR) service for the profile. Only one remote destination profile may be added for single number reach. If a mobile number has already been configured for a user, it is used to pre-populate the **Mobile Number** field when adding SNR for that user. You can enter a different mobile number for SNR, if required.
Cisco Jabber	Choose whether to include Jabber service, and one or more Jabber device types.
Microsoft Teams	Allows Microsoft services.
Hybrid	Allows Cisco and Microsoft services. Selecting this checkbox displays: • The **Hybrid Service** drop-down field to select a Service Type that is available from the list of Multi Vendor Service Definitions. This Service Type will then be applied when the user profile is used.[3] • The **Class of Service** drop-down field is exposed. Default value is empty.

Note: When both Microsoft Teams and Hybrid are selected in the user profile, the Hybrid Quick Add User steps are skipped when adding a user.

Related Topics

- *Flow through provisioning (FTP)*
- *Global settings*
- *Microsoft licenses* in the Core Feature Guide
- *Hybrid service definitions*

12.1.7. Flow through provisioning (FTP)

Tip: *Use the Action search to navigate Automate*

[3] See: *Hybrid service definitions*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate's Flow Through Provisioning (FTP) feature enables auto-provisioning of users and services without manual administrative input, during user sync from devices. When users are synced into Automate, their user records are inspected and attributes are evaluated against predefined criteria, checking for matching criteria to determine if they should automatically receive telephony services, phone numbers, group memberships, and more.

Note:

- Sync with flow through provisioning supports Cisco Webex, Microsoft, and several additional scenarios, including LDAP top down and LDAP/CUCM bottom up. While the legacy sync, move, and provisioning functionality remains available for compatibility purposes, flow through provisioning is the recommended procedure.
- Flow through provisioning *Add* syncs enable complete onboarding of users, while an update sync is available for Microsoft users that already exist at site level, to move these users from one site to another when changes are detected on their user records in Azure.

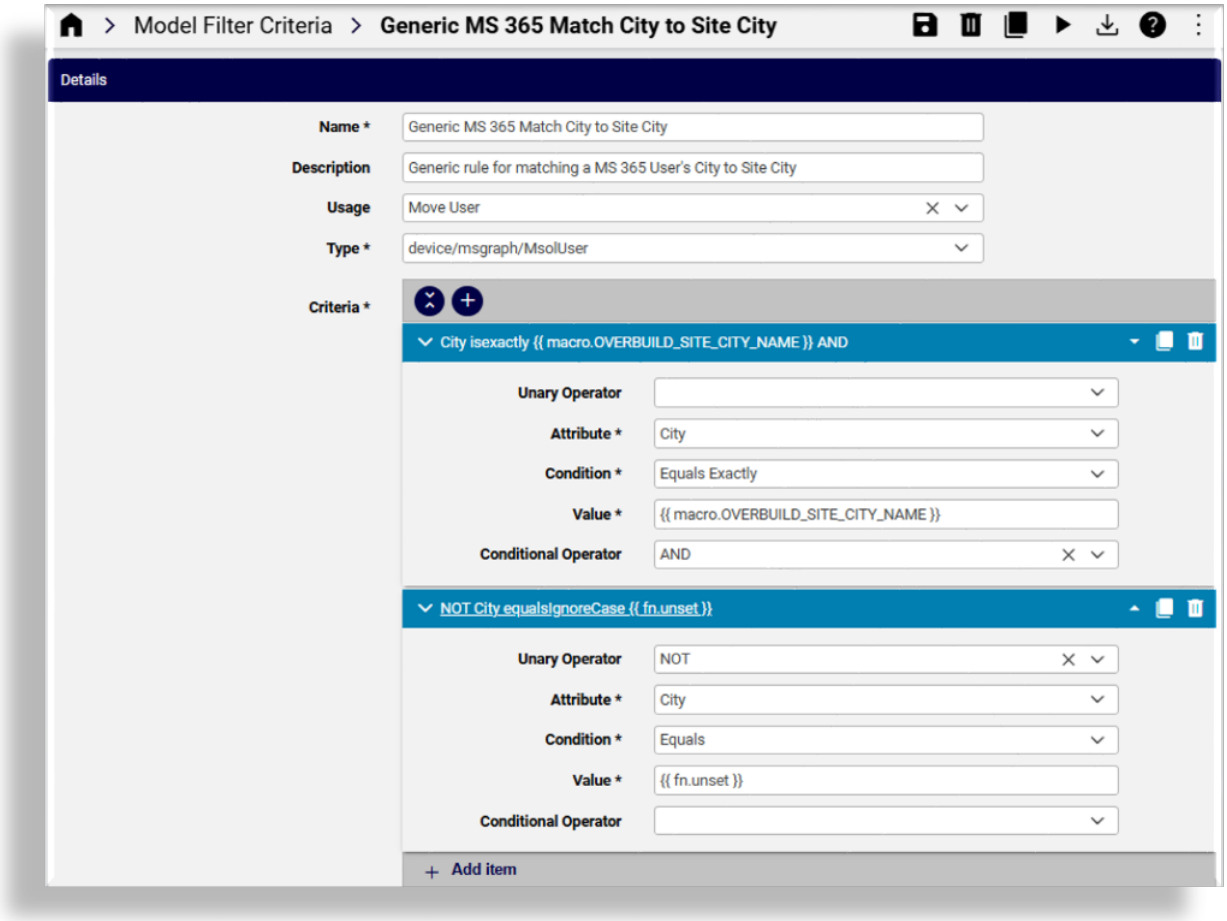
FTP Example Scenario: Acme Corp

Consider a fictional company, *Acme Corp*, which uses Microsoft Voice Services for their employees. As a global organization experiencing rapid growth, Acme's IT and Voice Services teams face increasing pressure to provision new employees efficiently and to keep up with changing roles and functions for existing employees. Traditionally, Automate admins would manually assign users to sites and apply profiles that provisioned their services and numbers. With *Flow Through Provisioning*, even these steps can be automated, eliminating the need for manual intervention entirely.

How it works

Administrators provide logic to determine how new users should be processed automatically, using model filter criteria and flow through provisioning criteria.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Example: New MS 365 user, Joe Adams, has their City attribute set to "Chicago", and they're in the "Engineering" department.

- The admin creates model filter criteria with:
  - **Usage** set as *Move User*
  - **Criteria** attribute set to *City*, with a value of "Chicago".

  In the Site Defaults for the Chicago site, select this model filter criteria for Joe's user type (MS 365 in this case).

  Automate now has instructions to automatically move any users synced in to the Chicago site, if they have matching criteria (City value of "Chicago").
- The admin can create model filter criteria with:
  - **Usage** set as *Flow Through Provisioning*
  - **Criteria** attribute set to *Department* with a value of "Engineering".

  This model filter criteria, combined with a pre-existing user profile used to provision "Engineering" users, can be used to set up the flow through provisioning criteria.

Criteria is now defined to match user locations based on their "City", and to match user persona, based on their "Department".

Finally, the administrator must enable automatic provisioning in the Global Settings:

In the **Global Settings**, on the **Flow Through Provisioning** tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

1. Set **Enable Move & Flow Through Provisioning** to *Yes*.
2. Set **Enable Move & Provisioning (Add Sync)** to *Yes*.
3. At **Flow Through Provisioning Criteria (Add Sync)**, select the criteria created to match "Engineering" users.

Once enabled, Automate will:

- Inspect any Microsoft users synced in to Automate for **City** attribute matching "Chicago".
- Move users with a **City** value of "Chicago" to the Chicago site.
- Only after a user is moved to a site, their "Department" is evaluated for provisioning.

Flow through provisioning is triggered only *after* a user is matched and moved to a site. Any combination of model filter criteria with **Usage** set to *Move* and *Flow Through Provisioning* can be configured to automatically move users to their respective sites and to automatically provision users at sites, with a profile that matches their provisioning criteria. No further administrator involvement is needed, provided sufficient licenses are available, and that settings such as profiles and numbers are correctly configured and assigned.

Related topics

- *Flow through provisioning onboard users (Add sync)*

Flow through provisioning onboard users (Add sync)

This section describes the steps for setting up your system to enable a seamless sync in of users to Automate from the hierarchy where the sync source device is set up (typically, Customer level), and the flow through provisioning of services to users at your sites.

- To move users to sites, the flow through provisioning references move filter criteria, and attributes set up as *Model filter criteria* (such as a user's department, division or city address).

  Flow through provisioning uses the move filter criteria in the site defaults (SDD) to determine whether to move users to site. Flow through provisioning won't run if the user is not moved to the site.

- To create a user and provision resources and services, the flow through provisioning references user profiles. See *User profiles*.

  You will need a user profile and Quick Add Group (QAG) with device configuration templates (CFTs) set up before using FTP.

- Each flow through provisioning criteria (one per customer) consists of one or more pairs of model filter criteria, and a user profile.

Related topics

- Model filter criteria in the Core Feature Guide
- User profiles in the Core Feature Guide
- LDAP integration in the Core Feature Guide
- Add CUCM server in the Core Feature Guide
- CUCM configuration in the Core Feature Guide
- Microsoft overview in the Core Feature Guide
- Sync to site with flow through in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Sync Webex App users with flow through provisioning in the Core Feature Guide
- Global Settings in the Core Feature Guide
- Site defaults in the Core Feature Guide
- Introduction to role-based access control in the Core Feature Guide
- *Flow through provisioning move users (Update sync)*

Flow through provisioning workflow

Copyright © 2025 VisionOSS Limited. All rights reserved.

Before you start: Add a server as sync source

Users are imported from the server sync source to the Customer level in Automate. The flow through provisioning is generic functionality and supports a number of scenarios, including Microsoft, LDAP, CUCM, Cisco Webex and other models (depending on predefined model criteria).

Note: See the Core Feature Guide for details around adding and setting up a server for your flow through provisioning scenario. For example, see *Microsoft Quick Start Guide for Automate*, *LDAP server*, *Cisco UCM servers*

Step 1: Add model filter criteria

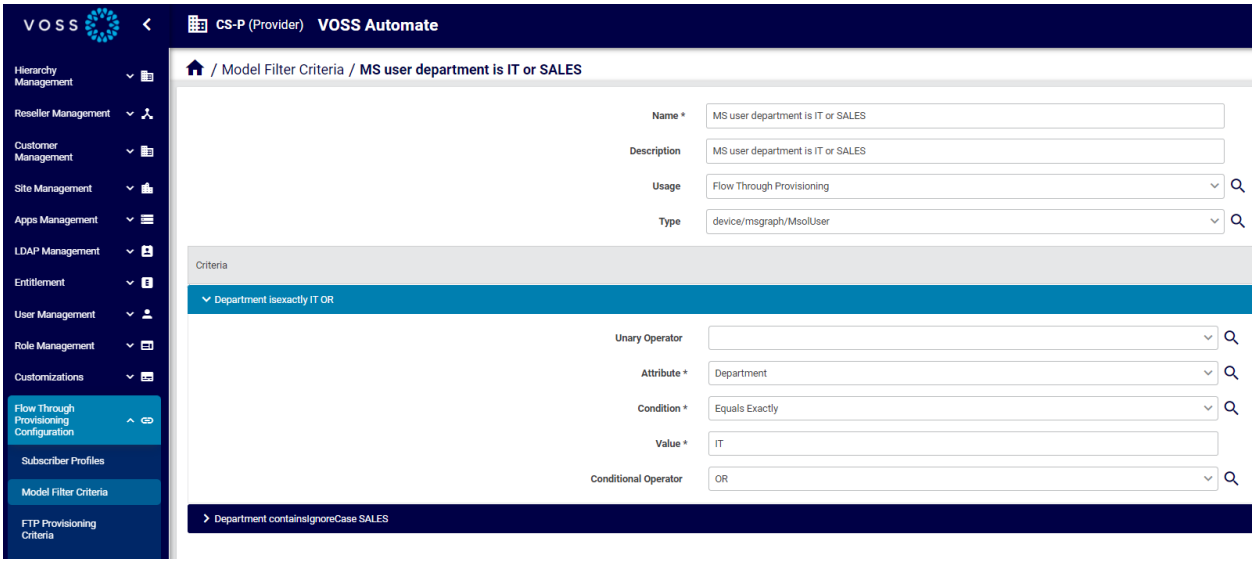
Flow through provisioning references model filter criteria set up for each user type (for example, Microsoft, LDAP, or CUCM).

When setting up the *Model filter criteria*, you will specify usage, either flow through provisioning, or move user:

- To move a user to the site on import, configure model filter criteria with **Move User** selected as the value for the **Usage** field.
- To provision a user once they're at the site, configure model filter criteria with **Flow Through Provisioning** selected as the value for the **Usage** field.

  Note:

  – The flow through provisioning process runs only if the user is at the site.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Model filter criteria*

Step 2: Add user profiles

Flow through provisioning uses the user profile to determine the services to be assigned to a user once they're moved to the site.

Related topics

- *User profiles*

Step 3: Add flow through provisioning criteria

Flow through provisioning criteria is a type of model filter criteria used for provisioning. One named flow through provisioning criteria can be added at each Customer level.

Each flow through provisioning criteria is a collection of one or more pairs of model filter criteria and user profile combinations. The flow through provisioning criteria defines how users are matched to both sites and user profiles, allowing the tool to seamlessly move users to the sites (based on model filter criteria) and to create a user and assign services from the user profile.

Flow through provisioning uses the first match to execute the move and service assignment operation.

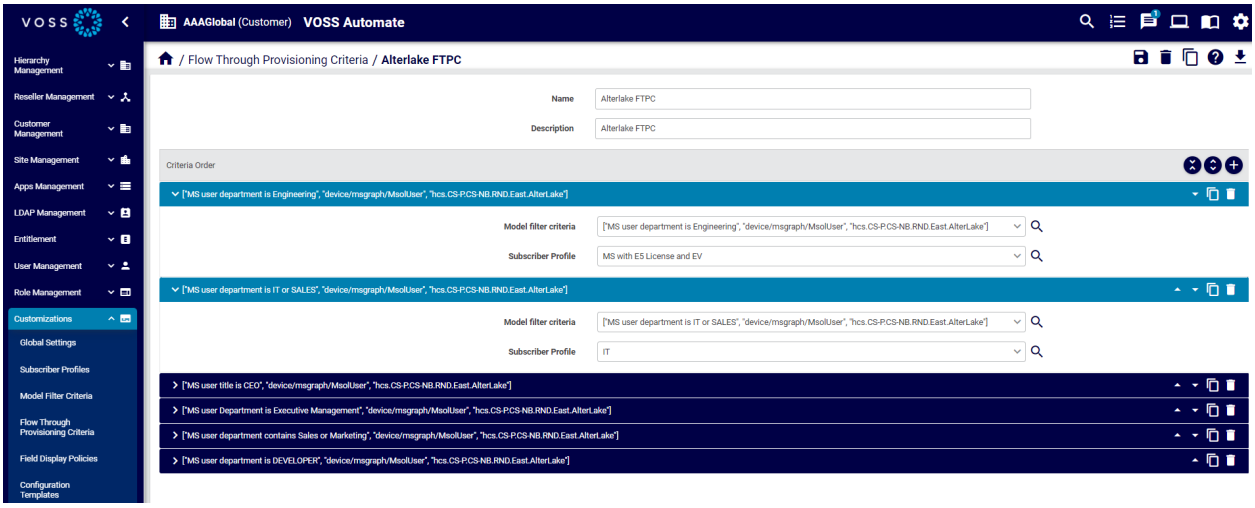
You can use a single flow through provisioning criteria to match any number of user profiles for this customer and its sites. For example, if you have ten different user profiles, you can add ten pairs of model filter criteria and user profile combinations.

Note: Flow through provisioning criteria is configured via the **Flow Through Provisioning Criteria** page.

Before setting up flow through provisioning criteria, configure the following:

- Server sync source
- *Model filter criteria*
- *User profiles*

Copyright © 2025 VisionOSS Limited. All rights reserved.



Step 4: Choose move criteria

To allow users to be moved in a flow through provisioning, you need to choose move filter criteria for the user type (Microsoft, LDAP, and/or CUCM). Move filter criteria defines how the system moves users to the correct site once they're synced in; that is, it matches each user to the relevant site.

Note: The system uses the existence of the move filter criteria from the site defaults to determine if the user must be moved. Flow through provisioning will not work if a user is not moved to a site.

Prerequisites:

- Server sync source
- *Model filter criteria* (set Usage field to **Move User**)
- *User profiles*
- Flow Through Provisioning Criteria

To choose move criteria . . .

1. Select the relevant site hierarchy.
2. Go to the **Defaults** page.
3. On the **Move Filter Criteria** tab, choose the criteria for the user types you're importing (Microsoft, LDAP, and/or CUCM).
4. Save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Step 5: Enable flow through provisioning

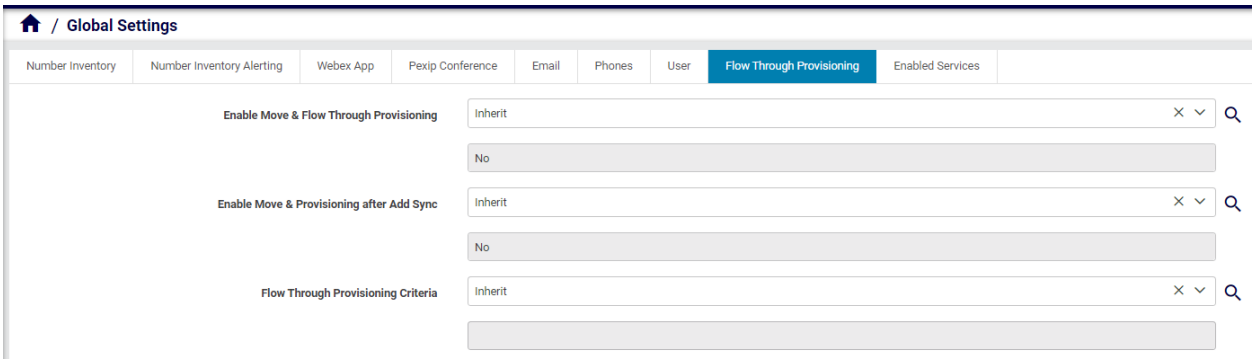
Enabling your system for flow through provisioning in the Global Settings allows Automate to perform a seamless sync in, to move users to the correct site (based on move filter criteria and model filter criteria), and to provision these users with appropriate services (based on the user profile).

Prerequisites:

- Server sync source
- *Model filter criteria*
- *User profiles*
- Flow through provisioning criteria
- Move criteria selected

To enable flow through provisioning . . .

1. Log in to the Admin Portal as Provider admin or higher.
2. Set the hierarchy to the level where the sync source device is installed. Typically, this is at the customer.
3. Go to **Global Settings**, then select the **Flow Through Provisioning** tab.
4. At **Enable Move & Flow Through Provisioning**, select **Yes**.
5. At **Enable Move & Provisioning after Add Sync**, select **Yes**.
6. At **Flow Through Provisioning Criteria**, choose the flow through provisioning criteria to use at the customer level (for all sites at the customer).
7. Save your changes.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Step 6: Sync with flow through provisioning

This section describes the general workflow in a generic sync with flow through provisioning.

You can run the sync directly, or via a schedule.

Ensure you have the following set up before a sync:

- Server sync source
- *Model filter criteria*
- *User profiles*
- Flow through provisioning criteria
- Move criteria selected

Sync with flow through provisioning workflow steps

The flow through provisioning workflow is executed per user and runs in parallel:

1. Imports user.
2. Creates a corresponding LDAP user (for LDAP scenario), and a local VOSS user.
3. Moves users to the sites (based on model filter criteria). If no criteria in place, user remains at Customer level.
4. Updates the user's role for the site.
5. Executes *Add User from Profile* to create the user, and checks the flow through provisioning criteria to match it to a user profile.
6. Provisions the users with appropriate services, from the user profile.
7. Sends a welcome email to users if the following applies:
   - The global setting to allow an email message to be sent to a user is enabled. See the *Email Tab* topic at *Global settings*.
   - An SNMP server has bee set up. See *Add a SMTP Server*.
   - The user has an email address.

   See also *Email HTML templates*.

You can monitor the progress of the transaction via the Transaction Log. When complete, verify the user's move and provisioning status:

1. Go to the **Users** list view and verify that synced in users are at the correct sites.
2. On the **Users** list view, check that users exist at the sites, with relevant services.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Flow through provisioning move users (Update sync)

This section describes an update sync with flow through provisioning that is designed to sync in changes on user accounts from Microsoft Azure to move users from one site to another.

Note: The update sync with flow through only supports moving users that already exist at a site, to move these users from that site to another site. To onboard new users with flow through provisioning in an *add* sync, see *Flow through provisioning onboard users (Add sync)*.

Handling updates and user moves

Flow through provisioning supports dynamic updates. For example, scenarios where users are frequently moved between locations and their assigned number or settings must be re-configured.

In this case, in the **Global Settings** (**Flow Through Provisioning** tab/panel), set **Enable Move & Provisioning (Update Sync)** to *Yes* to allow Automate to re-evaluate existing users at the site level for attribute changes.

For example, if user Jane Murphy's city changes from "Chicago" to "Dallas" in Microsoft Entra, the next time a sync occurs, Automate searches for any site with matching model filter criteria in the Site Defaults Doc, and a matching city value. If it finds a match, Jane is moved to the "Dallas" site along with all their services.

Additional controls for number assignment and settings

Admins have the ability to control default behavior for the assignment of numbers and for the user's services and configured settings during user moves in update syncs:

- **Number Assignment Control (Update Sync)**:
  - **Assign New Number** (default)
  - **Keep Existing Number** (for edge cases)
- **User Profile Control (Update Sync)**:
  - Select the user profile to be applied after a move.
  - When onboarding in an *add* sync, a user profile defines settings and services for new users. In an *update* sync for moving existing users, a user profile is configured for the services and settings to be assigned once they're moved to the new site.

To move Microsoft users between sites in an update sync with FTP

1. Configure model filter criteria to use in the user profile for the move in an update sync.
2. Configure the default user profile to apply after a move in the update sync.
3. Enable flow through provisioning on update sync in the Global Settings:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Global Settings in the Core Feature Guide

12.1.8. Manage number filters

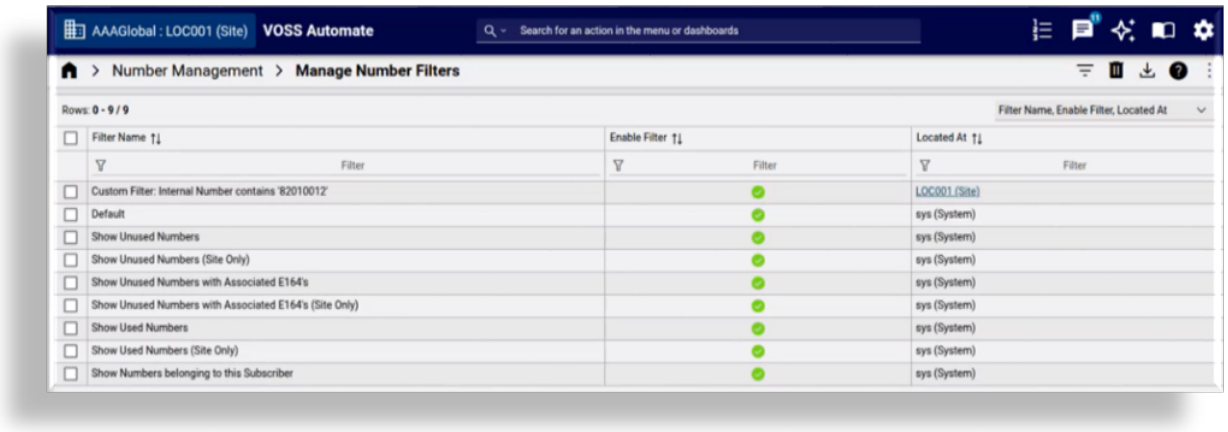
Tip: *Use the Action search to navigate Automate*

Overview

Automate ships with a collection of pre-defined, read-only filters for the number inventory (shipped filters), and allows an administrator to also create their own *Custom inventory filters*. When filtering is enabled at the hierarchy you're working at, number inventory filters can be selected to filter numbers from the number inventory for specified criteria.

Note: Shipped number inventory filters are located at the system level (*sys*) and cannot be disabled, enabled, or renamed. If you wish to enable or disable a shipped filter, you will need to clone that filter to a lower level of the hierarchy. The cloned shipped filter then becomes a custom number inventory, but it cannot be renamed.

The image shows the **Manage Number Filters** page with a collection of custom and shipped inventory filters.



Applying a number inventory filter means that when assigning a number during onboarding or provisioning, you'll be able to select from a smaller selection of relevant numbers. Additionally, when used with **Use next available line**, the system can use the next available line from a filtered selection of numbers.

Note: When using **Use next available line** functionality, the system prioritizes local numbers (numbers available at the current site) before checking for available numbers from higher levels in the hierarchy. If the user has *reserved numbers*, these are excluded and won't be applied as the *next available line*.

Inventory filtering functionality in Automate can be summarized as follows:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Shipped filters cannot be enabled, disabled, or renamed. To enable or disable shipped inventory filters you'll need to clone the shipped filter to a lower hierarchy, effectively creating a new custom filter, but you won't be able to rename it.
- Filtering is enabled by default, and only custom inventory filters can be disabled at specific hierarchies
- Provided filtering is enabled at the hierarchy you're working at, number inventory filters are available anywhere in the GUI where line filtering exists, for example, Quick Add User.
- Only the read-only shipped filters are available until you create your own custom filters
- You can only enable or disable custom filters at a hierarchy, for example, at a specific site
- Filtering is integrated with **Use next available line**.

Related topics

- *Enable/disable filtering*
- *Create a custom inventory filter*
- *Inventory filters and "Use next available line"*

Shipped inventory filters

Shipped number inventory filters are available at install, located at the system level (*sys*), and are enabled by default. Shipped filters are pre-defined and read-only. To disable shipped filters at specific hierarchies you will need to clone the shipped filter down to a lower hierarchy and then disable the clone at that hierarchy. Shipped filters can't be modified or renamed. Only the shipped inventory filters are available for your system until you create custom inventory filters.

Automate's collection of shipped inventory filters are the following:

- Show unused numbers
- Show unused numbers (site only)
- Show unused numbers with associated E164s
- Show unused numbers with associated E164s (site only)
- Show used numbers
- Show used numbers (site only)
- Show numbers belonging to this subscriber

As an example use case scenario for shipped inventory filters, let's say you wish to see only numbers reserved for or belonging to a user you're provisioning, in this case, you can select the shipped inventory filter, **Show numbers belonging to this subscriber**. For details around *reserved for* numbers, see *Reserve numbers for a user*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Custom inventory filters

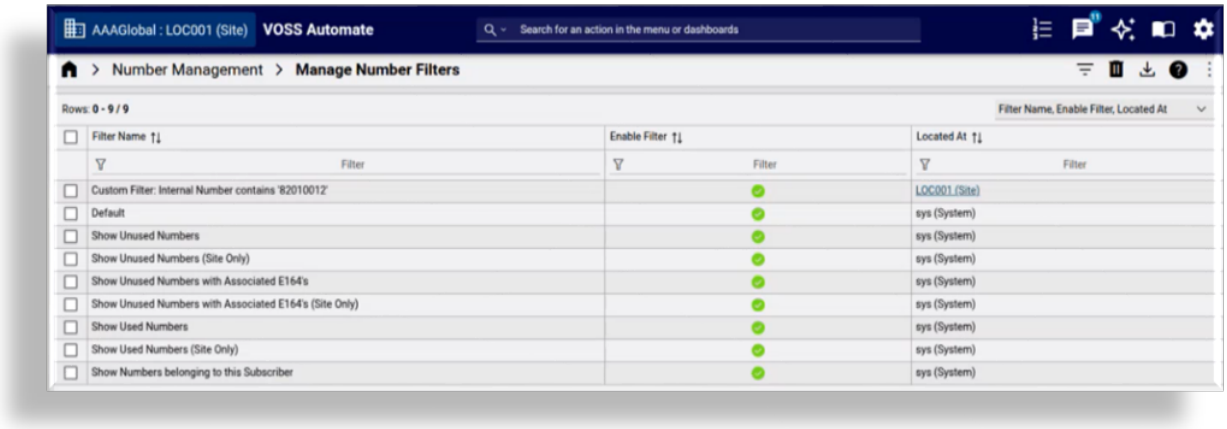
Automate allows administrators to create their own customized number inventory filters to define the numbers that will be available for selection in drop-downs where lines are provisioned, such as Quick Add User. For example, you may want to make available only Microsoft numbers at a particular site, or to display only a selection of numbers greater than or equal to a specified value, for example, to display only numbers greater than or equal to *820100001*.

Whereas shipped inventory filters are located at the system level (*sys*) and available at all hierarchies, custom inventory filters are created at the hierarchy you're at and are only available at that hierarchy. For example, when a Provider admin creates a custom inventory filter at a particular site, that custom inventory filter is located at that site and can only be used at that site. A system administrator can however create custom inventory filters at *sys* level.

The image shows the **Manage Number Filters** page with a collection of custom and shipped inventory filters. The custom inventory filters *Located At* value indicates the hierarchy where the inventory filter was created, *site* in this case. Green checkmarks indicate enabled inventory filters. You can click on a custom inventory filter in the list to enable or disable it, or to rename the custom inventory filter.

Note: A custom inventory filter cannot be given the same name as a shipped inventory filter as the settings of the shipped inventory filter will then override any settings you configured for the custom inventory filter. In this case, you will need to rename your custom inventory filter. However, if the custom inventory filter is a clone of a shipped filter, this filter cannot be renamed as it is still owned at *sys* level.

The name of a custom inventory filter must be unique at the hierarchy where it's located.



Custom inventory filters and saved search

Custom inventory filters are created at the hierarchy you're at when creating the filter, and can be used by any user at that hierarchy, provided the custom inventory filter is enabled at that hierarchy, at a specific site for example. Saved searches however, are personal filters created at the user's hierarchy and are only available at that hierarchy, for example, if a provider admin creates a saved search, that saved search is only available at the provider hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Global settings*

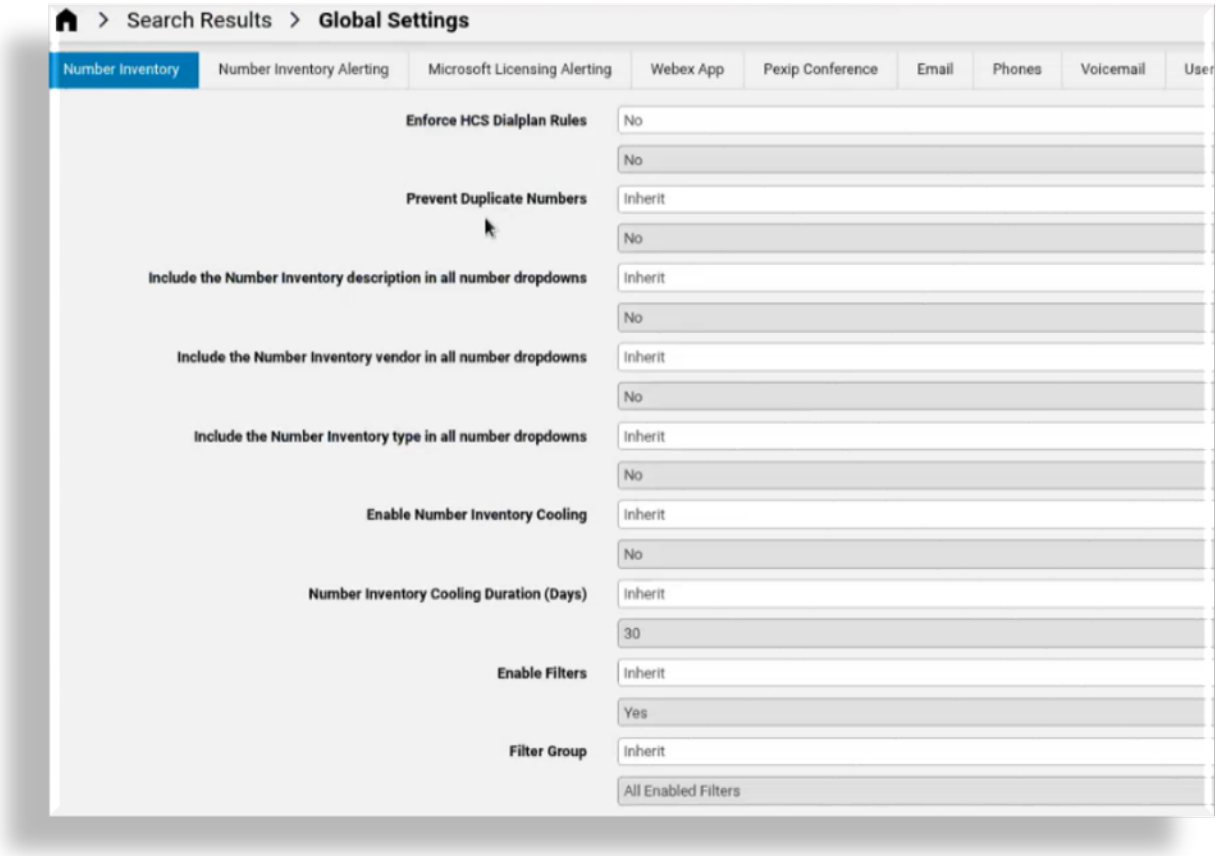
Enable or disable filtering and inventory filters

Filtering is enabled/disabled via *Global settings* (**Number Inventory** settings). By default, inventory filtering is enabled in Automate but can be disabled (custom inventory filters only) at selected hierarchies or at system level.

You'll need to ensure that filtering is enabled at the hierarchy you're working at to use the custom inventory filters in the drop-downs where lines are provisioned at that hierarchy, such as Quick Add User.

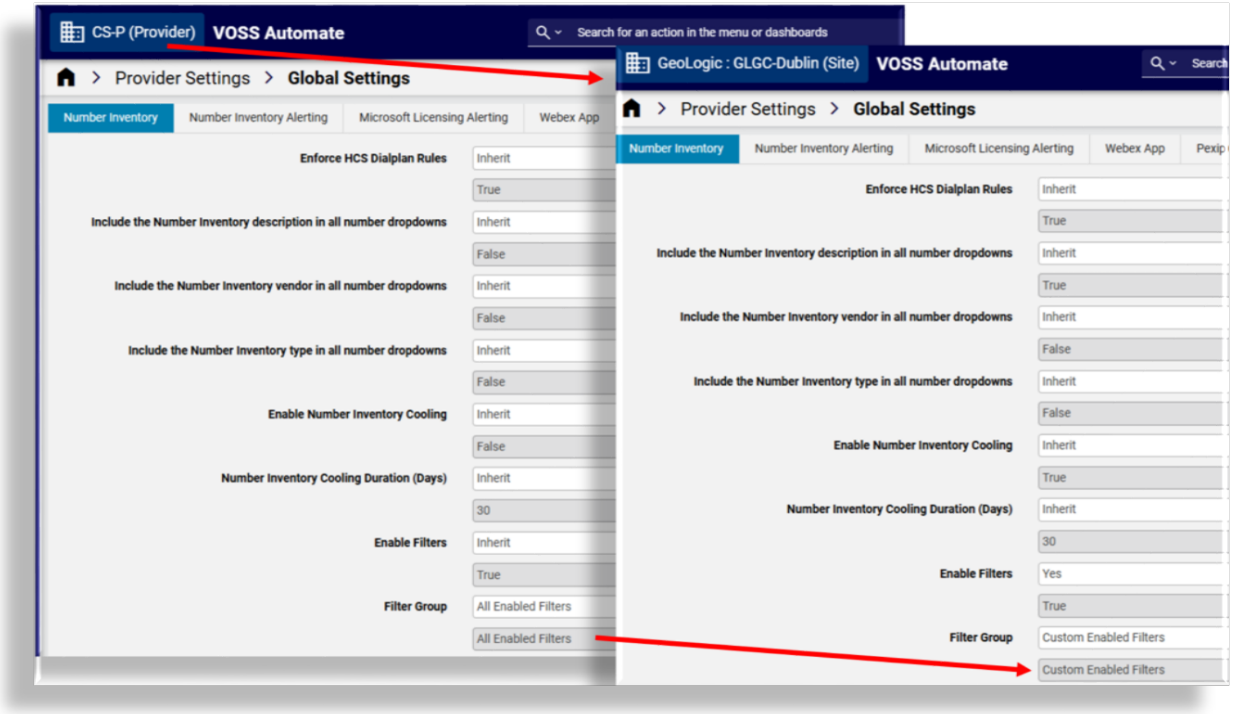
When enabling number inventory filtering, you can choose to make all enabled inventory filters available (custom and cloned shipped inventory filters), or only shipped inventory filters. Specific custom or cloned shipped inventory filters at a hierarchy can also be disabled. For example, you may want to make some cloned shipped inventory filters available at a particular site and not at others.

Note: All inventory filters are enabled at a hierarchy until you disable them. Only the read-only shipped inventory filters are available until you add custom inventory filters.



The image displays inventory filters enabled at Provider level with the filter group set to *All Enabled Filters*, while at a specific site, only *Custom Enabled Filters* will be available in the drop-downs.

Copyright © 2025 VisionOSS Limited. All rights reserved.



In **Manage Number Filters**, an administrator can enable or disable one or more cloned shipped filters or custom filters. In this case, even if the selected filter group is *All Enabled Filters*, you may want to disable specific cloned shipped or custom inventory filters at certain hierarchies.

Enable/disable filtering

This procedure enables or disables inventory filter functionality via the Global Settings in Automate.

Note: Custom and shipped inventory filters available at a hierarchy can be viewed and managed (enabled/disabled) via *Manage number filters*, at that hierarchy.

---

1. In the Admin Portal, set the hierarchy to the level where you want to enable or disable inventory filters.
2. Go to *Global settings*.
3. On the **Number Inventory** tab/panel, at **Enable Filters**, choose an option:

Option	Description
Inherit	Sets the current hierarchy to use the setting from higher up in the hierarchy. The value for **Filter Group** then displays the value that will be used.
Yes	Default. Enables inventory filtering at the current hierarchy and exposes the **Filter Group** drop-down, where you can select the type of inventory filtering.
No	Disables inventory filtering (custom filters only) at the current hierarchy.

4. At **Filter Group**, select the type of inventory filters you wish to use at the current hierarchy. Options are:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Inherit
- Custom Enabled Filters
- Shipped Enabled Filters
- All Enabled Filters (default)

Note: The filter group value is populated based on the inherited setting if you've selected *Inherit*. See *Global settings*. Only shipped inventory filters display until you've created custom inventory filters at this hierarchy.

5. At **Include the Number Inventory description in all number drop-downs**, define whether to include a description for numbers displaying in the drop-downs.
6. At **Include the Number Inventory vendor in all number drop-downs**, define whether to include the vendor along with the number in the drop-downs.
7. At **Include the Number Inventory type in all number drop-downs**, define whether to include the type of the number in the drop-downs.
8. Save your changes.

   Once the transaction completes and you've set **Enable Filters** to *True*, users will have the option to choose from the selected collection of inventory filters when assigning a line.

Related topics

- *Global settings*

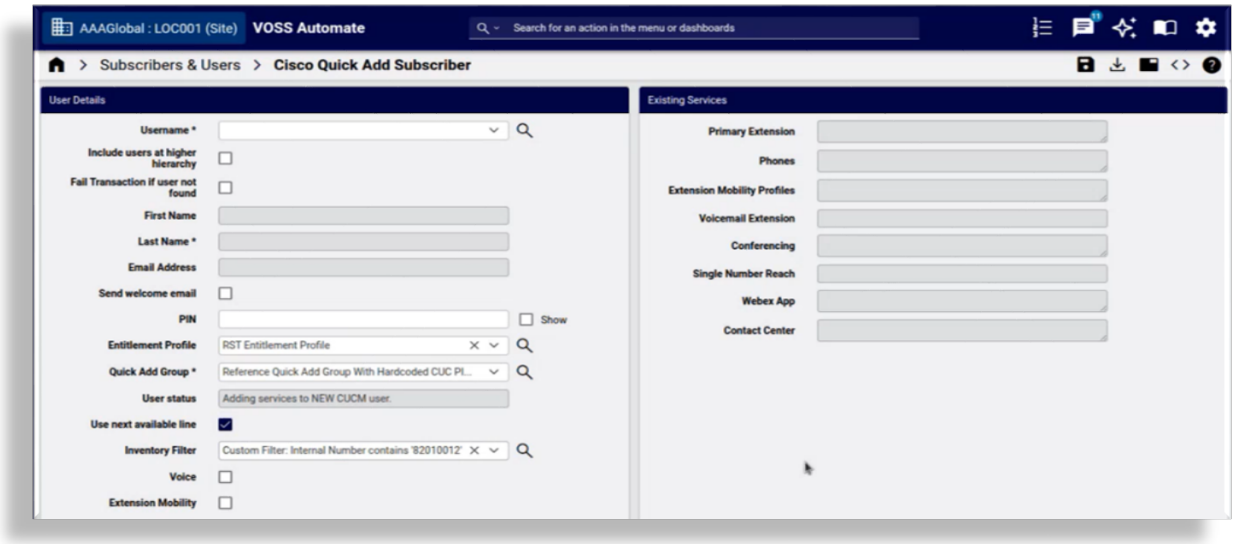
Inventory filters and "Use next available line"

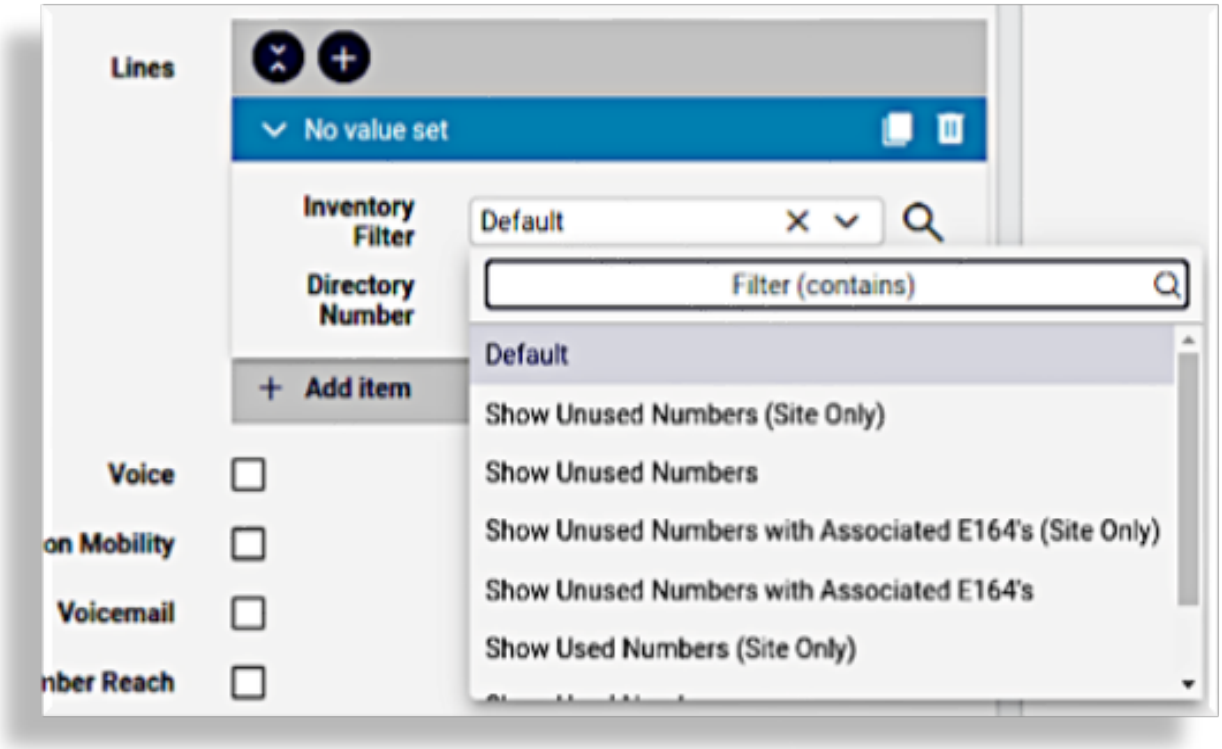
Custom and shipped inventory filters can be used with *next available line* functionality. When enabling **Use next available line** for provisioning, you can select a custom or shipped inventory filter to allow the system to choose the *first available line* from the collection of filtered numbers in the number inventory.

Note: By default, **Use next available line** is disabled (checkbox is clear) and inventory filtering is enabled.

When using **Use next available line** functionality, the system prioritizes local numbers (numbers available at the current site) before checking for available numbers from higher levels in the hierarchy. If the user has *reserved numbers*, these are excluded and won't be applied as the *next available line*.

Copyright © 2025 VisionOSS Limited. All rights reserved.





The table describes how **Use next available line** is integrated with inventory filtering:

Note: When using **Use next available line** functionality, the system prioritizes local numbers (numbers available at the current site) before checking for available numbers from higher levels in the hierarchy. If the user has *reserved numbers*, these are excluded and won't be applied as the *next available line*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
“Use next available line” - ENABLED / Filtering - ENABLED	• Select an inventory filter. • The system selects the first available line from the filtered subset of available lines included from the filter.
“Use next available line” ENABLED / Filtering DISABLED	The system automatically selects the next available line from the number inventory.
“Use next available line” DISABLED / Filtering DISABLED	Select a line from an unfiltered list of available numbers in the **Directory Number** drop-down.
“Use next available line” DISABLED / Filtering ENABLED	• Expand **Lines**. • Select an inventory filter • Select a number from **Directory Number**

View shipped and custom inventory filters

You can view and manage all number inventory filters via the **Manage Number Filters** list view.

- Shipped inventory filters are located at the system level (*sys*) and are by default available to all hierarchies. Only cloned shipped inventory filters can be enabled or disabled via **Manage Number Filters** but the inventory filter name is read-only and can’t be changed.
- Custom inventory filters are created at and then located for and at a particular hierarchy level, for example, a custom inventory filter created at a site is only available at that site (if enabled). Custom inventory filters can be deleted and updated via **Manage Number Filters**, where the name can be changed and the inventory filter can be enabled or disabled.

Copyright © 2025 VisionOSS Limited. All rights reserved.

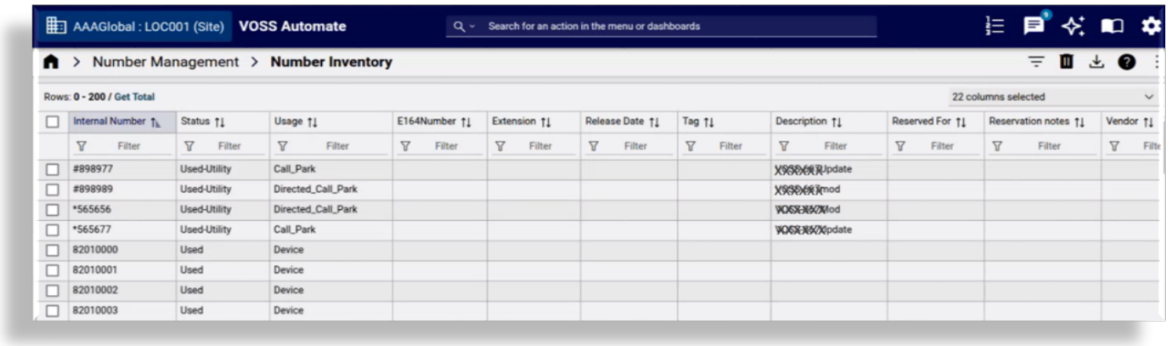
Create a custom inventory filter

This procedure creates a custom inventory filter at a specified hierarchy level.

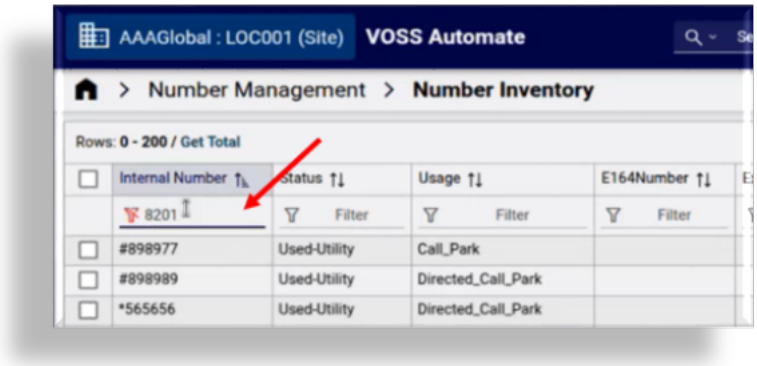
1. In the Admin Portal, set the hierarchy to the path where you want to create the inventory filter.

   Note: The custom inventory filter will only be available at the hierarchy where it's created.

2. Go to the **Number Inventory** list view.

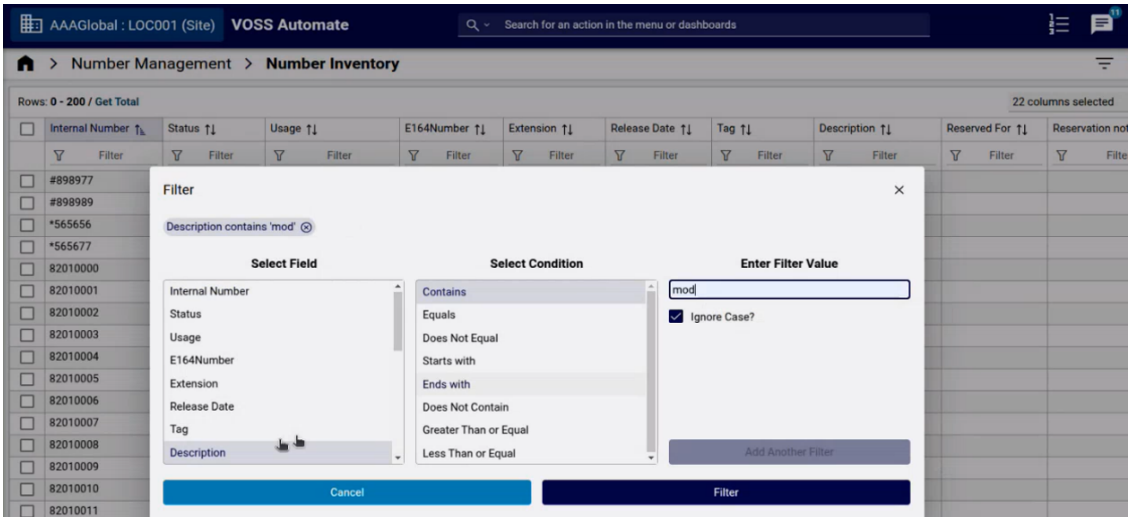


3. There are two ways to create custom inventory filter criteria:
   - Fill out inventory filter criteria at the top of the **Internal Number** column. Go to step 4.

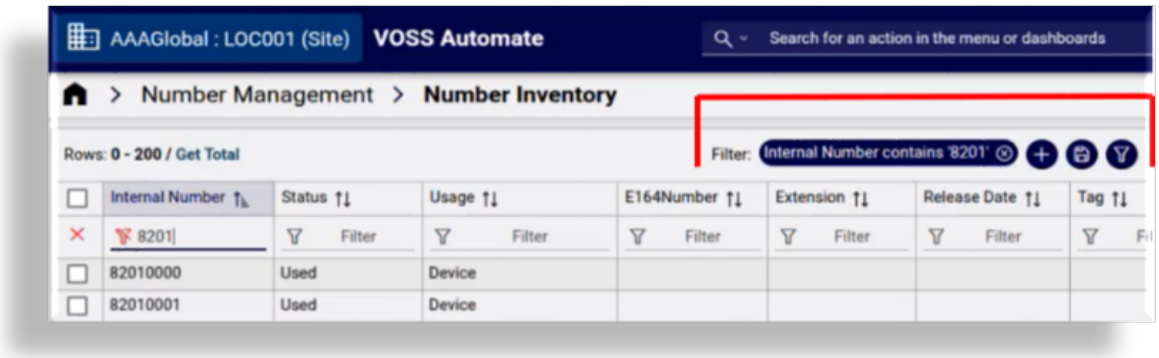


   - Click the toolbar **Filter** icon (funnel) to open the **Filter** dialog. Set up conditions for the inventory filter, then click **Filter**. Go to step 4.

Copyright © 2025 VisionOSS Limited. All rights reserved.



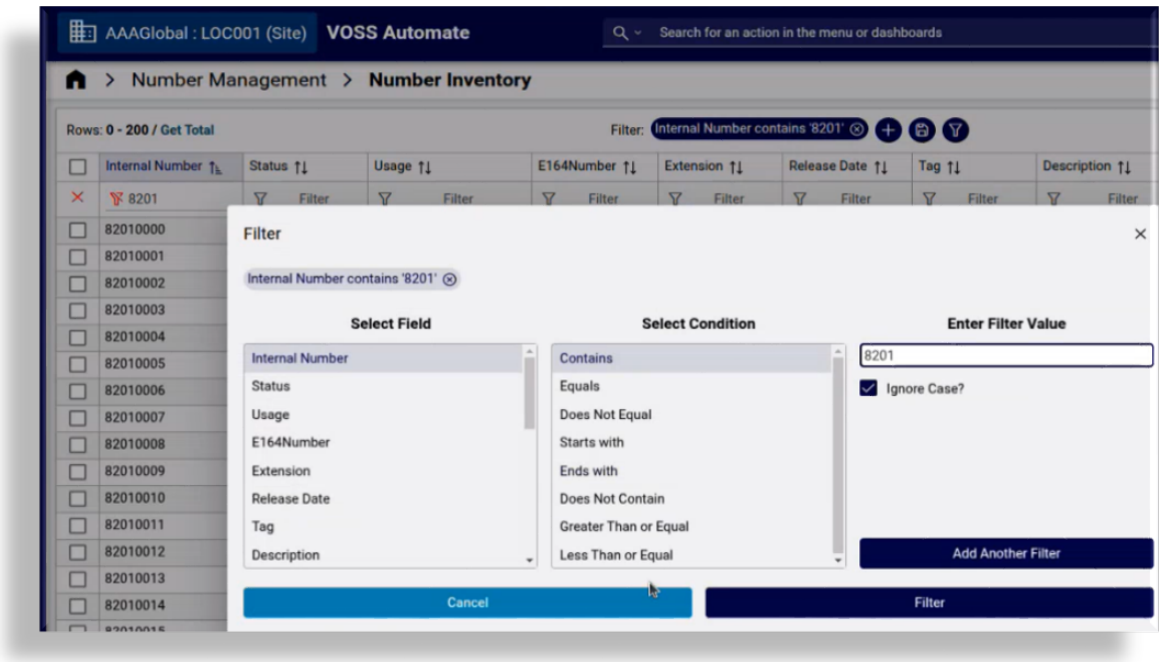
4. View the inventory filter and additional save and filter icons that now display at the top of the list view.



5. Optionally, to modify the custom inventory filter before you save it, click on the inventory filter name to launch the **Filter** dialog, where you can add or update inventory filter conditions, for example, to add a condition for only including numbers greater than or equal to, or less than or equal to the criteria you specified, or to add any other of the available conditions for filters. Click **Filter** to update the custom inventory filter.

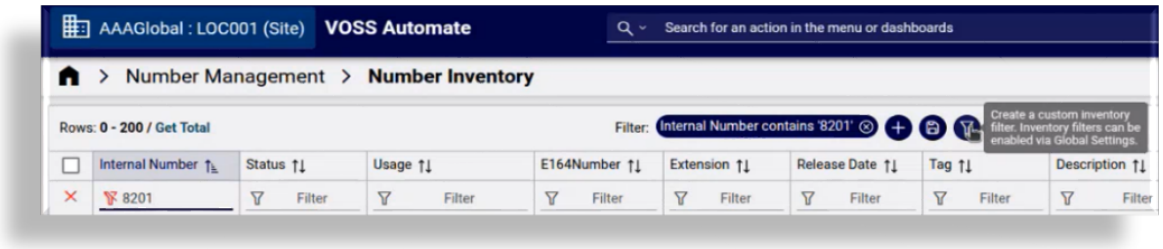
Note: By default, the custom inventory filter name is the column name and the filter criteria. You can click on the custom inventory filter to change its name. Special characters, such as the wildcard character (*) are supported.

Copyright © 2025 VisionOSS Limited. All rights reserved.

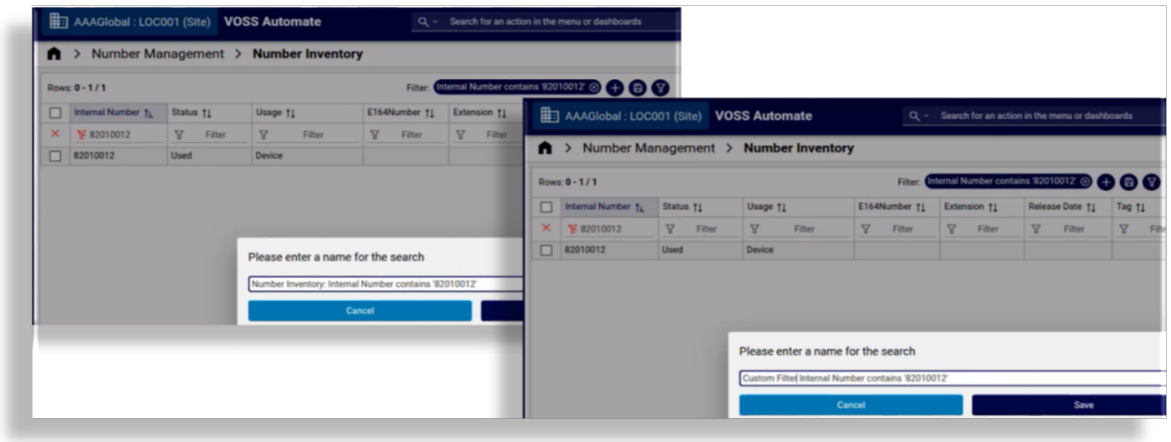


6. Click the toolbar **Filter** icon to launch a dialog where you can confirm or update the inventory filter name before saving the new custom inventory filter.

Important: A cloned shipped filter cannot be renamed. All shipped inventory filters exist at *sys* level in the Automate hierarchy and are read-only. Admin users with *sysadmin* privileges can also create custom inventory filters at *sys* level, but these custom inventory filters cannot have the same name as any shipped inventory filter since the settings from the shipped inventory filter with the same name will override any other settings you define for an inventory filter with the same name at *sys* level.



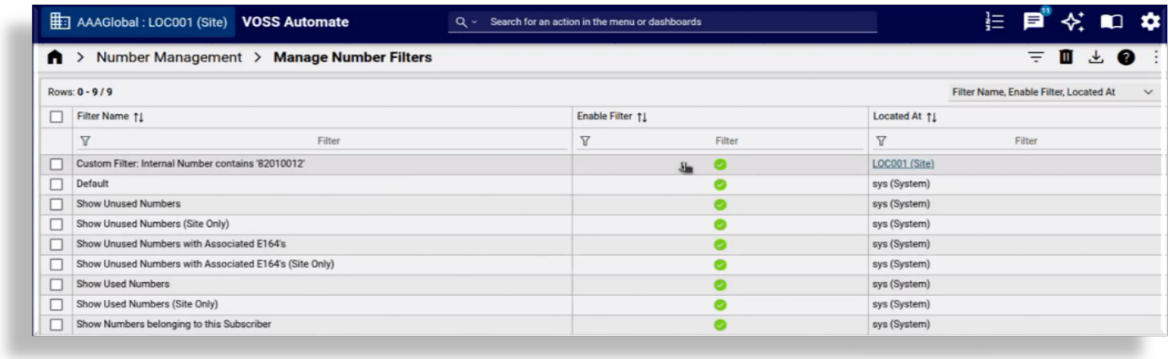
Copyright © 2025 VisionOSS Limited. All rights reserved.



7. Click **Save** to confirm the custom inventory filter name and save the filter.

   Once the transaction completes the custom inventory filter is enabled by default and is available in any number inventory filter drop-downs where you're provisioning lines, at the hierarchy where the custom inventory filter was created.

8. Go to **Manage Filters** at the hierarchy where you created the custom inventory filter to confirm that the new inventory filter now displays in the list of filters for the hierarchy.



   The custom number inventory filter you added can now be used in Automate wherever line filters are available, for example, Quick Add Subscriber and Subscriber from Profile.

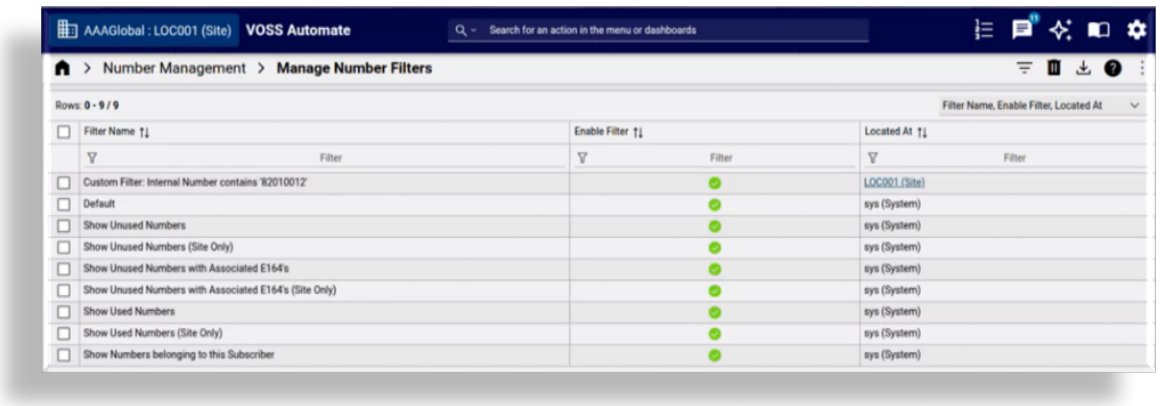
Enable, disable, or rename custom inventory filters

This procedure displays the collection of shipped and custom inventory filters at the current hierarchy, enables or disables custom or cloned shipped inventory filters, and renames custom inventory filters.

1. In the Admin Portal, go to **Manage Number Filters**.
2. Choose the hierarchy.
3. View all custom and shipped inventory filters at the hierarchy you're at. The list view contains the following details:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Description
Filter Name	The name of the inventory filter, read-only for shipped inventory filters.
Enable Filter	Defines whether the custom inventory filter is enabled at the current hierarchy.
Located At	The location of the inventory filter in the system. Shipped inventory filters are at system level (*sys*), whereas custom inventory filters are created and located at the current hierarchy.



4. **Do you want to** . . .
   - **Enable or disable a cloned shipped inventory filter or custom inventory filter**?
     - Click the inventory filter in the list view to open its settings.
     - If the inventory filter is enabled and you want to disable it at the current hierarchy, clear the **Enable Filter** checkbox
     - If the inventory filter is disabled and you want to enable it at the current hierarchy, select **Enable Filter**.
     - Save your changes.

     Drop-down lists that allow you to choose an inventory filter will now exclude any inventory filters you disabled.
   - **Rename a custom inventory filter**?

     Note: Only custom inventory filters can be renamed. Shipped inventory filters and cloned shipped inventory filters cannot be renamed.

     - Click a custom inventory filter in the list view to open its settings.
     - Click in the **Filter Name** field, update the inventory filter name, then save your changes.

Copyright © 2025 VisionOSS Limited. All rights reserved.

12.1.9. Create a filter to move users

This procedure creates a filter that will allow you to select multiple users, based on one or more user attributes, so that you can use the filter to move these users to a different hierarchy.

Note:

- Users moved with the filter must match all attributes in the filter, for example, a filter with State=Missouri and City=Kansas City, does not match a user in Kansas City, Kansas.
- Filters are automatically applied during LDAP and Cisco Unified Communications Manager user synchronization, if the User Move mode is set to automatic.
- Filters created here to filter users is not the only method to filter users. Refer to *Model filter criteria* for an alternative method - which is also the recommended method.

Tip: *Use the Action search to navigate Automate*

To define the filter:

1. Go to **Define Filters**.
2. Click **Add**.
3. On each tab, locate user attributes for the filter: **Base**, **Extended**, or **Custom**

   Provide the following information:

Field	Description
Name	Mandatory. Enter a name for the filter.
Move To Hierarchy	Choose the target hierarchy node. This field is mandatory.
Move To Role	Choose the role to be assigned to the user after the move. The available roles depend on the target hierarchy node selected. This field is mandatory. The list of available roles will include those where the **Hierarchies Allowed** list of the role contains the target hierarchy selected in the **Move To Hierarchy** list.[1]
Condition	Choose a condition for at least one of the available filters.
Value	Specify the value to evaluate for the condition. Set this field for at least one of the available filters.

   Example: Set the City Filter to Condition=isexactly and Value=Toronto to move users in Toronto to the target hierarchy node and give them the target user role.

4. Click **Save**.

   You can use the filter to manually move users using the **Move Users** page.

[1] See: *Role Management*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

12.1.10. Datasync builder templates

Tip: *Use the Action search to navigate Automate*

Overview

A data sync template is a collection of data syncs containing predefined configuration, based on the sync requirements for one or more *solution capabilities* selected for the template.

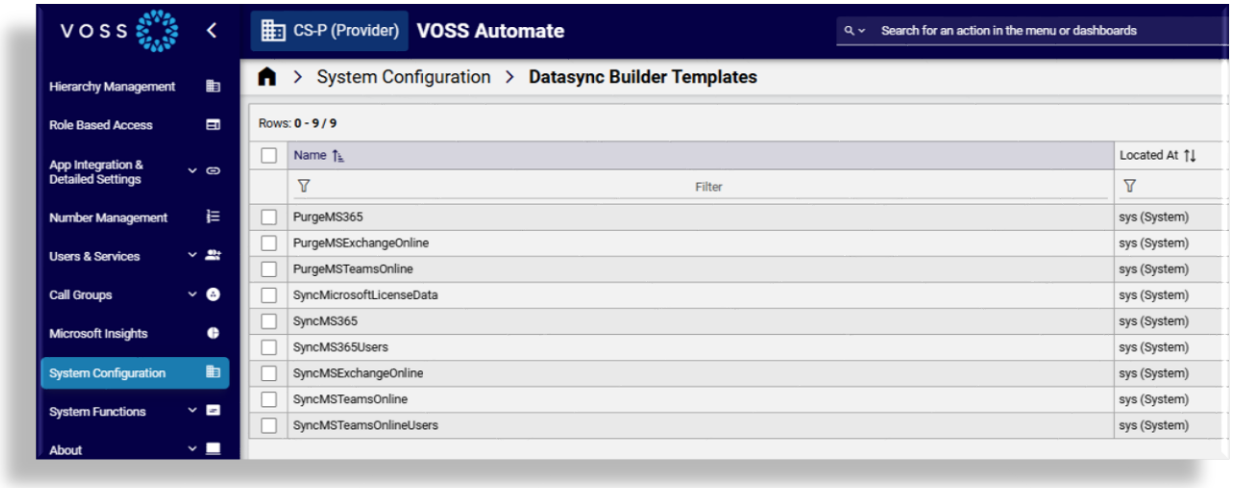
The template defines the data to be synced (whether add, update, or purge) and whether the sync is executed on demand or is a recurring sync, to be executed daily or weekly for example. The data sync template defines the model related to the sync and one or more model instance filters (MIFs, which can also be created as templates) that apply to the sync so that you can control the type and volume of data imported or purged in a sync.

Data sync templates can be executed individually or as a collection in a data sync profile.

The Datasync builder uses the templates to create predefined data syncs against any device type. If you have Webex customers for example, you can build a relevant template for the customer and use the Datasync Builder to build all required components for the data sync for the customers you execute it against.

Automate ships with a collection of predefined data sync templates, including templates based on Microsoft use cases that are integrated with the Microsoft tenant.

You can use the default data sync templates or clone and customize the templates as required.



Related topics

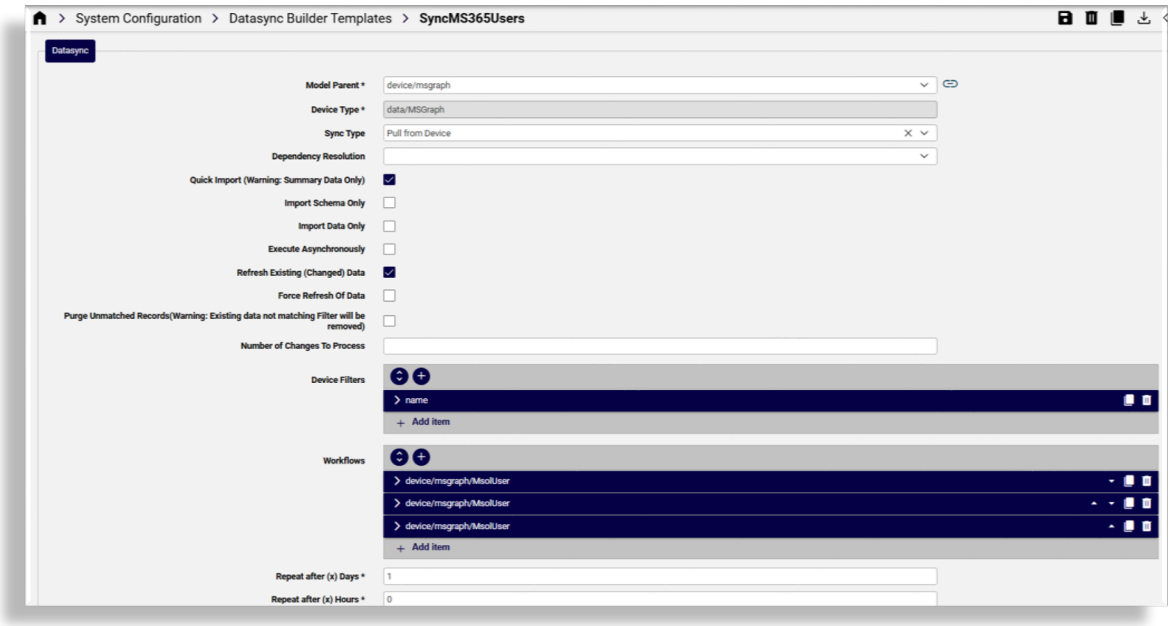
- *Datasync Builder* in the Core Feature Guide
- *Datasync profiles*
- *Microsoft tenant setup* in the Core Feature Guide
- Global Settings (Enabled Solutions) in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

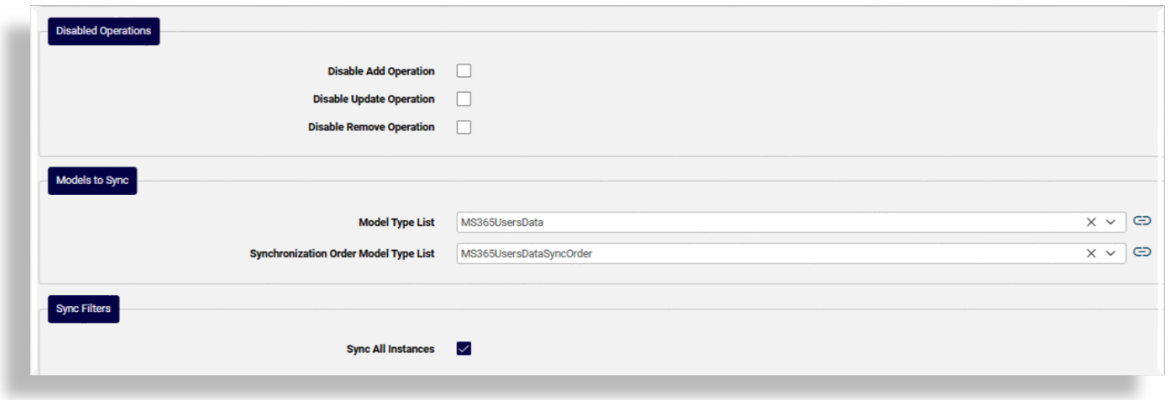
Configure a datasync builder template

1. Go to **Datasync Builder Templates**, then click on the template to configure.
2. At **Template**:
   a. Optionally, modify the template name, description, and prefix, if required.
   b. Select solutions, one or more.
3. At **Datasync**, configure settings:
   a. Select the model parent.
   b. Select the device type.
   c. Select the sync type.
   d. Select the dependency resolution.
   e. Define whether this data sync is for Quick Import (Warning: Summary Data Only).
   f. Define whether Import Schema Only.
   g. Define whether Import Data Only
   h. Define whether Execute Asynchronously
   i. Define whether Refresh Existing (Changed) Data
   j. Define whether Force Refresh of Data
   k. Define whether Purge Unmatched Records (Warning: Existing data not matching Filter will be removed)
   l. Define Number of Changes to Process.
   m. Add Device Filters (one or more).
   n. Add Workflows (one or more).
   o. Define daily frequency (Repeat after (x) Days. If the value is greater than zero (0), a start date and time is requested for the schedule.
   p. Define hourly frequency (Repeat after (x) Hours)
   q. Define Transaction Log Level (eg Debug).

Copyright © 2025 VisionOSS Limited. All rights reserved.



4. At **Disabled Operations**, optionally, select operations to disable, any of the following: Add, Update, or Remove



5. At **Models to Sync**:
   a. Optionally, select a Model Type List, List Type, and/or add Model Types (one or more).

   Note: You can choose an existing MTL from higher in the hierarchy to use in this data sync. In this case, the workflow won't build it, but will reference it in the data sync.

   Alternatively, choose List Type, for example, an option to Include Selected Model Types, in which case you add Model Types (one or more) to create new Model Type Lists (MTLs).

   You can leave Model Type List, List Type, and Model Types blank to exclude MTLs completely in the sync.

   b. Select a Synchronization Order Model Type List.
   c. Add Synchronization Order Sequence (one or more).
6. At **Sync Filters**, configure model instance filters:

Copyright © 2025 VisionOSS Limited. All rights reserved.

a. Define whether to Sync All Instances.

b. Select a Model Instance Filter.

c. Select a Filter Type (for example, Include Matching Instances)

d. Add User Filters (one or more) - either predefined filters (select from Filter Name), or create custom filters.

   The Datasync Builder will look up the definitions of predefined filters so that you can create these filters and re-use them across data sync templates, instead of creating custom filters in each Datasync Builder template.

7. Save the template.

12.1.11. Datasync profiles

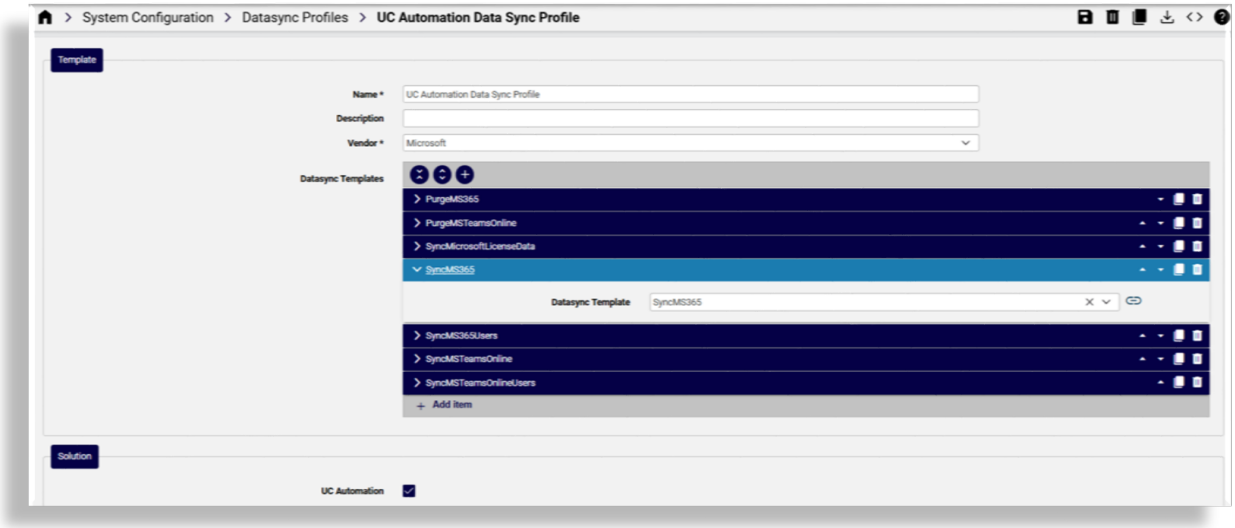
Tip: *Use the Action search to navigate Automate*

Introduction to datasync profiles

Datasync builder profiles are a collection of predefined data sync templates. Datasync profiles are a way of grouping syncs by solution. Data sync templates in the profile are used to create the data syncs needed for the solutions you're deploying.

Automate ships with predefined data sync profiles that can be cloned and updated to customer requirements, or you can create your own data sync profiles.

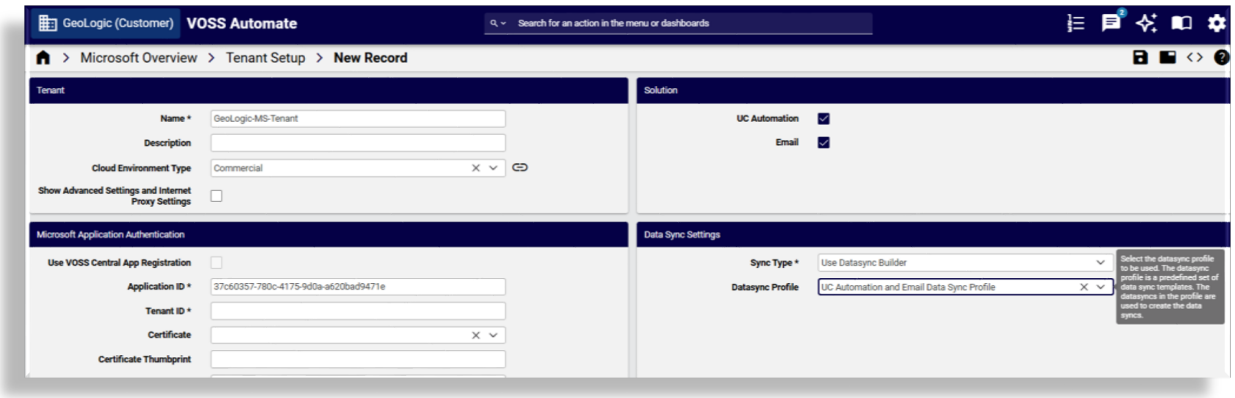
Copyright © 2025 VisionOSS Limited. All rights reserved.



Datasync profiles and the MS tenant

Data sync profiles are integrated with the Microsoft tenant so that when you have two or more solutions enabled you will need multiple data syncs. In the Microsoft tenant, data sync templates can be selected individually, or you can use a data sync profile containing a group of data sync templates.

Data sync templates or data sync profiles available for selection in the Microsoft tenant are filtered by the solutions you're choosing to deploy.



Related topics

- *Datasync builder* in the Core Feature Guide
- *Datasync builder templates*
- *Microsoft tenant setup* in the Core Feature Guide
- Global Settings (Enabled Solutions) in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

12.2. System Monitoring

12.2.1. System monitoring configuration

Overview

A `sysadmin` administrator can access the **System Monitoring** menu (menu model: `data/SystemMonitoringConfig`) to manage:

- A number of alerts that will trigger SNMP traps
- Metrics collection

Default values are set in an instance called **Global**.

Alerts

From the **Alerts** tab on the **Configuration** menu, the following settings and options can be managed:

- **Database**:
  - **Database Size Threshold (GB)**: Size when alert is enabled. The default size is 200GB.
  - **Database Index Size Threshold (GB)**: Size when alert is enabled. The default size is 50GB
- **Transactions**:
  - **Transaction Queue Size Threshold**: Count when alert is enabled. The default count is 500.
  - **Maximum time in 'Queued' state (hours)**: Time since last transaction update of a queued transaction before an alert is enabled. The default time is 6 hours (maximum:48h, minimum: 1h).
  - **Maximum time in 'Processing' state (hours)**: Time since last transaction update of a processing transaction before an alert is enabled. The default time is 6 hours (maximum:48h, minimum: 1h).
  - **Transaction Failures to Alert**: errors for operations on model types.

    The default operation is all **Import** operations on all data models (`data/*`)

For the configured alerts, *platform-level* notifications can be generated upon failure of the transaction in two ways - using the **notify** command on the platform CLI:

- SNMP traps
- Email message

Note: Either or both notification types can be configured.

Refer to the *Warnings and Notifications* and *SNMP Configuration* topics in the Platform Guide for notification setup, details and examples of the SNMP traps.

Note: It may take up to 2 hours from the time that a transaction is considered hung/stuck to the time that an alert is created. Thereafter, there will be at least one alert created within every clock hour. The subsequent alerts will not necessarily be fixed 60-minute intervals.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Metrics collection

The **Metric Collection** tab shows:

- A configurable **RIS API data collector interval** which is the time interval that the real-time information (RIS) data collector service polls the Unified CM to obtain the latest phone registration status information for phone instances stored in in the VOSS Automate database.

  The value is in seconds and the default interval is: `43200` seconds (12 hours) Refer to the Best Practices Guide for further information if this interval needs to be modified.

  Note that the **Cisco RIS Data Collector** service needs to be enabled and running on the Unified CM publisher.

  The RIS data collector service updates the current registration status and/or IP address from the Unified CM Registration Status and IP address at the specified interval - for all clusters in the system. The **Phones** list view show **Registration Status** and **IP Address** columns containing this data.

  The status of the collector service can be checked with the the platform CLI **app status** command - seen as `voss-risapi_collector` in the example console output snippet below:

```
platform@VOSS:~$ app status
selfservice v19.3.2 (2020-04-18 19:27)
   |-node                  running
voss-deviceapi v19.3.2 (2020-04-18 19:30)
   |-voss-cnf_collector    running
   |-voss-queue            running
   |-voss-risapi_collector running
   |-voss-monitoring       running
   |-voss-wsgi             running


...
```

  Note:

  – There is an **Activate Phone Status Service** check box in `data/Settings` that is selected by default. Real time data collection is available when this check box is selected. Phone status data is then fetched directly from the Unified CM and shown on the **Phones** list view. See: *Activate phone status service*.

  There is also a macro function `get_phone_status` available to return this Phone data, given as input parameters:

  – a phone PKID

  – followed by a comma and then exactly one RIS API field name.

    The fields below are for example used in the VOSS Automate Admin Portal list view of Phones:

    * `status`

    * `ip_address`

    * `cm_node`

    To see a full list of available fields, run the macro function without RIS API field names or refer to the Cisco RIS API documentation.

Copyright © 2025 VisionOSS Limited. All rights reserved.

For example:

```
{{fn.get_phone_status
      5ca2b90bce894e0014d488fb,
      status}}
```

output: “Registered”

12.2.2. System monitoring model counts

The `sysadmin` user defines a list of **Models to Aggregate** on the **Metric Collection** tab of the **Configuration** menu (menu model: `data/SystemMonitoringConfig`). By default, the following models are included in the list:

```
device/cucm/CallPickupGroup
device/uccx/Agent
device/uccx/Team
device/uccx/ContactServiceQueue
device/uccx/ResourceGroup
data/BaseSiteDAT
device/cucm/User
device/cucm/Phone
device/cucm/HuntPilot
data/InternalNumberInventory
data/HcsDpE164InventoryDAT
device/cucm/Line
device/cucm/User
device/cucm/DeviceProfile
device/cuc/User
device/spark/User
```

For these models, counts are collected daily. Daily, weekly and monthly aggregates *at a particular hierarchy: Provider, Customer or Site* are then stored as a **Grouping**. In other words, the counts include all hierarchy nodes below the particular hierarchy.

In the instance details, the **Group Number** is then the nth day, week or month of the year.

Note: For daily aggregates, only the most recent daily aggregate of the week is stored. Previous daily aggregates are aggregated into this daily aggregate and are then deleted.

A particular daily or weekly Model Counts instance will then show the **Average Count** of instances as specified in the **Models to Aggregate** list.

The data is also displayed as usage charts on the Admin Portal.

Copyright © 2025 VisionOSS Limited. All rights reserved.

12.2.3. Login sessions

Provider administrators and higher have access to the **Login Sessions** menu (`data/MonitoringSessions`).

- The **Interval** indicates the configured time interval for the entry: hourly or daily.

  Hourly intervals aggregate samples collected at 15 minute intervals. Daily intervals aggregate hourly intervals.
- The **Start** and **End** values are the time stamps for the interval.
- **Interface**: The user interface to which the limit applies: `administration` or `selfservice`.
- **Max sessions**: maximum number of sessions, for example in any of the 15-minute sampling records during an hourly interval.
- **Utilization %**: utilization percentage for the interval in accordance with the defined *customer* session limits (max sessions / defined limit).

  By default, the following limits apply:

  – per customer administration : 10

  – per customer selfservice : 1000
- The **Located At** column shows the hierarchy under which all sessions for a given entry are being counted. The sessions being counted are either by administrator or Self-service.

Note: The values reflected for at the `sys` hierarchy are global totals across all hierarchies, and the utilization percentage is calculated against the global limits.

Also refer to the use of the **voss session-limits** commands, for example to show and manage session limits, in the Platform Guide.

12.2.4. UC apps reachability

Provider administrators and higher have access to the **System Monitoring** menus:

- **Unity Connection** (`data/MonitoringCuc`)
- **Call Manager** (`data/MonitoringCucm`)
- **LDAP** (`data/MonitoringLdap`)

The displayed data is the aggregated reachability and Round Trip Delay Time (RTT) for a UC app. Reachability is tested from *all* unified nodes.

- The **Interval** indicates the configured time interval for the entry: hourly or daily.

  Hourly intervals aggregate samples collected 15 minute intervals. Daily intervals aggregate hourly intervals.
- The **Start** and **End** values are the time stamps for the interval. The difference corresponds with the selected **Interval**.
- The **Unified Node** is the node name of the source unified node.
- The **Host name or IP** is the IP addresses and port of the UC app.

  – Port 8443: HTTPS connectivity

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **Avg TCP RTT (ms)** is the average RTT in milliseconds over the interval for a successful connection.

  The details of a data instance also show the maximum RTT (**Max Tcp RTT**) during the interval.

  If the average RTT exceeds 400 ms, an alert is also triggered.
- The **Failures** is the number of connection failures to the UC app **Host name or IP** over the interval.

  For example, if the number of failures is 4 and the **Interval** is set to *hourly*, then all 4 reachability checks for the interval failed. Equally, if the **interval** is set to *daily* and all reachability checks failed, the value is 96 (24 x 4 hourly).

  The details of a data instance with failures show the network error messages in the **Errors** group.
- The **Located At** column shows the hierarchy of the UC app.

Failures would also generate alerts if an SNMP trap is configured.

12.2.5. System monitoring database statistics

The `sysadmin` user has access to the **Database Statistics** menu (menu model: `data/MetricDatabaseCollectionStats`) that shows the *weekly and monthly* collection metrics internal database collections.

Note:

- Mongo database collections are similar to tables relational databases.
- Mongo database documents are similar to rows in relational database tables.

- The **Group Number** corresponds to the number of the **Grouping** - month or week of the year - respectively.
- The **Top Collections by Data Size** list shows individual data collections by name and sorted by size - displayed in bytes.
- The **Top Collections by Index Size** list shows individual data collection indexes by collection name and sorted by index size - displayed in bytes.
- The **Top Collections by Number of Documents** list shows data collection names by collection name and sorted by number of documents - displayed as an integer.

The **Configuration** menu allows for SNMP alerts to be configured if thresholds are reached in total Data Size and Index Size.

12.2.6. Automate cluster status

The *sysadmin* user has access to the **VOSS Automate Cluster** page (model: `data/MonitoringCluster`), which displays aggregated Automate cluster Round Trip Delay Time (RTT) metrics at hourly and daily intervals.

Note:

- The retention period for data is 1 month.
- This metric uses the same data as the `cluster check` CLI command. See *Cluster Check* in the Platform Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **Interval** indicates the time interval for the entry: hourly or daily.

  Hourly intervals aggregate samples collected 15 minute intervals. Daily intervals aggregate hourly intervals.

- The **Start** and **End** values are the time stamps for the interval. The difference corresponds with the selected **Interval**.
- The **Source host** and **Destination port** are the IP addresses of the nodes in the cluster.
  - Port 27020: database connectivity
  - Port 8443: HTTPS connectivity

  For example, if **Source host** is `192.168.100.7` and **Destination port** is `192.168.100.6:27020`, then database connectivity is monitored between `192.168.100.7` and `192.168.100.6:27020`.

- The **Failures** is the number of connection failures between **Source host** and **Destination port** over the interval.

  Failures would also generate alerts if an SNMP trap is configured.

- The **Avg TCP RTT (ms)** is the average RTT in milliseconds over the interval for a successful connection.

12.2.7. Worker queue

Provider administrators and higher have access to the **Worker Queue** menu (`data/MonitoringQueue`).

Data is retained for 1 month.

The displayed data is the aggregated number of transaction requests per processing node and configured interval.

- The **Interval** indicates the configured time interval for the entry: hourly or daily.

  Hourly intervals aggregate samples collected 15 minute intervals. Daily intervals aggregate hourly intervals.

- The **Start** and **End** values are the time stamps for the interval. The difference corresponds with the selected **Interval**.

  For the same **Start** and **End** timestamp, an entry is shown for each **Processing node** showing the combination of **Status**, **Priority** and **Tx level**.

- **Status**: Transaction process status: “Queued” or “Processing”.
- **Priority**: Transaction priority: Low, Normal or High
- **Tx level**: Transaction level: either parent or child transaction.
- **Processing node**: the node that carried out the transaction.
- **Avg Transactions**: the average of the **Max Transactions** and **Min Transactions** for the selected **Interval**.

  Note: The record detail also shows the **Min Transactions** and **Max Transactions** for the configured interval. These values reflect the sampling in the interval. For example, if the **Interval** is hourly and **Min Transactions** is 0, then one or more of the 15-minute sampling intervals recorded no transactions.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The **Located At** column shows the hierarchy at which the transaction was run.

  Note: If the value shows as `sys(System)`, this includes all transactions at `sys` level and lower.

Also refer to the use of the **voss worker** and **voss workers** commands in the Platform Guide.

12.3. Email Setup

12.3.1. Add a SMTP server

Tip: *Use the Action search to navigate Automate*

This procedure adds a SMTP server at a hierarchy level.

Prerequisites:

- Enable email in the Global Settings (Email tab).

Perform these steps:

1. Log in to the Admin Portal.
2. Choose the relevant hierarchy.

   Note: Configure the SMTP server at the hierarchy where you want to allow VOSS Automate to send email messages.

   You may only set up one SMTP server at each hierarchy level. The SMTP server will be available at the current hierarchy and below. For example, for a SMTP set up at a specific customer, the sites below that customer can use that SMTP server.

3. Go to **SMTP Server**.
4. Click the Plus icon (+) to add a new SMTP server.
5. On the **SMTP Server** page, fill out details for the new SMTP server:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Name	The SMTP server name.
Description	A description for the email account.
Port	The port number.
Secure	Relevant only for SSL connections to the SMTP server. Select the checkbox (enable) to use the SSL protocol for connections to the SMTP server. Default is disabled (checkbox is left clear), for TLS and unsecure logins to the SMTP server.
Username	The username credential for establishing a connection to the SMTP server.
Password	The password credential for establishing a connection to the SMTP server.

6. Save your changes.

Related topics

- Email in the Core Feature Guide
- Global Settings in the Core Feature Guide

12.3.2. Email

Tip: *Use the Action search to navigate Automate*

Overview

Provider administrators can test email messages and manage email templates, provided an email SMTP server is set up, and when emails are enabled via the **Email** tab of the *Global settings*.

Email functionality is available for the following:

Component	Description
Quick Add User - Cisco (QAS)	Enable email functionality via Global Settings > Email tab, then select a checkbox in QAS to send a welcome email to new users added via QAS.
Quick User - Microsoft	Enable email functionality via Global Settings > Email tab, then select a checkbox in Quick User to send a welcome email to new users added via Quick User.
File Transfer Destinations	Configured by high level system administrators to transfer audit data for licensing. See the Licensing and Data Export Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Add a SMTP Server*
- *Global settings*

Send test email

On the **Send Test Email** page you can allow an email message to be sent to and from a specified email address, and select an email HTML template to test in the email body.

Email HTML templates

You can view and work with email templates on the **Email HTML Templates** page.

Email HTML templates contain placeholders for the email subject and body text, in HTML markup. The HTML markup can be:

- Previewed by using the **Preview** menu option in the editor
- Modified as required.

Default email templates

By default, the system provides the following email templates:

Note: When adding a HTML template from the list view, the **Name** can only be "Test Email Template", "Quick Add User", or "Number Inventory Alerting".

Default email templates	Description
Test Email Template	This default template is read-only. You can't modify it or change its name. To use this template, you can clone it to your hierarchy and customize the clone.
Quick Add User	This default template is read-only. You can't modify it or change its name. To use this template, you can clone it to your hierarchy and customize the clone. You can use this template only if the setting is enabled via the Global Settings. Values from the Quick Add User input form can be used to populate the template by adding variables to the HTML template.
Number Inventory Alerting	This default template is read-only. You can't modify it or change its name. To use this template, you can clone it to your hierarchy and customize the clone. You can use this template only if the setting is enabled via the Global Settings. Values from Number Inventory Alert message can be used to populate the template by adding variables to the HTML template.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Quick Add User email template variables

Values from the **Quick Add User** page can be used to populate the Quick Add User email template by adding variables to the HTML template.

The table lists the available variables for the **Cisco** Quick Add User email template:

Field name on input form	Variable available in HTML
Username	`{{ pwf.EMAIL.username }}`
First name	`{{ pwf.EMAIL.firstname }}`
Last name	`{{ pwf.EMAIL.lastname }}`
One time password	`{{ pwf.EMAIL.password }}`
One time PIN	`{{ pwf.EMAIL.pin }}`
Access Code	`{{ pwf.EMAIL.phone_access_code }}`
Email	`{{ pwf.EMAIL.email }}`
Extension	`{{ pwf.EMAIL.extension_number }}`
Mobile Number	`{{ pwf.EMAIL.mobile_number }}`
Entitlement Profile	`{{ pwf.EMAIL.entitlement_profile }}`
Phone Type	`{{ pwf.EMAIL.phone_type }}`
Phone Names	`{{ pwf.EMAIL.phone_names }}`
Jabber Device Names	`{{ pwf.EMAIL.jabber_names }}`
Extension Mobility Name	`{{ pwf.EMAIL.extensionmobility_name }}`
External E.164 number	`{{ pwf.EMAIL.e164 }}`

Note: When sending the welcome email to users added via Quick Add User, if there is more than one E.164 number associated with the user's extension, only the primary E.164 number displays. If there are no E.164 numbers associated with the user's extension, then no E.164 number value displays.

The table describes the default variables for the **Microsoft** Quick user email template:

Field name on input form	Variable available in HTML
Username	`{{ pwf.EMAIL.username }}`
First name	`{{ pwf.EMAIL.first_name }}`
Last name	`{{ pwf.EMAIL.last_name }}`
One time password	`{{ pwf.EMAIL.password }}`
Email	`{{ pwf.EMAIL.email }}`
Extension	`{{ pwf.EMAIL.line_uri }}`
Mobile Number	`{{ pwf.EMAIL.mobile_phone }}`
Phone Number	`{{ pwf.EMAIL.phone_number }}`

Example user details you can add to your QAS HTML template:

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
<p>Username: {{ pwf.EMAIL.username }}</p>
<p>First name: {{ pwf.EMAIL.firstname }}</p>
<p>Last name: {{ pwf.EMAIL.lastname }}</p>
```

Number inventory alerting email template variables

Values from the Number Inventory Alert message can be used to populate the Number Inventory Alerting email template by adding variables to the HTML template. The table describes the variables available for this template:

Name on alert message	Variable available in HTML
Threshold of available (%)	`{{ pwf.INI_ALERT_THRESHOLD }}`
Threshold reached (True/False)	`{{ pwf.INI_ALERT_THRESHOLD_REACHED }}`
Hierarchy node type	`{{ pwf.INI_ALERT_HIERARCHY_NODE_TYPE }}`
Hierarchy friendly name	`{{ pwf.INI_ALERT_HIERARCHY_NAME }}`
Hierarchy full path	`{{ pwf.INI_ALERT_HIERARCHY }}`
Total Numbers Available	`{{ pwf.INI_ALERT_TOTAL_INI_AVAILABLE }}`
Total Number count	`{{ pwf.INI_ALERT_TOTAL_INI_COUNT }}`
Total percent available	`{{ pwf.INI_ALERT_TOTAL_PERCENT_AVAILABLE }}`
Table of usage per site	`{{ pwf.INI_ALERT_NODES_EXCEEDED_THRESHOLD_TABLE }}`

Example HTML

```
<h1>Number Inventory Threshold Report</h1>
<table border='1' style='border-collapse:collapse'>
<tr><td><b>Hierarchy node name</b></td><td><center>{{ pwf.INI_ALERT_HIERARCHY_NAME }}</
↪center></td></tr>
<tr><td><b>Hierarchy node type</b></td><td><center>{{ pwf.INI_ALERT_HIERARCHY_NODE_TYPE }
↪}</center></td></tr>
<tr><td><b>Hierarchy full path</b></td><td><center>{{ pwf.INI_ALERT_HIERARCHY }}</center>
↪</td></tr>
<tr><td><b>Total numbers available</b></td><td><center>{{ pwf.INI_ALERT_TOTAL_INI_
↪AVAILABLE }}</center></td></tr>
<tr><td><b>Total numbers</b></td><td><center>{{ pwf.INI_ALERT_TOTAL_INI_COUNT }}</center>
↪</td></tr>
<tr><td><b>Total percent available</b></td><td><center>{{ pwf.INI_ALERT_TOTAL_PERCENT_
↪AVAILABLE }}%</center></td></tr>
</table>
<p></p>
<p>{{ pwf.INI_ALERT_NODES_EXCEEDED_THRESHOLD_TABLE }}</p>
```

Example message

Copyright © 2025 VisionOSS Limited. All rights reserved.

info@voss-solutions.com 12:23
to me

Number Inventory Threshold Report

Hierarchy node name	CS-P
Hierarchy node type	Provider
Hierarchy full path	sys.hcs.CS-P
Total numbers available	1830
Total numbers	1982
Total percent available	92%

List of hierarchy nodes with less than 15% of available numbers

Hierarchy node name	Hierarchy node type	Hierarchy full path	Total numbers available	Total numbers	Total percent available
Overton	Customer	sys.hcs.CS-P.CS-NB.Overton	2	25	8%

The email alert message also includes an attachment file called `NumberThreshold.csv` that contains the alert report in CSV format, for example:

```
Hierarchy Node Name,Hierarchy Node Type,% Available,Total Numbers Available,Total Numbers
CS-P,Provider,92,1830,1982
CS-NB,Reseller,92,1830,1982
AAAGlobal,Customer,91,1428,1557
Overton,Customer,8,2,25
LOC001,Site,74,284,382
LOC002,Site,83,20,24
LOC003,Site,90,46,51
```

Email groups

You can manage a group of email recipients via the **Email Groups** page:

- Add a name and a description to create the group
- Add a list of email addresses

The email group is now available and can be selected where email groups are selected.

See for example *Global settings*, for:

- Webex App email to specify recipients of generated CSV files.
- Number Inventory Alerting - email group to receive alerts.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Add a SMTP Server*
- *Global settings*

12.4. Customer Build Configuration

12.5. Preferences & Defaults

12.5.1. Global settings

Tip: *Use the Action search to navigate Automate*

Overview

Administrators (Provider level and up) may configure global settings for customizations that apply at a specific hierarchy only or across all hierarchies in the system.

On each tabbed page in Global Settings, a read-only field below the choice drop-down displays the current setting for your system. Options are:

Inherit	The service is enabled/disabled based on the setting at the hierarchy above the current one.
Yes	The service is enabled at the current hierarchy.
No	The service is disabled at the current hierarchy.

To change inherited settings, see *Changing inherited settings*.

Update Global Settings

Global settings are configured on the tabs of the Global Settings page:

- *Number Inventory*
- *Number Inventory Alerting*
- *Microsoft Licensing Alerting*
- *Webex App*
- Pexip Conference
- Email
- Phones
- Voicemail
- User

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Flow Through Provisioning
- Enabled Services
- *Enabled Solutions*

Number Inventory

The table describes the global settings for the Number Inventory:

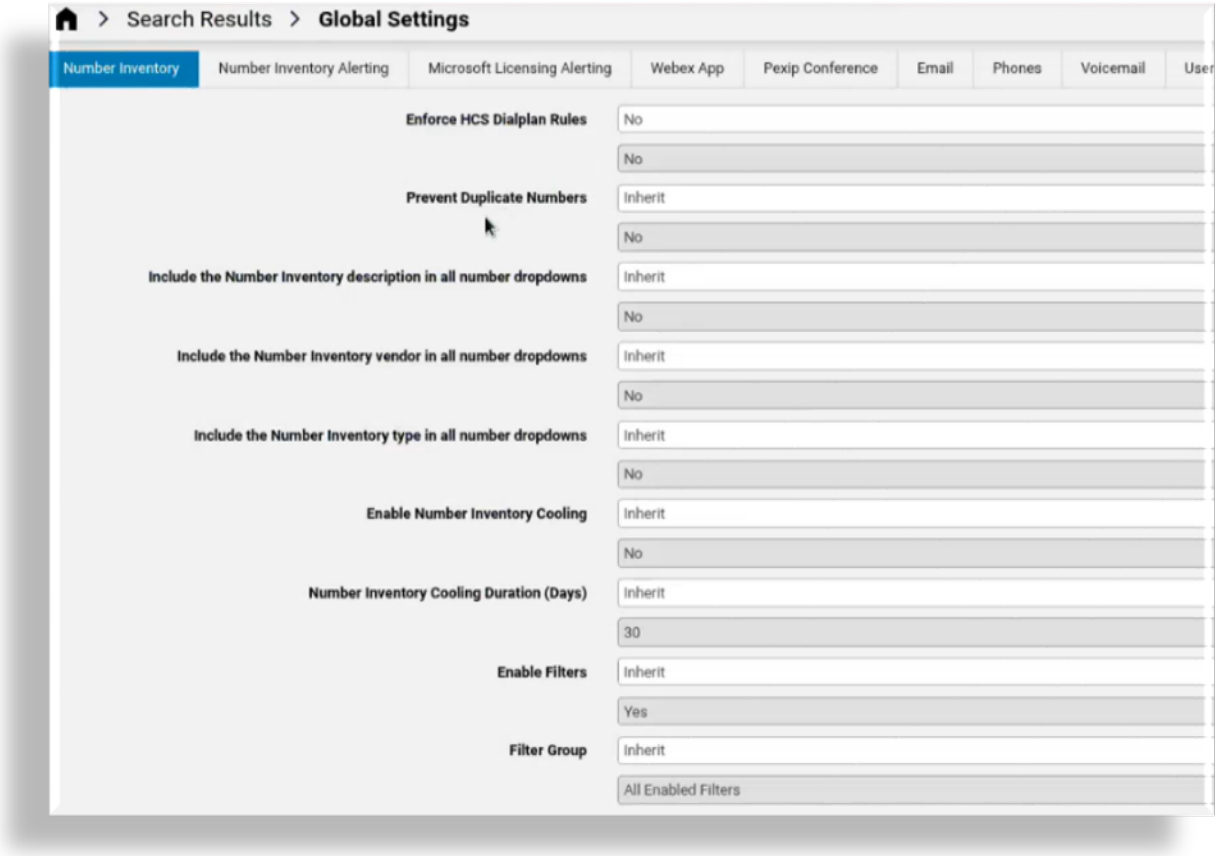
Field	Description
Enforce HCS Dialplan Rules	When enabled, dial plan workflows enforce HCS Rules when provisioning Customers, Countries, Site and so on. Default = **Inherit**. If your deployment uses a custom or specific dial plan that does not conform to the HCS rules, this setting should be set to **No** (False).
Prevent Duplicate Numbers	This setting displays only at hierarchies above site or or linked site levels, and only when Microsoft is enabled for your system (via the Enabled Services tab in Global Setting). When available, the setting is enabled only when *Enforce HCS Dialplan Rules* is set to *No* (disabled), else, the field is read-only. In Microsoft environments, defines whether to allow the creation of duplicate numbers at sites in Automate when syncing in and provisioning users, or when creating number ranges. Default is *No* (duplicate numbers are allowed). The system checks the setting for *Enforce HCS Dialplan Rules* before applying the *Prevent Duplicate Numbers* logic. When enabled, the system enforces unique number validation throughout the hierarchy.
Include the Number Inventory description in all number drop-downs	Defines whether descriptions for the numbers (which can be added when the number inventory is managed via **Number Management**), display along with the numbers in the drop-down lists. For example, let's say you have a number and its description as follows: *1000 - CEO Internal*. When this setting is enabled (Yes), both the number (1000) and its description displays in the lists (when using features such as Quick Add User). The default is No.
Include the Number Inventory vendor in all number dropdowns	Defines whether vendor names for the numbers show in number dropdown as an option. For example, a number `982017206` (which is from Microsoft vendor) will display as `982017206 [Microsoft]` in the drop-down list.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Include the Number Inventory type in all number dropdowns	Defines whether number types for the numbers show in number drop-down as an option. For example, a number `982017206` (which is from Microsoft vendor and is of type `OperatorConnect` will display as `982017206 [OperatorConnect]` in the drop-down list.
Enable Number Inventory Cooling	Defines the availability of numbers in the system when a phone, user, or service associated with the number is deleted, and the number is no longer associated with these entities. Options are: • **Inherit**: When set to True, number inventory cooling is enabled or disabled based on the setting defined for number inventory cooling at a higher level in the hierarchy. • **Yes** (True) Enabled at the current hierarchy. Numbers associated with deleted entities are kept in a cooled state for a specified number of days (based on the value defined in the **Number Inventory Cooling Duration (Days)** field. Numbers in a cooled state are unavailable in the system until the cooling period end date is reached, unless they are manually released before the "end cooling period" end date. • **False** (No) Default. Number inventory cooling is disabled by default.
Number Inventory Cooling Duration (Days)	When number inventory cooling is enabled (Yes/True), this field defines the period (number of days) the number is kept in a cooled state and unavailable for association with a phone user, or service. The default is 30 days.
Enable Filters	Enables/disables custom number inventory filters at the current hierarchy. Shipped inventory filters can't be enabled or disabled as these reside at *sys* level. When enabled, custom and shipped inventory filters display in a drop-down list on forms such as Quick Add User, Onboard User (to add a user from a profile), Multi vendor service user move, Cisco Advanced User, Phones, Extension Mobility, and Single Number Reach. Options are: • **Inherit** (default): When set to True, custom inventory filters are enabled or disabled based on the setting defined at a higher level in the hierarchy. • **Yes** (True) Enables custom inventory filters at the hierarchy. When set to True, select the inventory filters to make available for selection in relevant drop-down lists, either shipped and custom inventory filters or all enabled inventory filters. You can view the available filters at a hierarchy via **Manage Filters**. When enabled, you can enable or disable specific filters at specific hierarchies via **Manage Filters**. • **False** (No) Custom and/or cloned shipped filters are disabled at the hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Filter Group	When **Enable Filters** is set to Yes, the selected filter defines the number inventory filters available in the the drop-downs for choosing a number inventory filter. Options are: • Inherit • Shipped Enabled Filters • Custom Enabled Filters • All Enabled Filters (default) When set to *Inherit*, the value displays for the filter group that will be used from a higher level in the hierarchy. Custom enabled filters will only display in the drop-downs if these exist and are enabled at the hierarchy you're working at. *All Enabled Filters* includes all custom and shipped filters, provided they are enabled at the hierarchy you're working at.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Number Cooling in the Core Feature Guide
- Number Cooling Auto Expiry Schedule in the Advanced Configuration Guide
- Manage Number Filters in the Core Feature Guide
- Prevent duplicate numbers in the Core Feature Guide

Number Inventory Alerting

This tab configures the global settings for number inventory alerting, which defines how alerts may be raised once the number inventory is running low.

The table describes the settings on this tab:

Field	Description
Enable Alert on Available Numbers	By default, this setting is set to **Inherit**. However, it will not inherit the setting from higher up the tree unless it is explicitly set to **Yes** or **No**. **Inherit** in this instance just means it is *not configured*. Change to **Yes** to enable alerting.
Alert Aggregate Level	Choose a hierarchy level at which the *aggregate* of available numbers should be calculated (Provider, Reseller, Customer, Site), and displayed in the body of the alert. The shown data in the body for this hierarchy level is: • Hierarchy node name • Hierarchy node type • Hierarchy full path • Total numbers available • Total numbers • Total percent available Data is also included for lower hierarchies (as tables and in CSV format). For details, see the following topics: • Email in the Core Feature Guide • Number Inventory Alerts in the Core Feature Guide
Availability Threshold Percentage	Select or enter a percentage available of the total numbers at which point alerts will be raised. Sample percentages are available to choose from. If available numbers drop below this percentage, alerts will be raised.
Enable Email Group	Set to **Yes** to send email alert notifications to an email group. The email group needs to be available or should be set up.
Alert Email Group	If **Enable Email Group** is set to **Yes**, select the email group.
Ignore Hierarchies With No Numbers	If set to **Yes**, hierarchy levels with no numbers are excluded from reports.

Note: The email alert message also includes an attachment file `NumberThreshold.csv`, which contains the alert report in CSV format. See: *Email HTML templates*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Email in the Core Feature Guide
- Number Inventory Alerts in the Core Feature Guide
- SNMP Traps: Number Inventory Alerting in the Platform Guide

Microsoft Licensing Alerting

The table describes the global settings for the Microsoft Licensing Alerting:

Field	Description
Enable Alert on Microsoft Licenses	When enabled, alerts will be raised and optionally emailed if the Microsoft license availability threshold is reached at the hierarchy. Default = **Inherit**. Note that this setting requires that **Enable Microsoft User License Enforcement** is enabled under the **User** tab. Refer to **Availability Threshold Percentage** below.
Availability Threshold Percentage	Defines a percentage of remaining Microsoft licenses at which an alert is raised. Percentages are available in the drop-down lists: 10, 15, 20, 25. Default = **Inherit**.
Enable Email Group	Defines whether an email group will receive alerts. Default = **Inherit**. If set to **Yes** at the hierarchy, the **Alert Email Group** drop-down list provides available email groups.
Alert Email Group	The selected email group to receive alerts for Microsoft licenses consumption above the defined threshold. Default = **Inherit**.

Related topics

- Microsoft License Management and Alerting in the Core Feature Guide
- Email in the Core Feature Guide

Webex App

This tab configures the global settings for Webex App.

The table describes the fields on this tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Retain a Webex App User when a subscriber is deleted	Defines whether to delete Webex App user when a user is deleted. Default is **No**.
Send notification when the Webex App Refresh Token expires	Defines whether a notification is sent when the Webex App refresh token expires for a specified customer. A SNMP trap and Webex App message is sent to recipients configured in the email group.
Webex App Refresh Token expires threshold (in seconds)	The max threshold (in seconds) for when to send a SNMP trap to the SNMP (if **Send SNMP trap message when the Webex App Refresh Token expires** is enabled). The default is `172800` seconds, which is two days.
Automatically apply default calling behavior on Webex App user data sync	Whether to apply default calling behavior (set up in Customer settings), to new Webex App users synced in to Automate. Default is No.
Generate and send Webex App User CSV file via Webex App message	Whether to generate a CSV file on create/update of Webex App user. Default is No. If enabled (Yes), the CSV file is sent via Webex App to a predefined list of recipients.
Email group containing recipients of the generated Webex App user CSV file	The group of recipients of the Webex App message with the generated CSV file. The email group is set up on the **Email Groups** menu.
Send manual Webex App Workspace configuration steps via Webex App message	Whether manual configuration steps (on Webex App Control Hub) are to be sent on create/update of a Webex App workspace. Default is **No**. If enabled, the steps are sent via a Webex App message.
Email group containing recipients of the manual Control Hub steps	Email group recipients of the Webex App message containing the manual configuration steps.
Quick Add Group for Hybrid Calling Workspace Unified CM users	The Quick Add Group to use when creating dummy CUCM users with line and device for Webex App workspace hybrid calling.
Enable Cisco Webex Contact Center Model References	Defines whether to enable retrieval and display of Cisco Webex Contact Center device model references from the Webex Control Hub. It is recommended that you enable this setting in the Global Settings only for any customer where you want to retrieve the reference details. This is to prevent a performance impact on customers where the setting is not required.

Related topics

- Quick Add Groups in the Core Feature Guide
- Email in the Core Feature Guide
- Email Groups in the Core Feature Guide
- Create Webex App Service in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

Pexip Conference

This tab configures the global settings for Pexip Conference.

The table describes the settings on this page:

Field	Description
Retain a Pexip Conference when a user is deleted	Defines whether the Pexip conference set up from the user interface is to be removed when the user is deleted. By default the setting is inherited from the hierarchy level directly above the current one.

Email

This tab configures the global settings for Email.

The table describes the settings on this page:

Field	Description
Allow welcome email to be sent to user after Quick Add User	Defines whether an email is sent to a user when added via Quick Add User. The default is **No**. When set to **Yes**, and a SMTP server is set up via **Apps Management**), then selecting the option to send an email when using Quick Add User, a welcome email is sent to the new user.

Related topics

- SMPT Server in the Core Feature Guide
- Email in the Core Feature Guide

Phones

This tab configures the global settings of phones for a site.

Note: These settings only apply to phones within the same site; both the re-added phone and the existing phone must be on the same site.

The table describes the phone global settings on this tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Delete existing Unassigned Phone when re-adding an identical phone	Defines whether to delete an existing, unassigned phone (a phone without an owner), when re-adding a phone with the same name and product type (duplicate phone). Default is *Inherit* (*No*, inherited from the hierarchy above), which triggers a transaction failure if you try adding a duplicate phone, for example, in a Quick Add User bulk load or when updating a user. When set to *Yes*, a system check verifies whether the phone exists and/or if it is already assigned (whether ownerUserName field is populated): • If the phone exists and is assigned to a different user, the transaction fails. • If the phone exists and is unassigned, the existing phone is deleted, the phone is re-added, and is assigned to the user you're adding or updating. • If the phone exists and is already assigned to the user you're working with. The system performs an update.
Retain Desk Phones when Subscriber is deleted	Defines whether a user's associated desk (hard) phones (phones prefixed with SEP or BAP) are deleted or retained when that user is deleted. When set to *Yes*: • The deleted user's hard phones are retained. • The deleted user's soft phones (such as Jabber devices) are deleted. • An additional field displays (**Update the Retained Desk Phone with Configuration Template**), which allows you to define whether retained phones are updated via a CFT once the user is deleted. Default is Inherit (set to No). This setting defines hard phone delete/retain behavior for any method of deleting a user, for example, delete user via the User's list view, or delete user in LDAP import, purge or sync (where delete or purge mode is automatic). You can view the hard phones associated with the user on the Phones tab in the user settings.
Update the Retained Desk Phone with Configuration Template	This field displays only when **Retain Desk Phones when user is deleted** is set to **Yes** (True). Defines whether to update retained hard phones via a configuration template (CFT) when the associated user is deleted. This feature ships with a default CFT (RemoveOwnerFromPhoneCFT), which clears the phone's Owner User ID if the phone is retained when deleting the associated user. You can choose a different CFT for the update step, if required.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Include additional information in Phone dropdowns	Options are Yes, No, Inherit. Default is *Inherit* (inherited from the hierarchy above) Set to *Yes* to enable. You will need to save this update then refresh the tab to display an additional configuration field (Additional information in Phone dropdowns).
Additional information in Phone dropdowns	Options are Yes, No, Inherit. Default is *Inherit*. Additional information options are *Description*, *First Line*, and *Description + First Line*. The default, *Description*, means that the phone description (if defined) displays in the phone selection drop-downs on the **Replace Phone** configuration page (Existing Phone tab, Device Name drop-down), and on Quick Add User, allowing you to search by phone description when choosing a phone from the drop-down. In the same way, when the additional information option is set to either *First Line* or *Description + First Line*, you can search for or choose phones based on this criteria.
Prevent Duplicate MAC Addresses for Cisco Phones	Options are Yes, No, Inherit. Default is *Inherit*. For any transaction adding a Cisco phone, if this setting is enabled, the transaction will fail with a message: `Phone already exists with name:` if any phone is found containing the same MAC address within all clusters in a customer or reseller.

Related topics

- Replace Phone in the Core Feature Guide.
- Quick Add User for Cisco UCM Users in the Core Feature Guide.
- User, Phones tab in the Core Feature Guide

Voicemail

This tab configures the global settings for voicemail.

The table describes the settings on this tab:

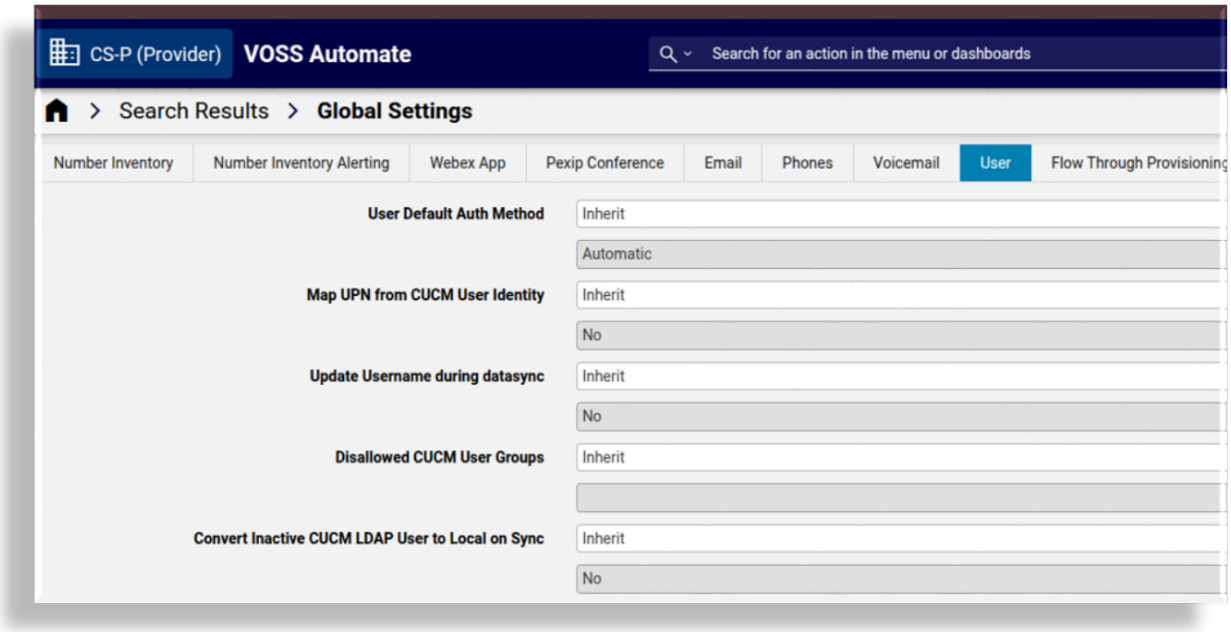
Field	Description
Retain a (Cisco) Voicemail Account when a user is deleted by data sync only	Defines whether to retain a Cisco (UCM) user's voicemail account when the user is deleted. Default is Yes (true). When set to Yes, the CUCM user's voicemail account is retained when the user is deleted and user sync is executed.

Copyright © 2025 VisionOSS Limited. All rights reserved.

User

This tab configures the global settings for users.

Note: When a user is either synced into or added manually on Automate, these settings apply by default. The settings can however be modified when adding a user via **User Management**.



The table describes the settings on this tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
User Default Auth Method	The default authentication method to use when a user is synced in or added manually. The default is **Local** (inherited).
Map UPN from CUCM User Identity	Maps the Microsoft Azure UserPrincipalName (UPN) attribute to CUCM userIdentity attribute - used in Cisco-Microsoft hybrid configurations where the same user ID is on every user account (MS Teams, CUCM, etc.). If enabled, the CUCM user's userIdentity attribute is used for the import of MS teams CsOnlineUser and MS 365 Msol user instances. The default is **No** (inherited).
Update Username during datasync	Defines whether to update the existing VOSS username when a new associated user is imported via a sync.
Disallowed CUCM User Groups	Defines the user groups (one or more) that admins will not be allowed to assign to user. This is to prevent users being incorrectly assigned elevated permissions to system resources that are reserved for users in the groups you specify here. Fill out the user group names in a colon-separated format, for example, *Standard CUCM SuperUser:MyGroupName*
Enable Microsoft User License Enforcement	Defines whether to Microsoft license allocation is enforced at hierarchy levels. Refer to the related topic below. Default is **Inherit**.
Convert Inactive CUCM LDAP User to Local on Sync	Defines whether to convert CUCM users that would normally be automatically deleted by the CUCM, to be converted into CUCM Local users during a data sync of CUCM. When disabled (default), users that have been in status "Inactive LDAP Synchronized User" for more than 24 hours are automatically deleted by the CUCM. These users and their services are then deleted from Automate on the next CUCM data sync. When enabled, users that have changed their status to "Inactive LDAP Synchronized User" are converted to "Enabled Local Users" on the next CUCM data sync. The data sync of the CUCM must occur within 24 hours of the users becoming inactive otherwise, CUCM will still delete them.
Retain User at Site after MS Offboard User	Defines whether to retain a user at a site instead of moving the user back to customer level when performing the task: Quick Offboard User. The default is **No** (inherited).

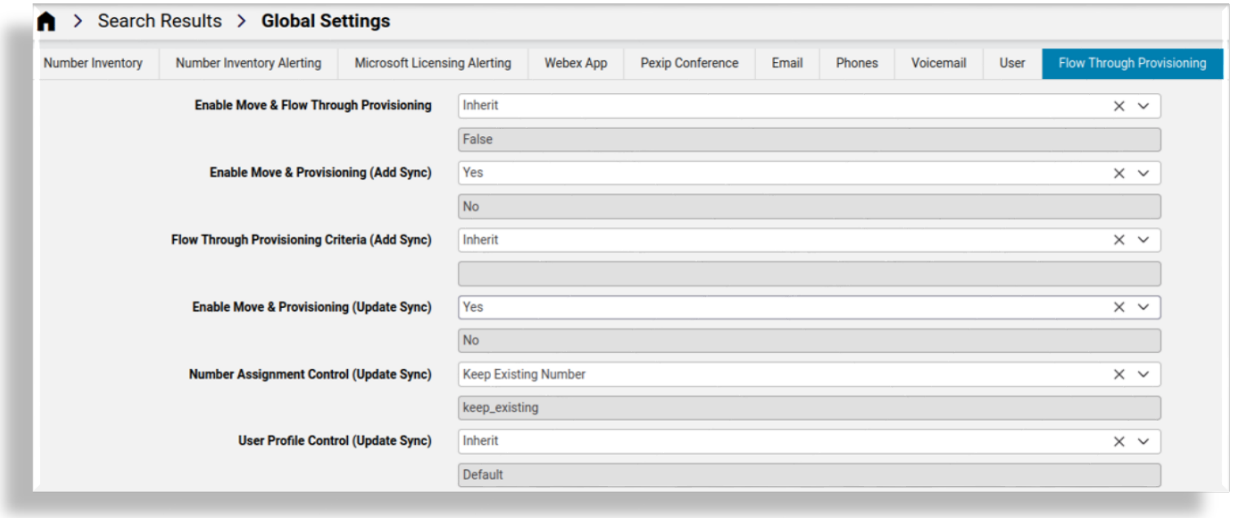
Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- User Authentication Methods in the Core Feature Guide.
- Microsoft License Management and Alerting in the Core Feature Guide
- Convert user type CUCM-LDAP to CUCM Local in the Core Feature Guide.
- Microsoft User Management, Offboard User in the Core Feature Guide.

Flow Through Provisioning

This tab defines global settings for sync with flow through provisioning.



The table describes the settings on the Flow Through Provisioning tab/panel:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Enable Move & Flow Through Provisioning	Defines whether move and flow through provisioning is enabled. The default is No.
Enable Move & Provisioning (Add Sync)	Enabled only when **Enable Move & Flow Through Provisioning** is enabled. Defines whether move and flow through provisioning on *Add* sync is enabled. The default is No.
Flow Through Provisioning Criteria (Add Sync)	Enabled only when **Enable Move & Flow Through Provisioning** is enabled. Used *only* for adding and onboarding users. Defines the default criteria applied in an *Add* sync when moving and provisioning a user with flow through provisioning. The user is synced in, moved to a site, and provisioned with relevant serves in one step, based on the flow through provisioning criteria.
Enable Move & Provisioning (Update Sync)	Microsoft users only. Allows the system to automatically move an existing non-hybrid, Microsoft-only user, from one site to a new site, with their services and a new line, in a scheduled or manually triggered sync. When set to Yes, triggers display of these additional fields to apply controls for move using between sites, and provisioning in an update sync: • Number Assignment Control (Update Sync) • User Profile Control (Update Sync) **Important:** Update syncs for move and flow through provisioning execute *only* on users that are already at Site level. These are users who have already been provisioned at a site and their settings on Azure have changed, therefore requiring a move to another site and, if relevant, changes to their provisioning at the new site. Users synced in at Customer level as Msol users aren't eligible for flow through provisioning. To move and automatically provision these users you can either purge them and sync them in again in an Add sync with flow through provisioning, or manually configure and move them.
Number Assignment Control (Update Sync)	Displays only when **Enable Move & Provisioning after Update Sync** is set to Yes. Update sync only. Defines whether a user keeps their existing number or is assigned a new number when moved from one site to another site. Options are *Inherit* (from the hierarchy settings above this one), *Keep Existing Number* (default), or *Assign New Number*. Note that this is a global setting at the hierarchy where you're applying the setting so all users updated in this move and sync will either inherit settings, or keep their numbers, or be assigned new numbers.
User Profile Control (Update Sync)	Displays only when **Enable Move & Provisioning after Update Sync** is set to Yes. Update sync only. A single default profile used *only* in update syncs with flow through provisioning to apply criteria for moving the user. In an update sync, only this user profile applies for the move. The **Flow Through Provisioning Criteria** setting on this tab/panel applies only for *add* syncs.

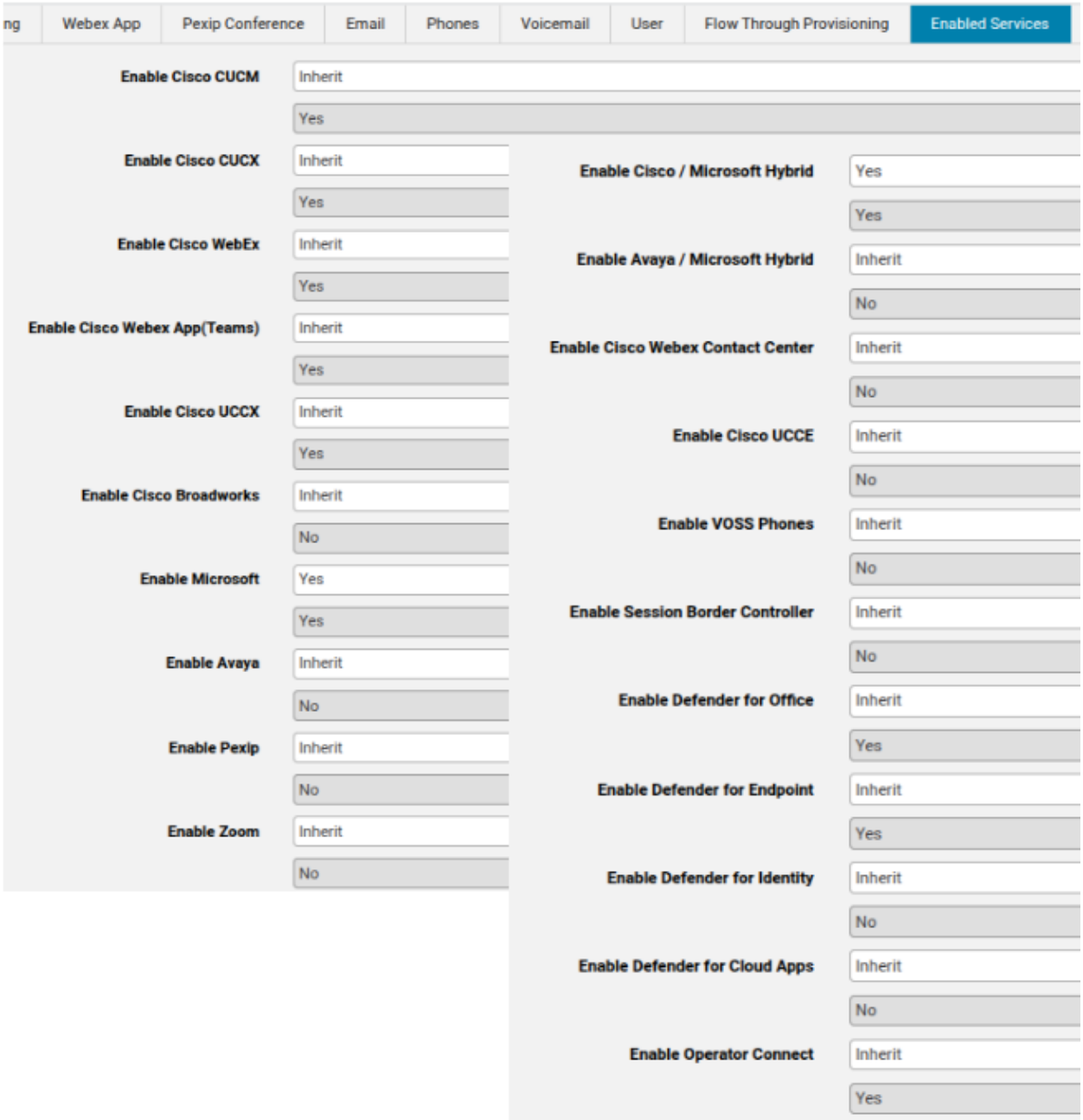
Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Flow through provisioning (FTP) in the Core Feature Guide.
- Move Microsoft user and services in the Core Feature Guide.
- User profiles in the Core Feature Guide

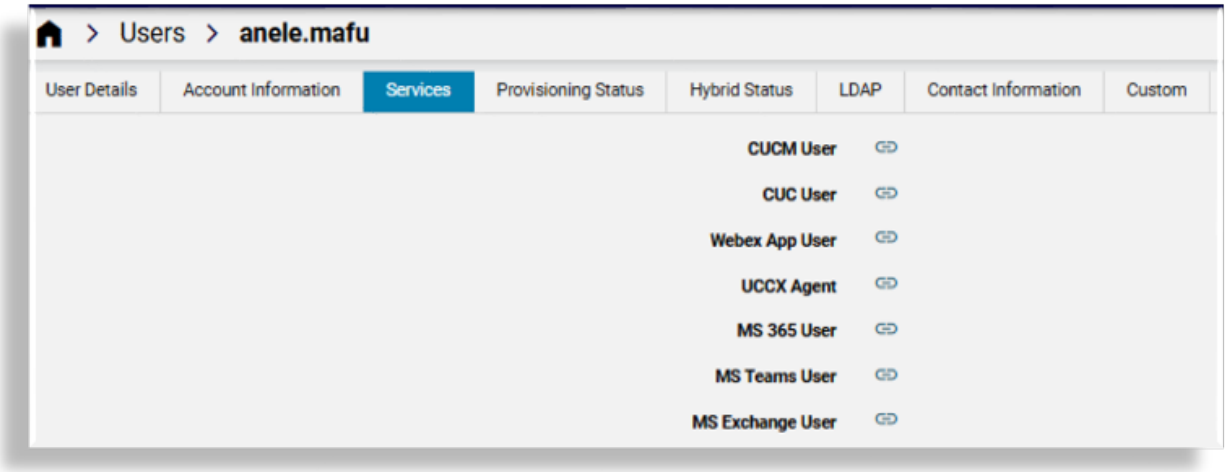
Enabled Services

This tab defines the global settings for enabling/disabling services for different vendors, such as Cisco or Microsoft. Options are Inherit, or Yes/No (True/False).



Copyright © 2025 VisionOSS Limited. All rights reserved.

Services that are available to users and enabled on this tab display on the **Services** tab of the user's management page. When enabled, an admin can click the link to the service details to view and update the settings for that service. For services that the user isn't using, you can disable the service (select *No*) on this tab so that it won't display on their user management **Services** tab/panel.



When provisioning services from two or more vendors, the global setting is the first of a number of system verification checks. For example, when the **Enable Cisco CUCM** global setting is set to **Yes** (enabled), the administrator can provision a user with new CUCM services (such as a Cisco phone, Jabber, and extension mobility), only if the CUCM device check (server installed), entitlement profile check, and field display policy check all pass the verification check. In the same way, if for example, the **Enable Microsoft** global setting is set to **No** (disabled), and all other checks are set to enabled, existing Microsoft services can be viewed but new Microsoft services cannot be provisioned.

Note: By default, for new installs, the global setting for the following services are inherited from higher levels in the hierarchy (Inherit set to True/enabled):

- Cisco CUCM
- Cisco CUCX
- Cisco WebEx
- Cisco Webex App
- Cisco CCX

When upgrading to a version of the system that allows multi vendor and hybrid users, the default setting for services other than these 5 services is *Inherit* (False).

To provision services to new users (added after an upgrade), you will need to enable the vendor service in global settings.

The table describes services that can be enabled/disabled on this tab:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setting	Description
Enable Cisco CUCM	Enables/disables Cisco CUCM services. The default is *Yes*. When set to *Yes*, allows an admin user to provision a user with new CUCM services, such as a Cisco phone, Jabber, and Extension Mobility, provided the server is installed, and the entitlement profile and field display policy pass a verification check.
Enable Cisco CUCX	Enables Cisco CUCX (Unity) services. The default is *Yes*.
Enable Cisco WebEx	Enables/disables Cisco WebEx services. The default is *No*.
Enable Cisco Webex App (Teams)	Enables/disables Cisco WebEx App (Teams) services. The default is *No*.
Enable Cisco UCCX	Enables/disables Cisco UCCX (Contact Center Express) services. The default is *No*.
Enable Cisco Broadworks	Enables/disables Cisco Broadworks services. The default is *No*.
Enable Microsoft	When enabled, allows provisioning of Microsoft services. The default is *No*.
Enable Avaya	Enables/disables Avaya services. The default is *No*.
Enable Pexip	Enables/disables Pexip services. The default is *No*.
Enable Zoom	Enables/disables Zoom services. The default is *No*.
Enable Cisco/Microsoft Hybrid	Enables/disables Cisco/Microsoft hybrid services. The default is *No*. When enabled, Automate allows for provisioning users and services from both Cisco and Microsoft devices, and makes available an admin user parent menu called **Hybrid Cisco-Microsoft Management**, and associated access profiles. For details, see *Hybrid Cisco-Microsoft Management* in the Core Feature Guide.
Enable Avaya/Microsoft Hybrid	Enables/disables Avaya/Microsoft hybrid services. The default is *No*.
Enable Cisco Webex Contact Center	Enables/disables Cisco Webex Contact Center services. The default is *No*.
Enable Cisco UCCE	Enables/disables Cisco UCCE services. The default is *No*.
Enable VOSS Phones	Enables/disables VOSS phones services. The default is *No*.
Enable Session Border Controller	Enables/disables Session Border Controller services. The default is *No*.
Enable Defender for Office	Enables Microsoft Defender for Office - security services for Office 365
Enable Defender for Endpoint	Enables Microsoft Defender for Endpoint - various devices
Enable Defender for Identity	Enables Microsoft Defender for Identity - for identity related threats
Enable Defender for Cloud Apps	Enables Microsoft Defender for Cloud - cloud security tools
Enable Operator Connect	Enables Microsoft Operator Connect for Providers in Automate. When set to Yes (enabled), displays Operator Connect settings in *Additional Apps*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Microsoft Defender for Office security management and policies

Enabled Solutions

This tab lists solutions that can be enabled in your system, provided you have the necessary licenses.

Note: As at the release of 25.3, the following solutions are available and enabled by default (provided you have the required licenses):

- **UC Automation**: Offers the same functionality as shipped in Automate pre-25.3.
- **Email**: Relevant for Microsoft customers using Automate for MS Exchange pre-25.3.

Deployment of the following solution capabilities is reserved for future development: UC Monitoring, UC Analytics, Security, License Management, Meetings Rooms

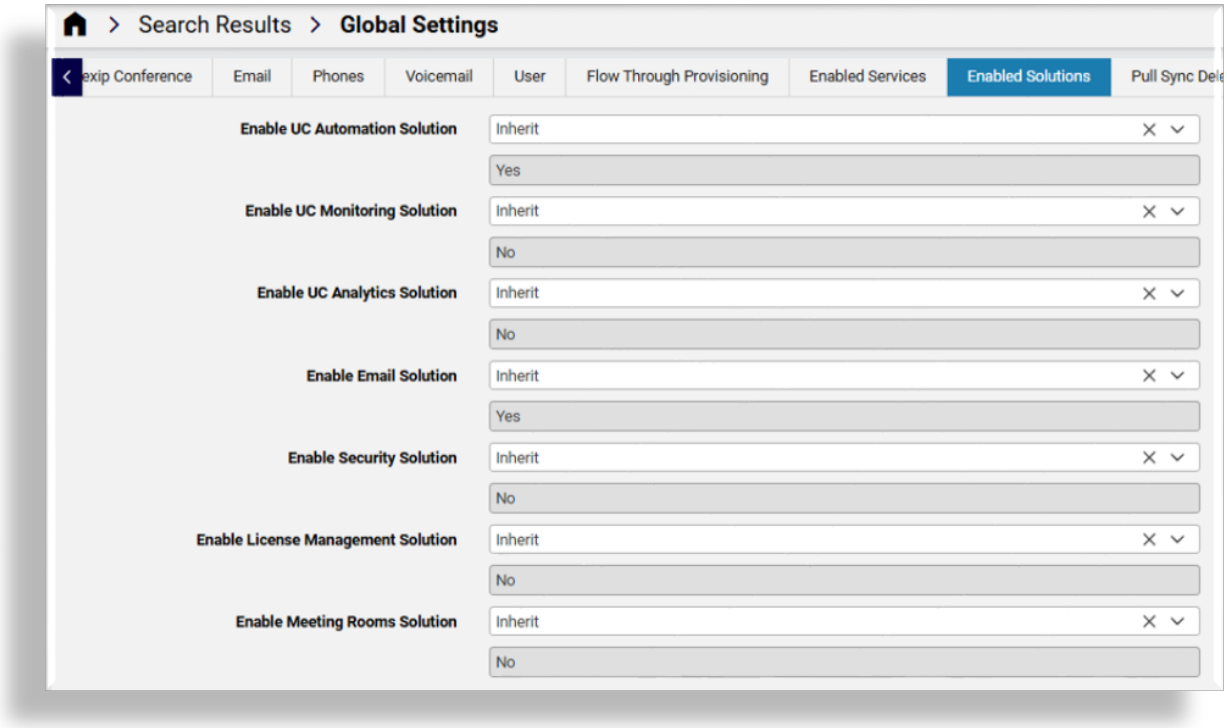
From 25.3, admins setting up a Microsoft tenant can add the tenant, select required solutions, and add the permissions for these solutions to a single application (app) registration directly in the customer tenant. When enabling two or more solutions, you will need to create your own app registration in this way, and add permissions to the app registration in the form of an uploaded certificate and/or a secret. Some solutions will require a certificate and others will need a secret.

Permissions required, by solution:

- UC Automation: Certificate
- Email: Certificate
- UC Monitoring: Secret
- UC Analytics: Secret
- Security: Certificate
- License Management: Certificate
- Meetings Rooms: Certificate

At the time of writing (25.3), shared central app registration can still be used provided you only have a single solution enabled; that is, *UC Automation* or *Email*.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Pull Sync Delete Thresholds

The Pull Sync Delete Threshold settings on the Enabled Services tab allow you to define the maximum number of items that may be deleted during a sync to protect against unwanted sync deletions. You can adjust the default values if needed. Sync will fail if the threshold is reached.

Setting	Description
Pull Sync Delete Threshold for CallManager	Blocks CallManager deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for LDAP	Blocks LDAP deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for MSExchangeOnline	Blocks MSExchangeOnline deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for MSGraph	Blocks MSGraph deletes if calculated number of local deletes exceeds the threshold. Default is 20.
Pull Sync Delete Threshold for MSTeamsOnline	Blocks MS-TeamsOnline deletes if calculated number of local deletes exceeds the threshold. Default is 20.
Pull Sync Delete Threshold for Spark	Blocks Spark deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for UnityConnection	Blocks UnityConnection deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for Zoom	Blocks Zoom deletes if calculated number of local deletes exceeds the threshold. Default is 50.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

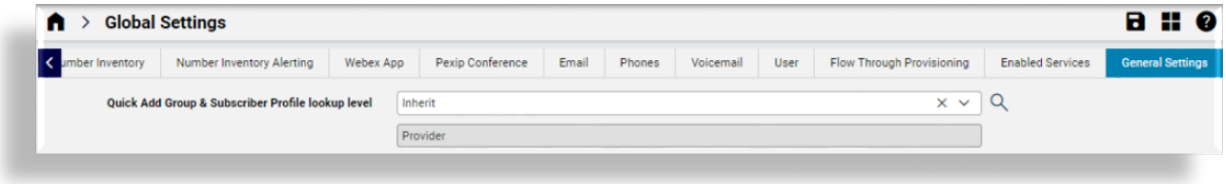
- Multi vendor users in the Core Feature Guide
- Role-based access for multi vendor users in the Core Feature Guide
- Configure multi vendor users in the Core Feature Guide
- Hybrid Cisco-Microsoft Management in the Core Feature Guide

General

This tab defines general global settings to manage system behavior.

The table describes services that can be enabled/disabled on this tab:

Setting	Description
Quick Add Group & User Profile lookup level	Specifies the hierarchy level up to which Quick Add Groups and user profiles will be searched for. The default is Provider level. (`sys` and `hcs` levels are not available.) When a lookup level is set, selections of available QAGs and user profiles will be restricted upwards to this lookup level. If you have hybrid customers (customers using both Cisco and Microsoft, for example), you can create hybrid-specific user profiles for those hybrid customers, then set the lookup level for those customers to *Customer* level so that they will have available a hybrid user profile in the drop-down at that customer hierarchy.



Changing inherited settings

- For numeric inherited values, for example, for “Number Inventory Cooling Duration (Days)” or “Webex App Refresh Token expires threshold (in seconds)”), you can overwrite the word “Inherit” with the required value, for example, 45, and save your changes. If the inherited value is already overwritten, for example, the value is already 45, then overwrite this value with the new value.
- For inherited values that are Yes/No (True/False), select an alternative from the drop-down (either Yes, No, or Inherit). This may change the current value.

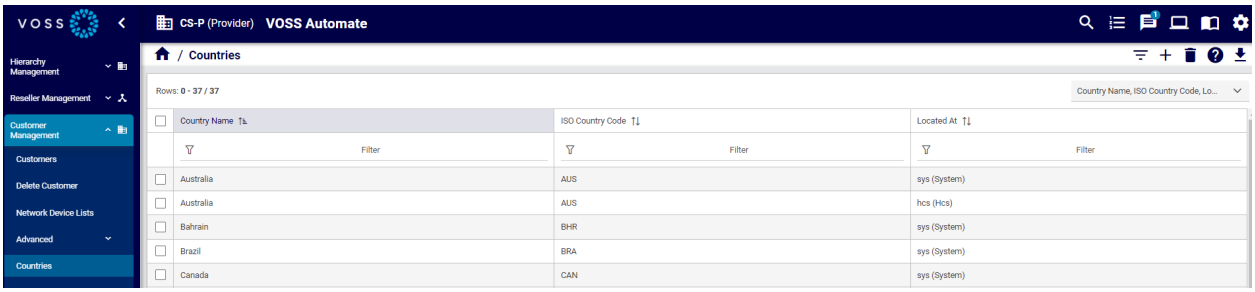
Copyright © 2025 VisionOSS Limited. All rights reserved.

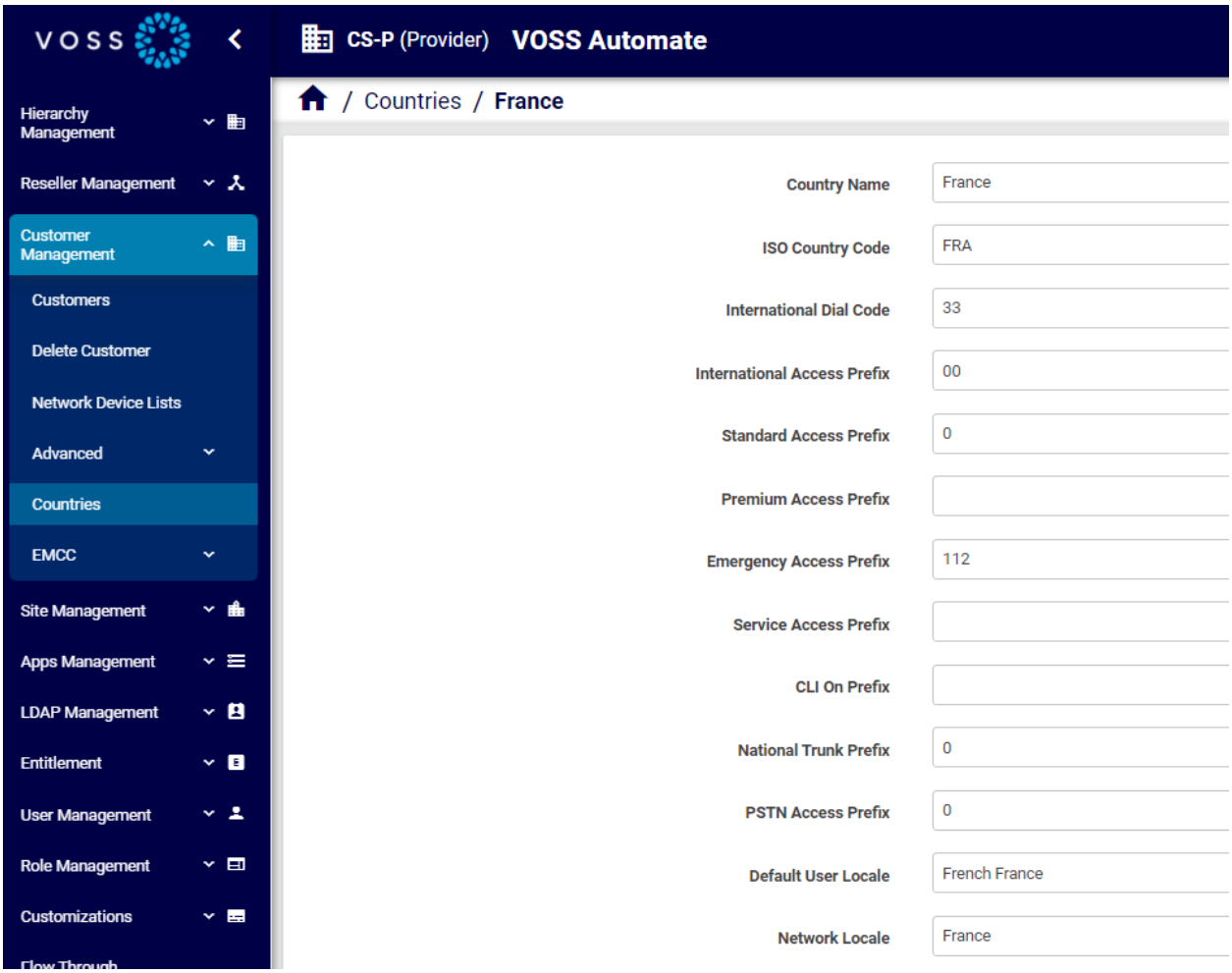
12.5.2. Countries

The **Countries** page in VOSS Automate allows you to view, add, or delete country data for your system. This page displays details such as country codes, international dial codes, access prefixes, and network and user locale information.

You can add, update, or delete country data, perform bulk actions (such as bulk delete, or export the list), and filter data by country name, ISO country code, and located at (hsc or system).

Use the toolbar Action search to go to the **Countries**. See *Use the Action search to navigate Automate*.





Copyright © 2025 VisionOSS Limited. All rights reserved.

12.5.3. Configuration mapping for phones, device profiles, and lines

Tip: *Use the Action search to navigate Automate*

Overview

Configuration mapping is available for higher level administrators as a part of the overall configuration as well as for other purposes.

The table describes the purpose of configuration mapping:

Type	Purpose
For phones and device profiles	• Define the phones types available for selection. • Define the configuration settings used when a specific phone type is selected. • Allow multiple configurations, for example, different button templates for the same phone type. • Provide business-friendly names for different phone type configurations, rather than UCM-defined names. For example: “Executive Phone with 2 lines”. • Make use of phone-type-agnostic configuration templates (CFTs), allowing for the management of fewer CFTs in the system rather than a CFT for each phone type.
For lines, phones and device profiles	Define a set of feature templates for use by lower-level administrators, and customize the configuration of the applicable item. This allows you to have different versions of configuration, as required.
For soft phones (specifically)	Provide CFTs to manage the process of moving the soft phones of users.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Phone configuration mapping

There may only be one phone configuration mapping at any hierarchy. This phone configuration mapping must be `Default`.

Mapping profiles

Mapping profiles define the list of phone types that can be selected, and include:

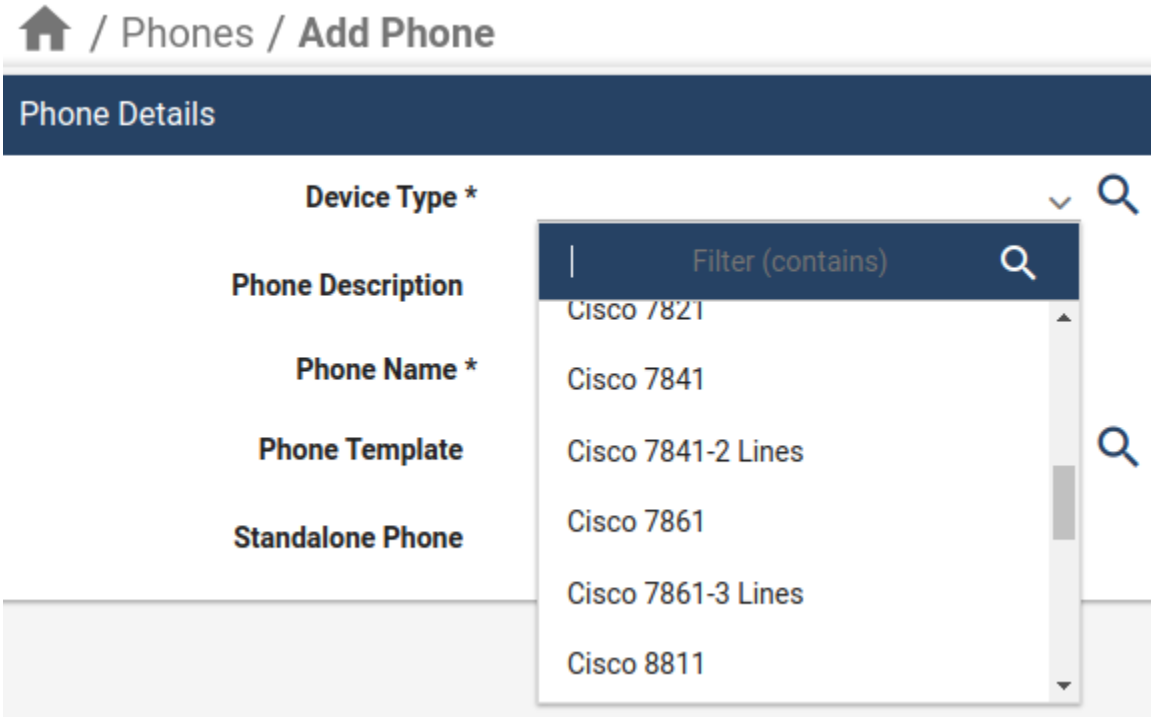
- Profile name
- Profile items: Phone type, Protocol, Button template, Security profile
- Base configuration template (CFT)

	Profile Name	Phone Type	Protocol	Button Template	Security Profile	Base Configuration Template	
	Cisco 7841	Cisco 7841	SIP	Standard 7841 SIP	Cisco 7841 - Standard SIP Non-Secure Profile	Basic Phone CFT	
	Cisco 7841-2 Lines	Cisco 7841	SIP	Standard 7841 SIP-2 Line	Cisco 7841 - Standard SIP Non-Secure Profile	Basic Phone CFT	

The value in the **Profile Name** field is presented to the lower-level administrator user in **Phone** drop-downs in the Admin Portal.

For example, if the administrator selects “Cisco 7841”, then:

- The phone is provisioned as a “Cisco 7841” SIP device
- The phone will have a button template called *Standard 7841 SIP*
- The phone will a security profile called *Cisco 7841 - Standard SIP Non-Secure Profile*
- The phone configuration will come from a basic CFT called *Basic Phone CFT*



Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: The *Base Configuration Template* and the *Feature Configuration Template* may also contain profile item fields such as **Phone Type** and **Protocol**. In this case, the order of precedence for the values is:

1. Feature configuration template
2. Base configuration template
3. Profile items

For example, a phone type specified in the **Phone Type** field under **Profiles** is superseded by the phone type specified in the *Base Configuration Template* or the *Feature Configuration Template*.

Feature templates

The **Feature Templates** section of the Phone and Device Profile configuration mapping allows a higher-level administrator to configure a list of *Feature Configuration Template* CFTs, providing different configurations to complete the setting of the phone, device profile or line.

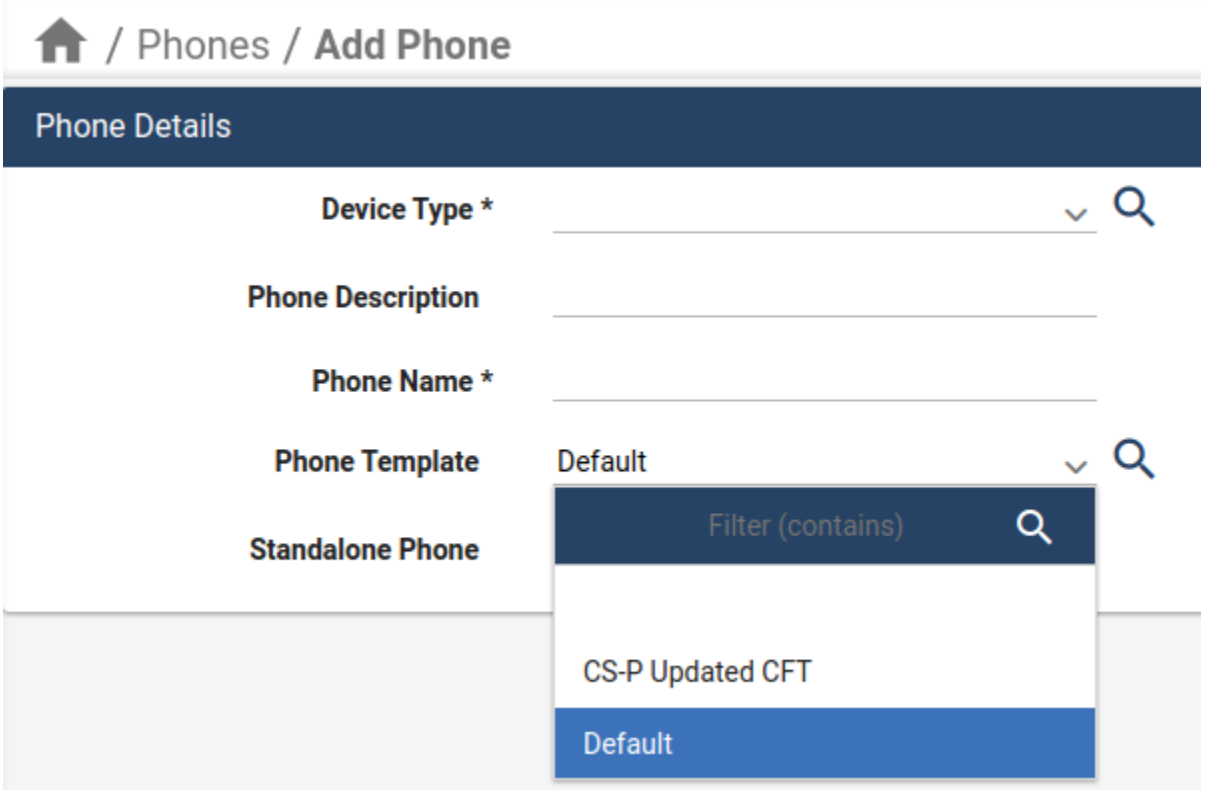
The image shows the list of available Feature templates:

Feature Templates

	Template Name	Feature Configuration Template	
	Default	Default Phone Feature CFT	
	CS-P Updated CFT	CS-P Phone Template BAP	

The Feature templates are presented to the lower-level administrator as the list of templates (phone, device profile or line) that can be chosen when adding either a phone, extension mobility, or line. The *Feature* templates will contain the additional configuration settings that are applied on top of the settings mentioned above.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Macros for phone configuration mapping

The table describes the available context macro variables when defining configuration templates for the phone mappings:

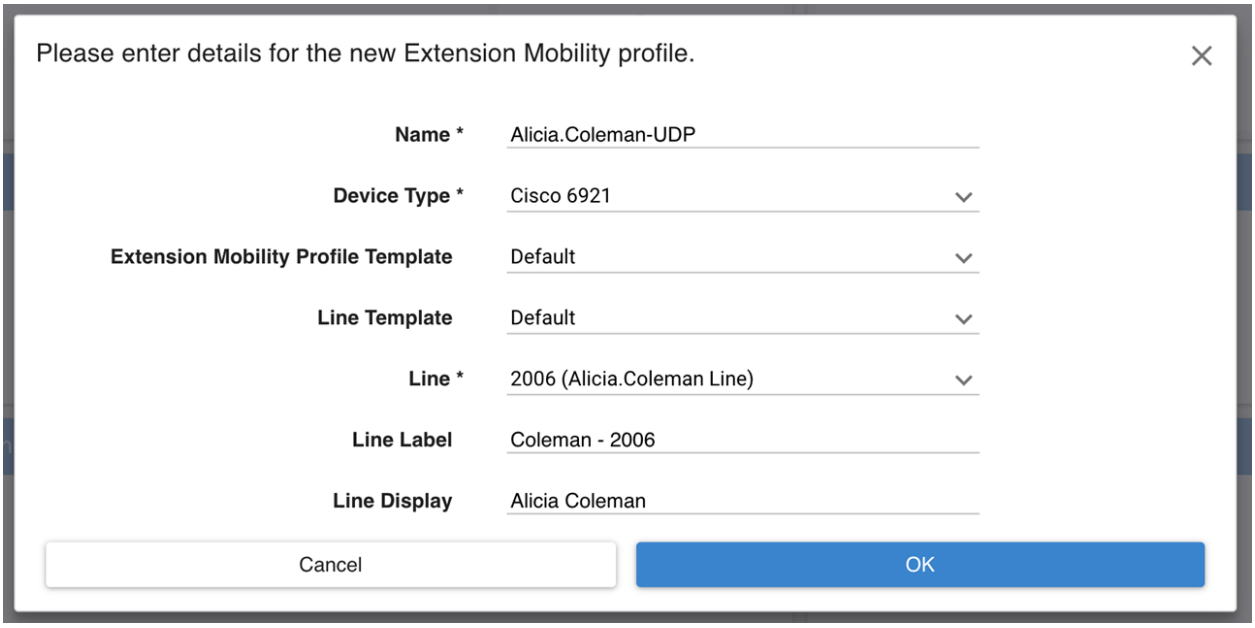
Copyright © 2025 VisionOSS Limited. All rights reserved.

Macro	Description
`{{ input.standalone }}`	Flag whether it is a standalone phone or being associated with a user.
`{{ input.username }}`	Username of the user the phone is being associated with. Only when standalone is false.
`{{ input.device_type }}`	The user selected device type. This in fact is the phone mapping profile name.
`{{ input.template_name }}`	The user selected feature template.
`{{ input.name }}`	The user entered phone name.
`{# input.lines #}`	The user entered list of lines.
`{{ input.lines.0. directory_number }}`	The number of the first line.
`{{ input.lines.0. template_name }}`	The user selected line template.
`{{ input.lines.0.label }}`	The user entered line label.
`{{ input.lines.0.display }}`	The user entered line display.
`{{ pwf.user }}`	Object containing all UCM user settings of the associated user. Only when standalone is false.

Device profile configuration mapping

There may only be one device profile configuration mapping at any hierarchy, and the name of this mapping (at any hierarchy) must be `Default`.

The setup for device profile configuration mapping is identical to the phone configuration mapping. The phone type list and *Feature** templates are presented to the administrator when adding an extension mobility service to a user via **User Management**. See *Feature Templates* under *Phone configuration mapping*.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Line configuration mapping

There may only be one line configuration mapping at any hierarchy, and this line configuration mapping (at any hierarchy) must be `Default`.

A list of line templates can be configured and these will be presented to the administrator when new lines are be created, for example when adding a new phone.

Macros for line configuration mapping

The table describes the available context macro variables when defining configuration templates for the line mappings:

Macro	Description
`{{ input.userid }}`	User ID for description.
`{{ pwf.PassedLine.pattern }}`	Line pattern description.
`{{ input.firstName }}`	User first name for Alerting name or ASCII Alerting name.
`{{ input.lastName }}`	User last name for Alerting name or ASCII Alerting name.
`{{ input.Phone.0.lines.line.0.dirn.pattern }}`	The destination.

The table describes the named macros that can be used when defining configuration templates for the line mappings. High-level administrators with access to `data/Macro` can inspect and evaluate these named macros to verify result values. For details on Configuration Template customizations, see the *Advanced Configuration Guide*.

- For `callingSearchSpaceName`

```
{{ macro.CUCM_LINE_callForwardAll_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardAlternateParty_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardBusy_callingSearchSpaceName-2 }}
{{ macro.CUCM_LINE_callForwardBusyInt_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardNoAnswer_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardNoAnswerInt_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardNoCoverage_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardNoCoverageInt_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardNotRegistered_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardOnFailure_callingSearchSpaceName }}
{{ macro.CUCM_LINE_callForwardOnFailure_callingSearchSpaceName }}
```

- For `presenceGroupName`

```
{{ macro.CUCM_LINE_presenceGroupName }}
```

- For `routePartitionName`

```
{{ macro.CUCM_LINE_routePartitionName }}
```

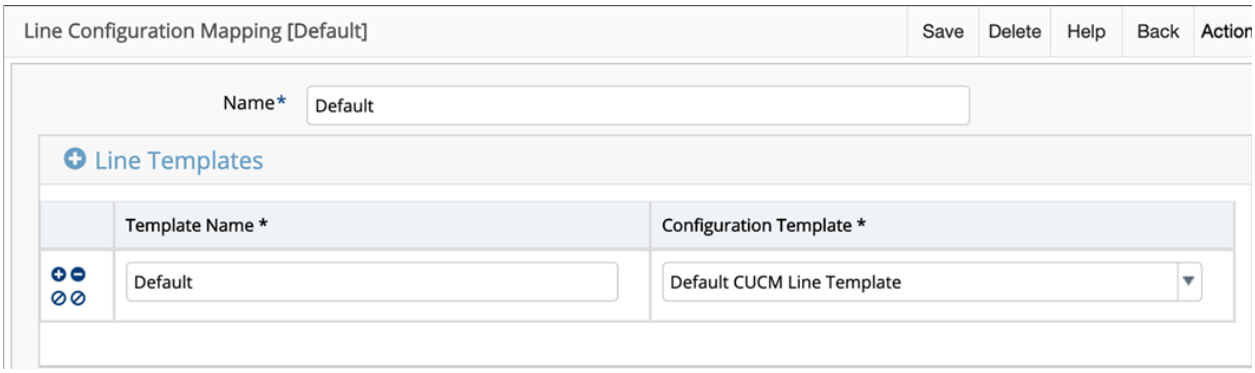
Copyright © 2025 VisionOSS Limited. All rights reserved.

- For `secondaryCallingSearchSpaceName`

```
{{ macro.CUCM_LINE_callForwardAll_secondaryCallingSearchSpaceName }}
```

- For `voiceMailProfileName`

```
{{ macro.CUCM_LINE_vmprofile }}
```



12.5.4. Line delete preferences

Tip: *Use the Action search to navigate Automate*

When deleting a phone, device profile, or remote destination profile from Automate, the line or lines (Cisco UCM lines) in use by the phones or devices are not automatically deleted.

Automate's **Line Delete Preferences** allow a Reseller (or higher) administrator to define whether the lines are deleted when deleting the phone or device, or updated (using values contained in a specified configuration template).

You can configure the following via the **Line Delete Preferences** page:

- Allow deletion of a line
- Allow update of a line
- Configuration template to use for update (if enabled)

When:

- a phone, device profile or remote destination profile is deleted
- a line is deleted or changed from a phone, device profile or remote destination profile

then the following logic applies:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Allow Line Deletion if unused	• If the line is not shared with another phone or device, the line is deleted and the number inventory updated. See *Lines*. • If the line exists on another phone belonging to the same user as the deleted device, no action is taken. • If the line is shared with an MGCP Gateway Endpoint, no action is taken.
Allow Line Update after Device Deletion	• If the line is not shared with another phone or device, the line is updated with the details from the selected configuration template. • If the line is shared with another phone or device belonging to another user, the line is updated with the details from the selected configuration template specified in **Line Update Configuration Template name**. • If the line is shared with another phone or device belonging to the same user, no update is performed.

Note: To determine the user associated with a phone, the owner ID must be set on the deleted phone.

Affected Models

- Model Type: device/cucm/Phone
  - Operation: Delete
  - Phase: Post Execution
  - Workflow: LineDeletion_PhoneDataSync_PWF
  - Synchronous: False
- Model Type: device/cucm/DeviceProfile
  - Operation: Delete
  - Phase: Post Execution
  - Workflow: LineDeletion_PhoneDataSync_PWF
  - Synchronous: False
- Model Type: device/cucm/RemoteDestinationProfile
  - Operation: Delete
  - Phase: Post Execution
  - Workflow: LineDeletion_PhoneDataSync_PWF
  - Synchronous: False

Copyright © 2025 VisionOSS Limited. All rights reserved.

12.6. License Audit Setup

12.6.1. Distributing Licensing Reports

As part of the license reporting process, the product has multiple options to enable sending the generated license report files automatically and/or to make them available via the admin portal. This simplifies the collection of the files for internal use as well as sending to VOSS as required. It is highly recommended that at least one of the options is set up to make the process of file collection/sharing easier in the environment.

The easiest and most recommended approach to sharing the file with VOSS is to utilize the **VOSS Cloud Licensing Service**. This process will register your platform which streamlines support engagement but also will automate the license audit collection required. This can be used in conjunction with the other automatic file sending options for internal use as needed. However if this is not possible, there are a number of other options to still streamline getting the file which can then be sent on to VOSS.

As a reminder, for internal use, the license audit data can be reviewed via the admin portal and does not require the files to be viewed.

Further details are available in Viewing License Audit Counts in the Licensing and Subscriber Data Export Guide.

In order to set up automated handling of the generated license audit report, the summary of steps are:

1. Decide the destination(s) and the file for each destination
2. Set up the destinations and related configuration
3. Validate that the destinations are utilized when the file is generated (via schedule or adhoc).

In the event that it is required, you can also access the files via SFTP to the platform:

- Connect to the primary node IP using SCP or SFTP on port 22.
- The extracts will be located in the `media/data_export/license/` directory.
- Collect the appropriate file(s)

Configure License Delivery

System administrators with the required permissions (default is sysadmin) have the option from the **Licensing** menu to configure the delivery of the audit data by means of one or more of the following delivery methods and combine them into one or more **File Transfer Destinations**. These destinations can then be used to transfer the audit data.

The delivery method configuration can be accessed from the menus:

- **VOSS Cloud Licensing Service** (recommended)
  - Automatically upload license audit files to the VOSS Customer Portal - see: *VOSS Cloud Licensing Service*.
- **Email Destinations**
  - Requires an SMTP server configured on the **SMTP Server** menu. (*Add a SMTP Server*)
  - Destination name, SMTP server, sender, addressee and email subject are mandatory.
  - Options can be input for email addressees, otherwise the addressee is the sender.
- **File Destinations**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Allows for data files to be stored in the database and downloaded via the **Audit Report Files** menu.
  - A mandatory **Name** at either the `sys` hierarchy level or provider hierarchy level is added to define the file destination.
  - If this destination is used, as an instance of the **File Transfer Destinations**, the **Audit Report Files** menu shows the list of data files at the specified hierarchy level. Files on the system starting with `vlf` are listed here.

    Note: If needed, the files can be deleted from the list, but this action does not remove files saved to the file system.

    To download the files, choose **Export** > **JSON** from the menu bar. The export will be a `.zip` file with a `FILES` directory containing all the files selected in the list view.

- **HTTP Destinations**
  - Destination name, hostname, HTTP method and URL endpoint must be provided.
  - Options are available for user credentials, port, a secure connection and a client certificate.
- **SFTP Destinations**
  - Destination name, hostname and username is mandatory
  - Options are available for port, user password and destination directory
- **Web Proxies**
  - Proxy setup for delivery methods using web proxies - see: *Set up a Web Proxy*.

When the required methods have been configured, the scheduled audit data collection can also deliver the data files by these methods.

Workflow steps:

1. Set up one or more delivery method destinations listed above.
2. Combine configured delivery method destinations into one or more file transfer destinations (**File Transfer Destinations** menu).
3. On the **Settings** menu:
   - Configure one or more settings instances that combines a file transfer destination and a file format and save the settings.
   - The **File format** options correspond with the available audit report file types.

     For details on the format and contents, refer to the Licensing and Subscriber Data Export Guide.

     - `Anonymous ZIP` (file format: `vlf_<provider_name>_<host_name>_license_<YYYY-MM-DD_HHMM>.zip`)

       Contains `<YYYY-MM-DD_HHMM>_license` directory with files of format:

       * `vlf_<provider_name>_<host_name>_anonymous_<YYYY-MM-DD_HHMM>.csv`
       * `vlf_<provider_name>_<host_name>_anonymous_<YYYY-MM-DD_HHMM>.csv.hash`

       The files with `_breakdown_` in the name refer to Microsoft license usage.

       * `vlf_<provider_name>_<host_name>_anonymous_breakdown_<YYYY-MM-DD_HHMM>.csv`

Copyright © 2025 VisionOSS Limited. All rights reserved.

    * `vlf_<provider_name>_<host_name>_anonymous_breakdown_<YYYY-MM-DD_HHMM>.csv.hash`

  Additional files:

    * `vlf_<provider_name>_<host_name>_adaptation_log_<YYYY-MM-DD_HHMM>.json`
    * `vlf_<provider_name>_<host_name>_adaptation_log_<YYYY-MM-DD_HHMM>.json.hash`
    * `vlf_<provider_name>_<host_name>_patch_<YYYY-MM-DD_HHMM>.json`
    * `vlf_<provider_name>_<host_name>_patch_<YYYY-MM-DD_HHMM>.json.hash`

  – `Detailed ZIP` (file format: `vlf_<provider_name>_<host_name>_license_detailed_<YYYY-MM-DD_HHMM>.zip`)

    Contains `<YYYY-MM-DD_HHMM>_license_detailed` directory with files of format:

    * `vlf_<provider_name>_<host_name>_detailed_<YYYY-MM-DD_HHMM>.csv`
    * `vlf_<provider_name>_<host_name>_detailed_<YYYY-MM-DD_HHMM>.csv.hash`

    The files with `_breakdown_` in the name refer to Microsoft license usage.

    * `vlf_<provider_name>_<host_name>_anonymous_breakdown_<YYYY-MM-DD_HHMM>.csv`
    * `vlf_<provider_name>_<host_name>_anonymous_breakdown_<YYYY-MM-DD_HHMM>.csv.hash`

    Additional files:

    * `vlf_<provider_name>_<host_name>_adaptation_log_<YYYY-MM-DD_HHMM>.json`
    * `vlf_<provider_name>_<host_name>_adaptation_log_<YYYY-MM-DD_HHMM>.json.hash`
    * `vlf_<provider_name>_<host_name>_patch_<YYYY-MM-DD_HHMM>.json`
    * `vlf_<provider_name>_<host_name>_patch_<YYYY-MM-DD_HHMM>.json.hash`

- More than one combination of destination and file format can be set up if needed.
- An option is available to test the delivery of sample dummy data from an instance of the settings, in other words, delivery to the configured destinations.

4. At the scheduled collection date of the system or when the command is run manually on the platform CLI, the files are then:
   - saved to the platform filesystem (see Licensing and Subscriber Data Export Guide)
   - transferred to destinations and with methods according to the configured **Settings** combination(s) of: file transfer destination and file format
   - if the **File Destinations** destination is used:
     – available for export on the GUI from the **Audit Report Files** menu
     – an entry is shown in the transaction log (*data/File save* with either *succeeded* or *failed*)

Copyright © 2025 VisionOSS Limited. All rights reserved.

VOSS Cloud Licensing Service

In order to automate the retrieval of the VOSS license audit files from the system to deliver them to VOSS as required, the files can automatically be uploaded to the VOSS Customer Portal.

The integration and automation is carried out by:

- Capturing and activating customer organization details on VOSS Cloud Licensing Service from VOSS Automate:
  - *Set up the VOSS Cloud Licensing Service*
  - *Set up a Web Proxy*
- Automatic inclusion upload of license audit files to the VOSS Cloud Licensing Service when the system runs an internal schedule to generate monthly license reports.
  - License Count in the Licensing and Subscriber Data Export Guide.

Set up the VOSS Cloud Licensing Service

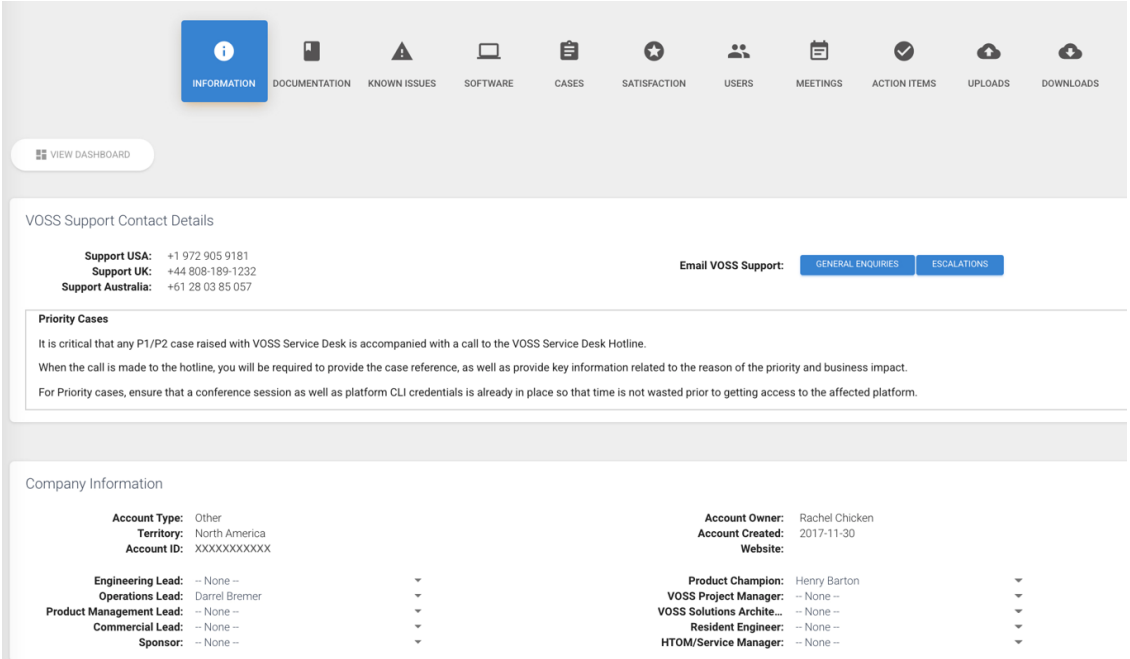
VOSS Automate provides options to set up your VOSS Cloud Licensing service. The system registers your VOSS Cloud Licensing Service when saving the form.

Before you start

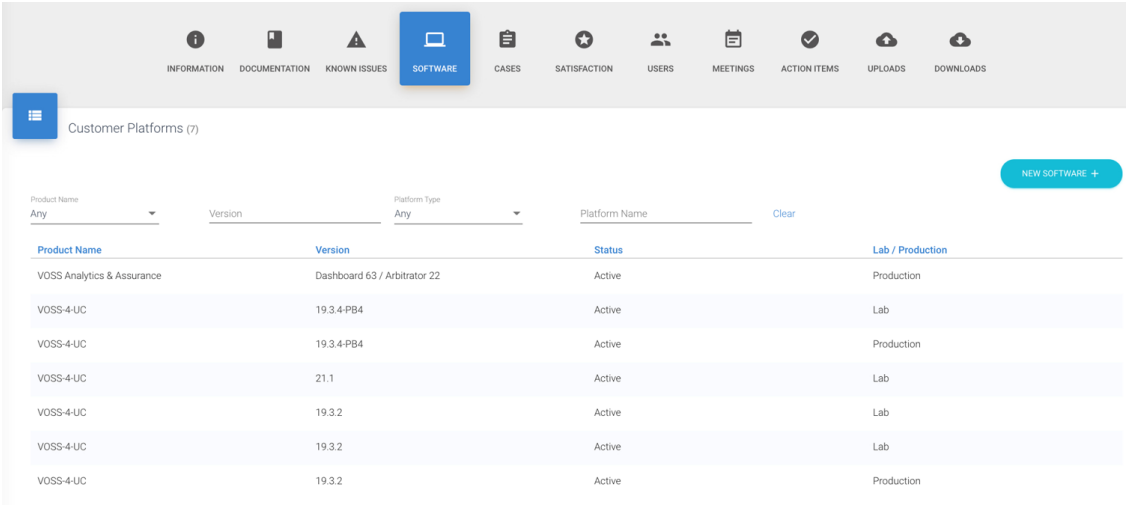
1. Open these ports to communicate with the VOSS Customer Portal:
   - Default HTTP: port 80
   - Default HTTPS: port 443

     See Network Communications External to the Cluster in the Installation Guide.
2. Add the host name to an allowlist for trusted servers: platform.voss-solutions.com
3. Obtain license details for your organization from the **VOSS Customer Portal**, at voss.portalshape.com/organisations:
   - On the **Information** tab, locate and copy your **Account ID**.

Copyright © 2025 VisionOSS Limited. All rights reserved.



- On the **Software** tab, identify the installation type (Lab or Platform), and copy the platform name.



To add and activate the license

1. Log in to the Admin Portal as a high-level administrator (system admin or above).
2. Go to **Administration Menu > Licensing > VOSS Cloud Licensing Service**.
3. In the **Organization ID** field, enter the account ID you obtained from the VOSS Customer Portal.
4. In the **Customer account information** field, enter the platform name you obtained from the VOSS Customer Portal (or enter a new server name) to identify your VOSS Automate installation.
5. Choose your **Installation Type**, either `Lab` or `Production`, as obtained from the VOSS Customer Portal.
6. At the **File format** drop-down, choose your file format. `Anonymous ZIP` and `Detailed ZIP` both include a checksum hash.

Copyright © 2025 VisionOSS Limited. All rights reserved.

See also the Data Export Types section in the Licensing and Subscriber Data Export Guide.

7. Choose whether to enable **File Upload Active**.
8. If a web proxy is required, ensure that it is set up on the **Web proxy** menu and choose it from the drop down.

   For web proxy setup, see *Set up a Web Proxy*.
9. Click **Save**.

Note:

- Save will fail if no internet connection can be established to the VOSS Cloud Licensing Service.
- Once the configuration is saved, the connection to the VOSS Cloud Licensing Service can be tested through the **Test Connection** actions on the form when investigating failures to upload license data files.
- In the unlikely event that it is required to change the **Organization ID** associated with the platform, it is possible to modify the instance, which will attempt to re-register the platform with the VOSS Cloud Licensing Service. A failure will rollback the configuration to the previous state.

Add a SMTP Server

This procedure adds a SMTP server at a hierarchy level.

Prerequisites:

- Enable email in the Global Settings (Email tab).

Perform these steps:

1. Log in to the Admin Portal.
2. Choose the relevant hierarchy.

   Note: Configure the SMTP server at the hierarchy where you want to allow VOSS Automate to send email messages.

   You may only set up one SMTP server at each hierarchy level. The SMTP server will be available at the current hierarchy and below. For example, for a SMTP set up at a specific customer, the sites below that customer can use that SMTP server.

   ---

3. Go to (default menus) **Apps Management > SMTP Server**.
4. Click the toolbar Plus sign (+) to add a new SMTP server.
5. On the **SMTP Server** form, fill out details for the new SMTP server in the form fields:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Name	The SMTP server name.
Description	A description for the email account.
Port	The port number.
Secure	Relevant only for SSL connections to the SMTP server. Select the checkbox (enable) to use the SSL protocol for connections to the SMTP server. Default is disabled (checkbox is left clear), for TLS and unsecure logins to the SMTP server.
Username	The username credential for establishing a connection to the SMTP server.
Password	The password credential for establishing a connection to the SMTP server.

6. Save your changes.

Related Topics

- Email in the Core Feature Guide
- Global Settings in the Core Feature Guide

12.7. Entitlement Management

12.7.1. Introduction to entitlement

Tip: *Use the Action search to navigate Automate*

Overview

Entitlement in Automate represents the set of rules for the suite of services and devices available to specified users.

Note: Entitlement is an optional feature. When adding or updating a user, you can choose whether to assign an entitlement profile.

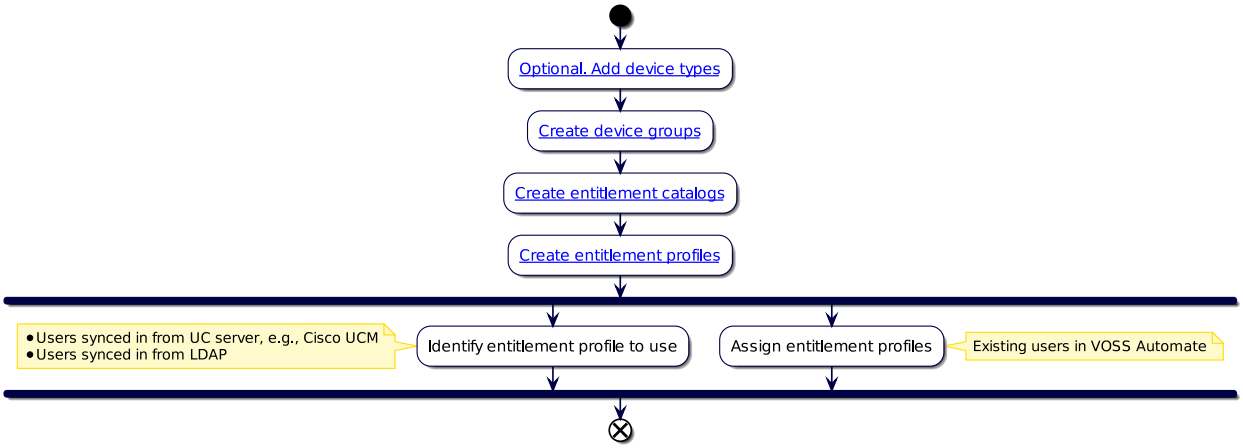
Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Add Device Type in the Core Feature Guide
- Create Device Group in the Core Feature Guide
- Create an Entitlement Catalog in the Core Feature Guide
- Create an Entitlement Profile in the Core Feature Guide

Entitlement workflow in Automate

The diagram provides an overview of the entitlement set up workflow:



The table provides an example for how customers could define different entitlement rule sets for their users:

Customer A	Creates entitlement rules that allows their end users to have: • Voice service only • Maximum of two devices: – One device being a flavor of IP set – One device being an analog set
Customer B	Creates entitlement rules that allows their end users to have: • Voice service • Voicemail service • Maximum of ten devices (limited to SIP sets)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Entitlement components

The table describes entitlement components. These are the the Automate models and the rules that define how entitlement works in the system:

Model	Description
Device types	One or more physical devices, which may be grouped into device groups for entitlement purposes. Device types must correspond with supported product types available for the UC vendor, for example, Cisco or Microsoft. The device type data model is pre-populated with a snapshot of current product types. Provider admins can add, update, or remove device types.
Device groups	A group of device types. The same device types may exist across different device groups Provider admins can add, update, or remove device groups. Reseller and customer admins can only view device groups.
Entitlement catalogs	Defines the supported device groups and available services at a particular hierarchy. Within a device group you also specify the maximum allowed total number of devices, and the maximum allowed number of devices in each device group in the catalog. Provider admins can add, update, and delete entitlement catalogs at their hierarchy level and below. Reseller and customer admins can only view entitlement catalogs.
Entitlement profiles	Defines a set of services, device groups, and device limits to which an end user may be subscribed. • Initial settings are inherited from the first entitlement catalog above it in the hierarchy. • Service and devices allowed in the profile can't exceed those allowed by the associated entitlement catalog. Provider admins can add, update, and delete entitlement profiles at their hierarchy level and below. Reseller and customer admins can only view entitlement profiles.
Entitlement defaults	Default entitlement profiles can be set up and assigned in Automate, but in some cases, the default is based on settings outside of Automate, depending on how users are added to Automate. See Default Entitlement Profiles

Copyright © 2025 VisionOSS Limited. All rights reserved.

Default entitlement profile

Entitlement defaults work differently depending on how a user is added to Automate:

User add option	Description
Bottom-up (UCM user sync)	This is based on the entitlement profile setting on the UCM server (publisher) the user is being synced from. The default entitlement profile is not used in this path.
Quick Add User	This assigns the entitlement profile selected on the portal/loader by the administrator who adds the user. When using Quick Add User via the portal, it pre-populates the entitlement drop-down with the entitlement profile tagged as default.
LDAP Top-down	Entitlement is determined by the entitlement profile setting on the LDAP User sync that is syncing the user in. The default entitlement profile is not used in this path.
Admin Portal or loader	User added via User Management. This uses the value provided via the Admin Portal or loader. The default entitlement profile is not used in this path.

Important: When a user has an empty value for their entitlement:

- If the user's entitlement value is blank, and none of the entitlement profiles in the user's hierarchy tree have the **Default Profile** checkbox selected (set to true), then no entitlement profile is applied and no entitlement checking is done. This means all services and all phones are available to the User.
- If the user's entitlement value is blank, and one of the entitlement profiles *does* have the **Default Profile** checkbox selected (set to true), in the user's hierarchy tree, then the user will inherit this entitlement profile.
- If the **Default Profile** checkbox is cleared (set to false) from one entitlement profile and added to another entitlement profile, then this new entitlement profile will become the default profile applied to all users in the hierarchy below whose entitlement profile is blank.

12.7.2. Add a device type

Automate is prepopulated with a list of current product types. However, the provider administrator may add additional device types as needed.

Add a new device type:

Tip: *Use the Action search to navigate Automate*

1. Log in as provider administrator.
2. Go to **Device Types** for entitlement (default).
3. Click **Add**.
4. Enter the new device type.
5. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

The new device type is added to the list of available device types that can be assigned to a device group.

12.7.3. Entitlement catalogs

Overview

Entitlement catalogs are used in entitlement to limit the devices and services that entitlement profiles (those defined at the same hierarchy or below) may assign to users.

Entitlement catalogs can be defined at the provider, reseller, or customer hierarchy level. Only one entitlement catalog may be defined at a given hierarchy node.

Note: The animation shows the procedure for creating both an entitlement catalog *and* an entitlement profile. An entitlement catalog must exist at or above the hierarchy level at which you want to create the entitlement profile.

Add an entitlement catalog

Tip: *Use the Action search to navigate Automate*

Pre-requisites:

- An entitlement catalog must exist at Provider level.
- Device groups you want to add to a catalog at the current hierarchy must first be added to a catalog higher in the hierarchy. For example, before adding a device group to a catalog at Customer level, you'll need to add the device group to a catalog at Provider or Reseller level.

To add an entitlement catalog:

1. Log in as provider administrator.
2. Choose the hierarchy where you want to create the entitlement catalog.

   Note: You can only create one entitlement catalog at each hierarchy.

3. Go to **Catalogs**.
4. Click **Add**.
5. On the **Catalogs** page, complete the basic configuration for the new entitlement catalog:
   - Enter a name and optionally, a description.
   - Choose the services to include in this entitlement catalog. Options are: Voice, Voicemail, Presence, Extension Mobility, Single Number Reach, Conferencing, Collaboration.
   - Specify the maximum number of devices allowable for the entitlement catalog. The maximum number can't exceed the total of the maximums for all the device groups included in the entitlement catalog.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: Restrictions defined for device groups, device counts, and services in a catalog at a particular hierarchy apply to entitlement profiles and catalogs at that hierarchy, and below. For example, restrictions in a catalog at customer level apply at that customer and to all sites below the customer.

Also:

- An entitlement profile can't be more restrictive than its associated entitlement catalog.
- An entitlement catalog can't be more restrictive than an entitlement catalog at a higher level of the hierarchy.

6. Add device groups:

Important: While one entitlement profile can have many device groups, device types in those groups must be unique across these groups. The same device can't be added to more than one device group.

   - Click the Plus (+) icon at **Device Groups**.
   - From the **Device Group** drop-down, choose a device group to include in the entitlement catalog.
   - Specify the maximum number of devices allowed for the selected device group. The maximum number for any device group can't exceed the maximum number of devices for the catalog.
7. Click the Plus icon (+) to add more device groups to the entitlement catalog.
8. Click **Save** to add the new catalog.

   Next steps:

   - Create entitlement profiles, at or below the hierarchy level of the entitlement catalog (see: *Entitlement profiles*).

12.7.4. Add device group

Tip: *Use the Action search to navigate Automate*

1. Log in as provider administrator.
2. Go to **Device Groups**.
3. Click **Add**.
4. Enter a name and optional description for the device group.
5. Choose devices from the list of available device types and move them into the selected list by clicking **Select**.
6. Click **Save** to create the device group.

   You can use the device group in entitlement catalogs and in entitlement profiles.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Entitlement enforcement*

12.7.5. Entitlement profiles

Tip: *Use the Action search to navigate Automate*

Overview

Entitlement profiles are used to define the services and devices a user is entitled to.

An entitlement catalog restricts the service and devices that can be assigned via an entitlement profile. An entitlement profile can further restrict the services and devices that may be assigned to a user. An entitlement profile can't give a user more services and devices than what is defined in the entitlement catalog.

You can assign an entitlement profile to users when:

- Syncing users into Automate from LDAP.
- Syncing users into Automate from a UC server, such as Cisco Unified Communications Manager (UCM).
- Adding or updating a user Automate via User Management.

Note: The animation shows how to create an entitlement catalog *and* an entitlement profile. An entitlement catalog must exist at or above the hierarchy level at which you want to create the entitlement profile.

Add entitlement profile

Tip: *Use the Action search to navigate Automate*

Prerequisites:

- Add an entitlement catalog at or above the hierarchy node where you're adding the entitlement profile. See *Entitlement catalogs*

To create an entitlement profile:

1. Log in as provider administrator.
2. Choose the hierarchy where you want to create the entitlement profile.

   Note: You can add multiple entitlement profiles at any hierarchy, provided each entitlement profile has a unique name at that hierarchy.

3. Go to **Profiles**.
4. Click **Add**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

5. Configure at least the mandatory values:

Note: The Maximum Number of Devices and Maximum Number of Devices in a Group are limitations for each individual user, not for all users in the system.

Field	Description
Name	Mandatory. The entitlement profile name. The name must unique within the hierarchy.
Description	Optional. Provide a description of the entitlement
Default Profile	Defines whether this is the default entitlement profile at this hierarchy node. Any other entitlement profile at this hierarchy node that was previously chosen as the default is now no longer the default.
Available Services	Choose the services to assign via this entitlement profile: • Voice • Voicemail • Presence • Extension Mobility • Single Number Reach • Conferencing • Collaboration • Contact Center
Maximum Number of Devices	Mandatory. Defines the maximum number of devices allowed for this entitlement profile. The maximum number cannot exceed the total of the maximums for the entire device group included in the entitlement profile.
Device Group	Mandatory. Choose a device group to include in this entitlement profile.
Maximum Number of Devices in Group	Mandatory. For the selected device group, specify the maximum number of devices allowed. The maximum number for any device group cannot exceed the maximum number of devices for the profile.

6. Optionally, click the Plus sign (+) adjacent to **Device Groups** to add more device groups to the entitlement profile.

Note: You can add multiple device groups to an entitlement profile, provided device types in these groups are unique across the groups.

7. Click **Save**.

   The new entitlement profile can now be assigned to users.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Contact Center*

12.7.6. Entitlement enforcement

Tip: *Use the Action search to navigate Automate*

Device groups

Device groups are used in entitlement catalogs and entitlement profiles to limit entitlement to a defined subset of available device types.

A user to whom an entitlement profile is applied is limited to devices in the device groups assigned in the entitlement profile. Adding a phone to a user in User Management fails if the added phone is not in a device group assigned to the entitlement profile applied to the user.

Related topics

- *Add device group*

Device limits

A user to whom an entitlement profile is applied is subject to the following device limits set in the entitlement profile:

- Total number of devices
- Total number of devices in a device group

Adding a Phone to a user in User Management fails if the total number of devices limit or the total number of devices in a device group limit is exceeded.

Transaction log

The transaction log messages contain detailed information that can be used to determine what entitlement profile limitation caused an action to fail.

Service levels

The table describes the impact on a user when a service is disabled in the entitlement profile applied to the user.

Note: An entitlement profile can be explicitly assigned to a user, or implicitly applied if an entitlement profile is designated as the default entitlement profile in a hierarchy node at or above the user's hierarchy node.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Service disabled	Result
Default Profile	(ENTERPRISE) Defines whether this entitlement profile is the default entitlement profile displayed in the Quick Add User **Entitlement Profile** drop-down.
Voice	Adding a phone to a user in User Management fails. For an existing user with a phone with this profile (where voice is disabled), the update of the user from "User Management" fails, unless the existing phones for the user are dissociated.
Voicemail	Adding Voicemail to a user in User Management fails. For an existing user with Voicemail, updates in User Management fail after an entitlement profile with Voicemail disabled is applied to the user.
Presence	Enabling Cisco Unified Communications Manager IM and Presence Service for a user in User Management fails. For an existing user with Cisco Unified Communications Manager IM and Presence Service enabled, updates in User Management fail after an entitlement profile with Presence disabled is applied to the user.
Extension Mobility	Adding Extension Mobility to a user in User Management fails. For an existing user with Extension Mobility, updates in User Management fail after an entitlement profile with Extension Mobility disabled is applied to the user.
Single Number Reach	For a new user, adding Single Number Reach in User Management fails, and for an existing user with Enable Mobility checked, adding Single Number Reach fails after an entitlement profile with Single Number Reach disabled is applied to the user.
Conferencing	Adding or assigning Conferencing feature to the user fails if this field is enabled. For an existing user if you enable Conferencing and an entitlement profile with Conferencing disabled is applied, the update operation fails.
Contact Center	Contact Center is not available for a new user if this field is disabled. If Contact Center is enabled for an existing user, and an entitlement profile with Contact Center disabled is applied, the update operation fails.

Copyright © 2025 VisionOSS Limited. All rights reserved.

13. System Functions

13.1. Transaction Overview

13.1.1. Automate - Additional Admin Functions - Transaction Overview

This dashboard provides an overview of key transaction metrics

Counters

- User Transaction Count
- User Transaction Count
- Configuration Transaction Count
- Unique User Count

Charts

- **Transaction Status Overview**
  - **Description:** Shows a split of top level transaction statuses
  - **Type:** chart-pie
  - **Resource:** Transactions
- **Top 10 Admins**
  - **Description:** Shows the 10 most active admins
  - **Type:** chart-pie
  - **Resource:** Transactions
- **Admin Hierarchies**
  - **Description:** Shows a split of hierarchies of the admin that executed the transaction
  - **Type:** chart-pie
  - **Resource:** Transactions
- **Top 10 Actions**
  - **Description:** Shows a split of the top 10 actions performed
  - **Type:** chart-pie
  - **Resource:** Transactions
- **Status Trend**

  - **Description:** Shows the transaction status over time
  - **Type:** chart-line
  - **Resource:** Transactions
- **Admin Hierarchy Trend**
  - **Description:** Shows the number of transactions performed by admin hierarchies over time
  - **Type:** chart-line
  - **Resource:** Transactions

Tables

- **Configuration Entities**
  - **Resource:** Transactions
  - **drilldown-modelType:** Transaction
  - **Fields:** Entity
- **Impacted Hierarchies**
  - **Resource:** Transactions
  - **drilldown-modelType:** tool/Transaction
  - **Fields:** Hierarchy Type, Hierarchy Name
- **Admin Hierarchies**
  - **Resource:** Transactions
  - **drilldown-modelType:** tool/Transaction
  - **Fields:** Username, Hierarchy Type, Hierarchy Name

13.2. Tools

13.2.1. Add Custom Variables

System administrators can create custom macros for use in for example custom Configuration Templates.

Note:

- The macro needs to be evaluated at the hierarchy that it is created.
- The same macro variable can be defined to have different values at different hierarchies.

1. Choose **Advanced Tools > Custom Variables** and click **Add**.
2. Enter the macro name, optional description and value. The name must be prefixed with `CV_`. For details on macro syntax, refer to the “Advanced Configuration Guide”.
3. Click **Save**.

To test the macro, enter it in the macro evaluator at **Administration Tools > Macro Evaluator**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Example

Create:

```
CV_current_time

Current time is: {{ fn.now }}
```

Invoke:

```
{{ macro.CV_current_time }}
```

Output example:

```
Current time is: 2017-03-31 13:20:18.509871
```

13.2.2. General Tools

Transaction Log

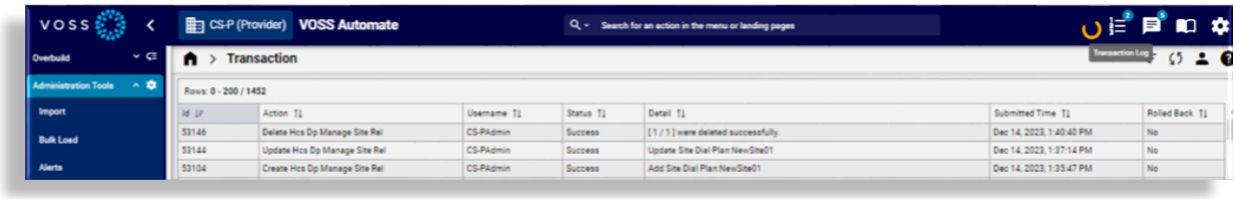
Transaction logging and audit

Tip: *Use the Action search to navigate Automate*

Overview

Transactions are a record of all activities that occur in Automate. You can inspect the summary list view of past and in-progress transactions in the **Transaction Log**, where you can drill into the details of a transaction and related sub-transactions, as well as view the logs to audit the transaction steps.

Note: You'll only have access to the Transaction Log if your access profile permissions allow it (read permissions on `tool/Transaction`).



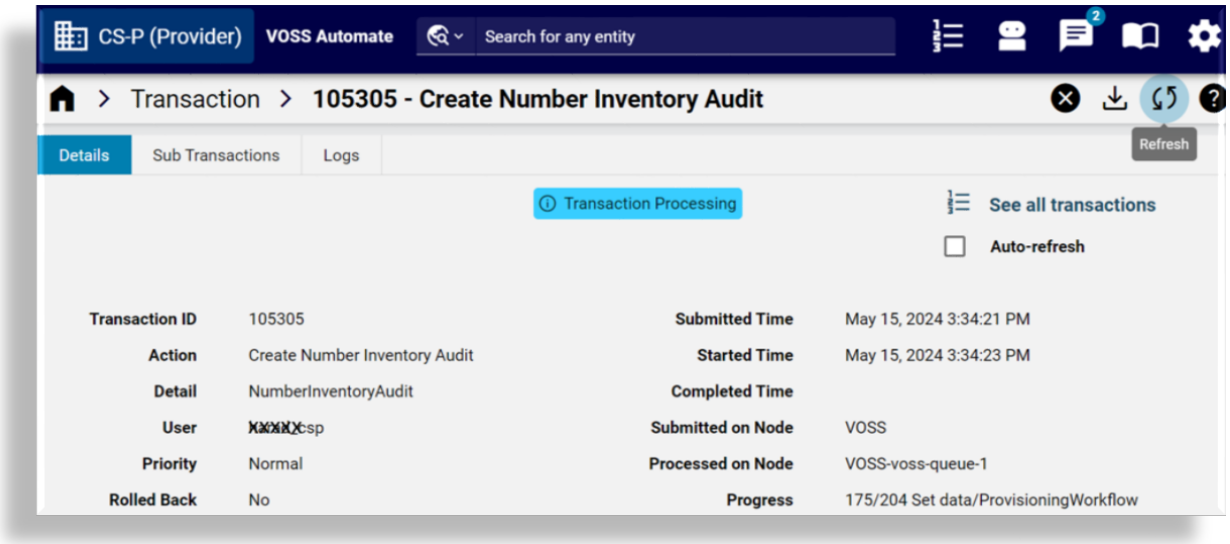
Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- *Bulk load transactions*
- *Filter Transactions*

View a transaction

In the Transaction logs you can click on a transaction to view the transaction details, and if available for this transaction, any sub-transactions, as well as the logs.



Additional tabs may display for transaction details:

- Details
- Sub Transactions
- Logs
- Failed Asynchronous Transactions

Transactions toolbar

When viewing the details of a transaction the following toolbar actions may be available, depending, for example, on the transaction type, and on whether the transaction is in progress or complete, and whether it is a successful or failed transaction:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Refresh	You can click the **Refresh** button while a transaction is running to update its progress and status in realtime
Auto-refresh	Automatically refreshes the transaction progress and its status, every 5 seconds, while the transaction is running.
Cancel	Cancels a transaction, if its still running. The status of a cancelled transaction updates to *Fail* with a system message that says *Transaction canceled*. If you cancel a transaction that has sub-transactions, a currently in-progress sub-transaction will complete, and then this sub-transaction as well as any preceding sub-transactions will rollback to their previous states. However, for a cancelled bulk transaction, the system views each bulk load sub-transaction as a main transaction, and thus only the currently in-progress sub-transaction is rolled back to its previous state.
Replay	For completed transactions, you can click the **Replay** button to repeat (replay) the transaction, if required. For example, let's say a transaction fails because a target system service was not running. In this case, you can replay the transaction instead of having to re-input data on the form in the Admin Portal.

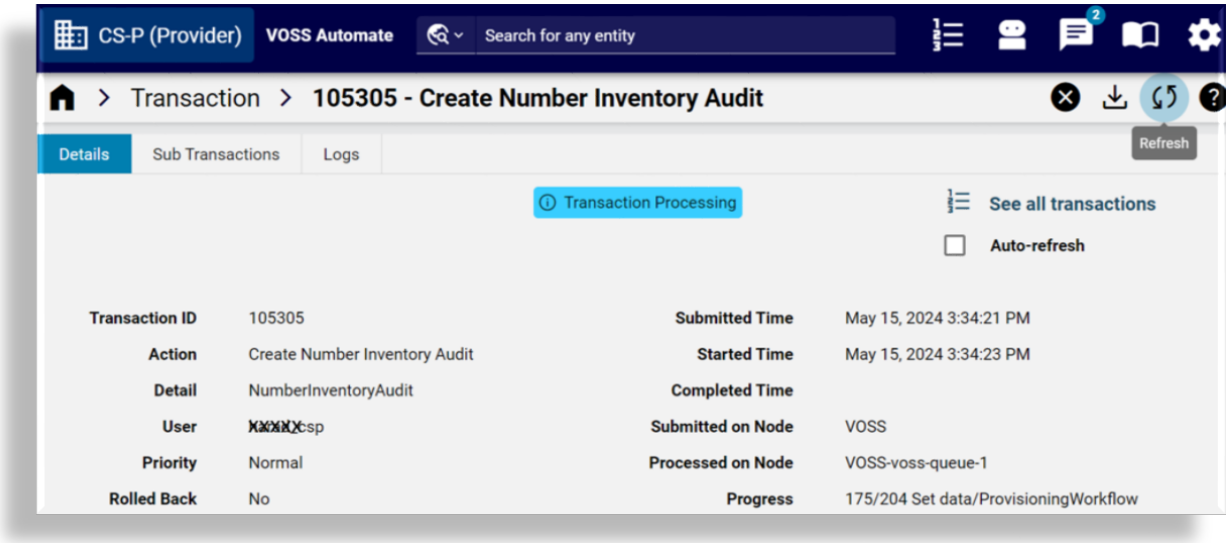
Edit and Replay	Click **Edit and Replay** to first open the form that was used for input data prior to running a transaction. You can now make changes to the input data that was used, and then re-run the transaction. This is useful where, for example, incorrect input data causes a transaction to fail. Note the following: • Edit and Replay is only available for transactions that don't originate from bulk loads or from pop-up forms. • Edit and Replay should only be used at the same hierarchy where the original transaction was executed. This is because GUI rules apply to forms at specific hierarchies. • Replay and Edit and Replay are not supported by the bulk loader, because the bulk load files are not stored by default. The bulk loader extracts data from the spreadsheets and then performs the necessary action. A bulk load file is only stored in the database is when the bulk load is scheduled. In this case, the bulk loader keeps the file until it is triggered by the scheduler to execute the actions in the file. When the data is extracted from the file, it is deleted. • When using Edit and Replay for a failed Quick Add User transaction, the following user information fields will not automatically update when changing the Username field and will need to be edited manually: – Entitlement Profile – Firstname – LastName – Email

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: If the transaction queue service stops and is restarted, any queued transactions will resume processing, while processing transactions will fail and displays the following message: `Transaction aborted due to queue service restart`.

Details

This tab provides high level transaction details, such as the transaction ID, the user who initiated the transaction, duration, and so on.



The table describes the details available for transactions:

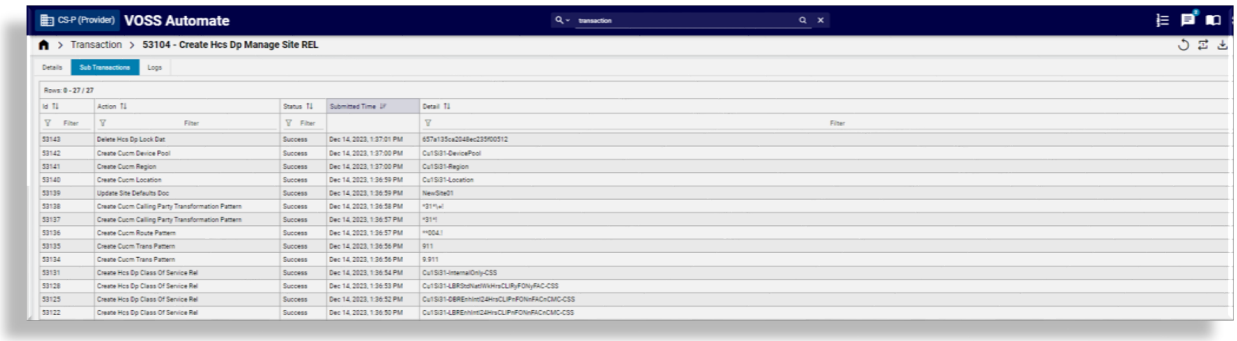
Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Transaction ID	Unique identifier for the transaction.
Action	The type of action recorded in the transaction, for instance Execute, Create, Modify, Data Import and so on.
Detail	A brief description of the processed transaction.
User	The user who initiated the transaction.
Priority	The priority of the transaction, for example Normal.
Status	For transactions to process, this is Queued. For running transactions, this is In Progress; for completed transactions it is Fail or Success.
Message	The message displayed upon completion of the transaction.
Submitted Time, Started Time and Completed Time	The date and time indicating the transaction progress.
Submitted on Node	The host name of the application node that scheduled the transaction. On a clustered system, this can differ from the 'Processed on Node' name below.
Processed on Node	The host name of the application node that processed the transaction (this value will only be set once the transaction is processed). On a clustered system, this can differ from the 'Submitted on Node' name above.
Rolled Back	Indicates whether the transaction was rolled back or not.
Duration	The duration of the selected transaction. If there are sub-transactions, this parent transaction duration is the total duration of the transaction. This includes the total duration of import transactions that carry out provisioning workflows asynchronously.

Sub-transactions

Sub-transactions display in a list for transactions that have sub-transactions:

On the Admin Portal, the sub-transaction list will show below the transaction details if there are 10 or less sub-transactions. Otherwise, sub transactions display on a new tab on the page.



Sub-transactions contain links to their details and the sub-transaction form displays a link to its parent transaction.

Failed transactions show a Message of the error. However, a sub-transaction with a Create action that has a

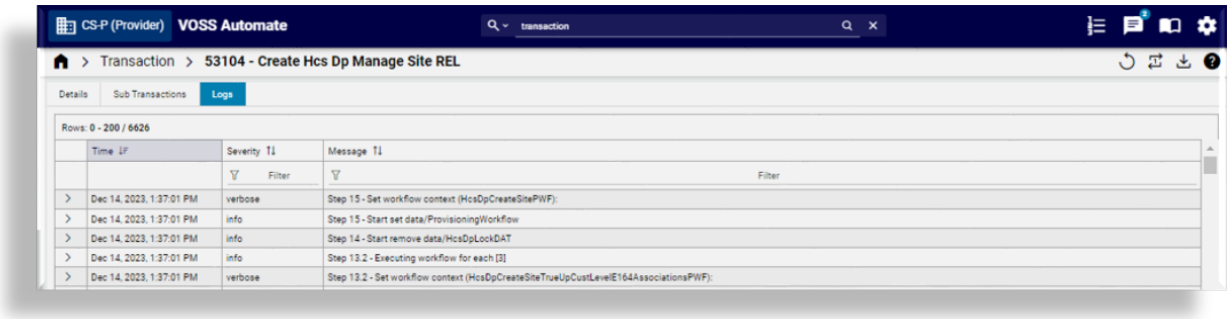
Copyright © 2025 VisionOSS Limited. All rights reserved.

"fail on error" workflow condition for *duplicates*, may show its Status as Fail when not creating a duplicate, while the parent transaction then shows its Status as Success.

For asynchronous transactions and sub-transactions, refer to Parent and Sub-transactions for Asynchronous Transactions.

Logs

The Logs tab displays a time stamp, Message and Severity details of transactions.

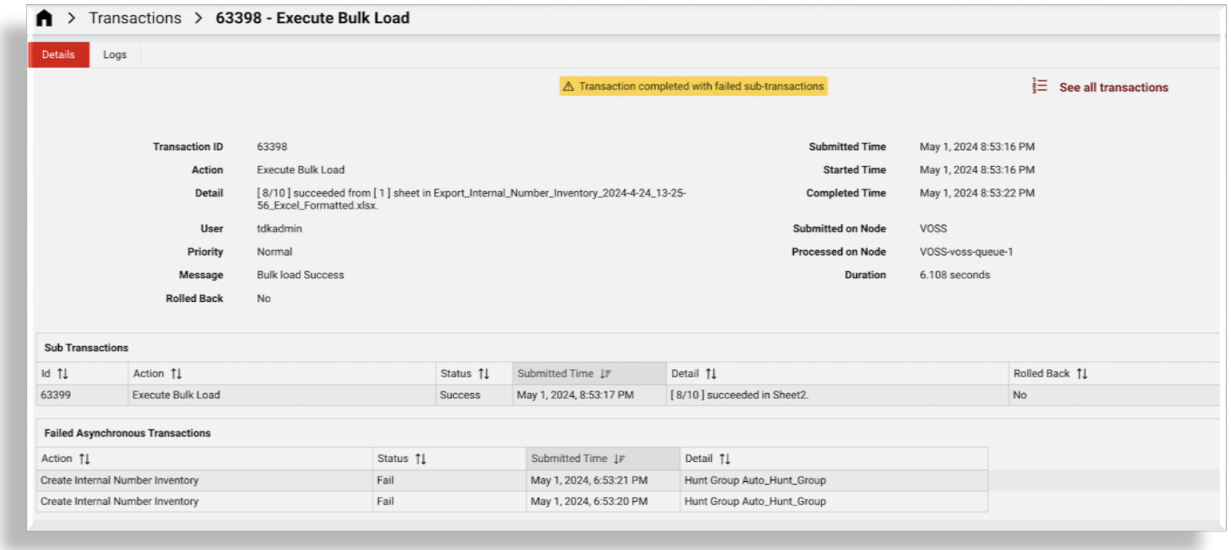


If the Severity has the status of `error`, the Message section can be expanded to inspect the error, and optionally copy it and send it to Support.

If a workflow is inspected, a separate log entry provides details of each step with a log message as *Step n*, starting with Step 0.

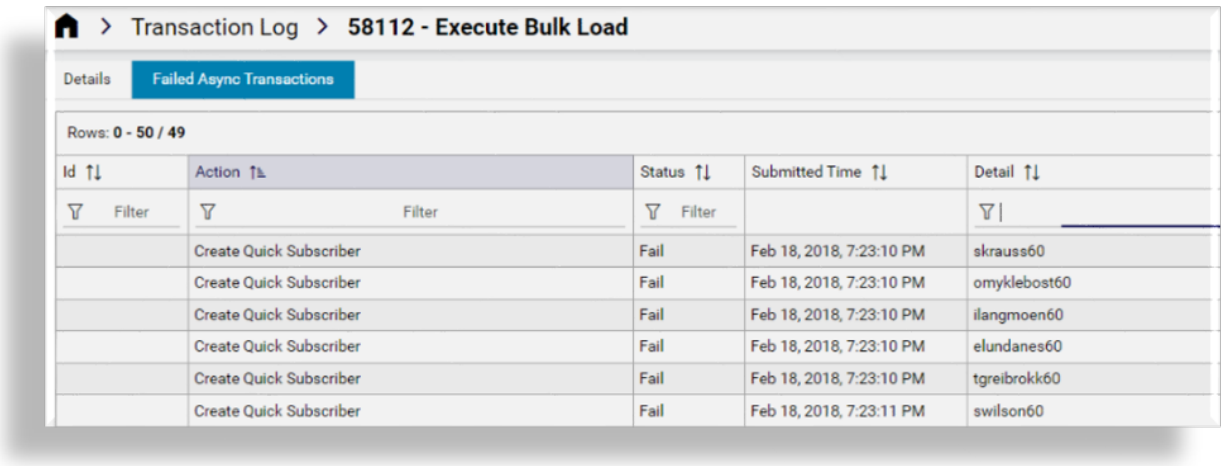
Failed async transactions

Failed asynchronous transactions display below the sub transactions.



If there are more than 10 failed async transactions, these details display on a new tab on the page.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Resource or record

Depending on the transaction type, an option is available to navigate to the original record where a resource changed.

Parent and sub-transactions for asynchronous transactions

Parent and sub-transactions for asynchronous transactions are shown in the transaction logs as follows:

- Parent transactions are in a “Processing” state until the last asynchronous child transaction completes (with either “Success”, “Success With Async Failures”, or “Fail”). These include:
  - Asynchronous workflows triggered by Device Import
  - Asynchronous operations triggered by Bulk Load (with parallel = true)
  - Asynchronous workflow steps
- Asynchronous transactions for non-bulk operations are not grouped under the parent transactions. These include:
  - Asynchronous device import triggered by DataSync execute
  - Asynchronous event execute triggered by another operation
- The status of top level transactions with failed asynchronous at any level of sub-transactions is “Success With Async Failures”. The detail view of the top-level transaction also shows the list of failed async transactions below the list of sub-transactions. This list allows for easy access to all failed async transactions. The Detail column of the sub-transactions also show the number of failed async transactions.
- The details of parent transactions with the status “Success” also show the number of failed sub-transactions for the following:
  - Device Import
  - Workflows

Copyright © 2025 VisionOSS Limited. All rights reserved.

Bulk load transactions

Tip: *Use the Action search to navigate Automate*

Overview

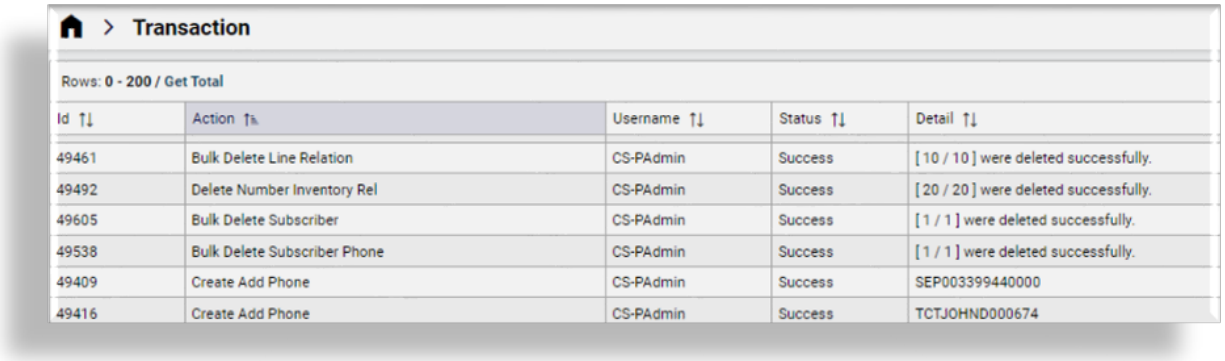
Once you run a bulk load transaction, you can view its transaction details on the **Transaction** log (accessible via the toolbar).

Related topics

- Transaction logging and audit in the Core Feature Guide
- View a transaction in the Core Feature Guide

View bulk load transaction details

Click the toolbar icon to go to the **Transaction Log**. Bulk load transactions show in the log:



Transaction

Rows: 0 - 200 / Get Total

Id	Action	Username	Status	Detail
49461	Bulk Delete Line Relation	CS-PAdmin	Success	[10 / 10] were deleted successfully.
49492	Delete Number Inventory Rel	CS-PAdmin	Success	[20 / 20] were deleted successfully.
49605	Bulk Delete Subscriber	CS-PAdmin	Success	[1 / 1] were deleted successfully.
49538	Bulk Delete Subscriber Phone	CS-PAdmin	Success	[1 / 1] were deleted successfully.
49409	Create Add Phone	CS-PAdmin	Success	SEP003399440000
49416	Create Add Phone	CS-PAdmin	Success	TCTJOHND000674

- In the list view, the bulk load is shown in the **Action** column of the log. If the bulk load was scheduled, this is shown as a schedule with the detail column indicating it to be a bulk load. The **Action** column will show “Execute Bulk Load” or “Execute Schedule” respectively.
- The submitted, start, and stop time for the entire bulk load transaction is also shown.
- The Detail tab displays the name of the bulk loaded file as the workbook sheet number and the number of successful rows out of the total, for example:

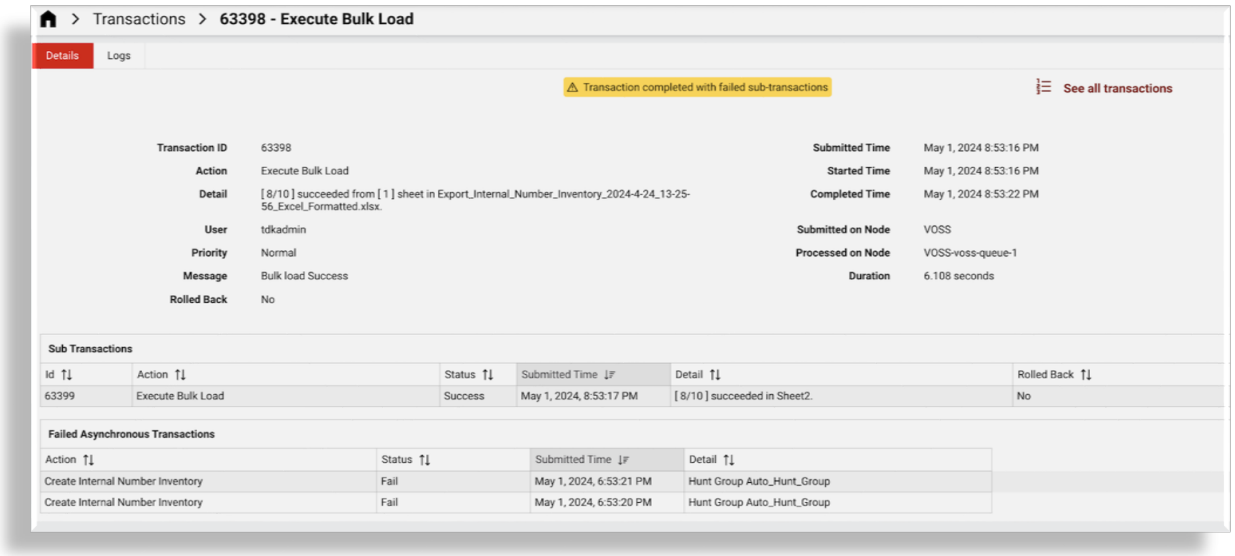
```
[ 8/9 ] succeeded from [ 1 ] sheet in data_Users_bulkloadsheet.xlsx.
```

Checks are made to validate the user’s access profile, the provided hierarchy information, and data constraints for the bulk load transaction when updating the target models. The parent bulk load transaction will show the error message if this validation fails and no rows will be loaded.

Where rows are loaded, each row in the bulk load sheet appears as a sub-transaction within the bulk load transaction. The Message dialog displays the number of successful and failed rows loaded.

Failed asynchronous transactions display below the sub transactions. If the number of failed asynchronous transactions exceeds 10, these details display on a new tab on the page.

Copyright © 2025 VisionOSS Limited. All rights reserved.



For each loaded sheet, bulk load transactions are run in series for each row. Multiple bulk load sheets can be loaded and these transactions will load in parallel.

Sheet rows can be processed in parallel. The sheet should then not contain multiple, sequence dependent models. Refer to *Bulk load template sheet layout*.

For each row of the bulk load sheet carrying out the default add action, a Create action is shown on the list of transactions. Sheet rows that led to a successful *Create* action have a *Success* status, while rows that failed show a *Fail* status. If a row fails, the load process continues. For failed actions, the transaction can be selected to show the error message.

If one or more rows of the sheet failed to load, the Bulk Load Sub Transaction shows a *Success* status, while the Log list will show “error” for failed rows.

On the list of sub transactions, you can inspect the details of each sub transaction. For example, the submitted, start, and stop time for the bulk load sub transaction corresponding with a row on the bulk load sheet is shown. In the case of a failed sub transaction, further information about the failure - such as the error message and row data - is shown in the sub transaction.

A canceled bulk load transaction means the Processing worksheet sub transaction, as well as all sub transactions within the worksheet transaction in a *Processing* or *Queued* state, will fail.

For parallel transactions, multiple resource transactions may be in a *Queued* or *Processing* state. By default, 14 rows are processed in parallel. Refer to *Bulk load template sheet layout* for details.

If a worksheet transaction fails as a result of bulk load transaction cancellation, subsequent worksheet tabs in the bulk load workbook will not be processed by the bulk loader.

View a transaction

Tip: *Use the Action search to navigate Automate*

You can only view transactions that are relevant to your specific hierarchy level. For instance, if you’re logged into the system as a customer administrator you’ll be able to view all transactions that were performed at the customer for which you’re the administrator. This includes transactions that were performed at any of the sites that belong to the customer.

Copyright © 2025 VisionOSS Limited. All rights reserved.

If you're logged in as a site administrator you'll be able to view only the transactions that were performed at your specific site.

Note: See the topic on Data Partitioning in the Core Feature Guide and to the API Guide to view transactions by means of the API.

To view transactions in the Admin portal:

1. Go to **Transaction** to open the list view.
2. View all parent transactions in the list view. The **Status** column indicates whether a transaction is executed, in progress, success, success with async failures, or failed.
3. Click on a parent transaction to view its child transactions (sub-transactions).

   Note:

   - Failed transactions are highlighted (red by default, but this can be changed via themes), and display an exclamation icon along with the text, "Fail".
   - The **Detail** column provides additional details on the transaction if available.
   - The **Rolled Back** column displays either **No** or **Rolled Back** - the latter for any failed transactions (with **Status** is **Fail**) that have been rolled back.

4. Click a sub-transaction to view further details.

   For top-level transactions with status **Success With Async Failures**, the list of failed async transaction display below the sub transactions. If there are more than 10 failed async transactions, these display on a separate tab on the page.

   Failed async transactions can be at any level below the top-level transaction. Click the transaction to see the details of the failed async transaction(s).

   The **Detail** also shows the number of failed async transactions.

Related topics

- Transaction logging and audit in the Core Feature Guide.
- Prevent duplicate numbers in the Core Feature Guide

Transaction log levels

Automate users with access to the `data/Settings` model or `view/DataSettings` can manage global transaction logging levels. These logging messages display below a selected transaction on the **Transactions** page, and have no impact on the transaction or sub-transaction action or detail information.

Log levels are *cumulative*, that is, more detailed levels include all details from less detailed levels.

The table describes the transaction log levels and their severity values:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Level	Description	Severity
Disabled	Disables all transaction log messages	999
Error	Only displays error messages	40
Warning	Also adds warning messages to above	30
Info	Also adds informational messages to above	20
Verbose	Also adds messages used for diagnostic purposes to above	15
Debug	Also adds advanced diagnostic messages - for future use	10

- Severity values are referenced (from value - to value) in transaction details when the log level is changed on this setting or changed by lower level administrators from the **System Settings** menu. See: *Settings*.
- If a transaction fails, the Log block includes all entries with severity values larger than that of the default or selected level of logging.
- The log levels of data syncs can be set to override these global levels.

  The transaction log level used for data sync and its immediate sub-transactions is by default set to Warning when it is not set.

  For details, refer to the Create a Custom Data Sync topic in the Core Feature Guide.

Transaction log levels are configurable based on your needs, for example, set to `Verbose` to include greater details for immediate troubleshooting and customization work:

1. Toggle the log level to `Verbose`.
2. Reproduce the issue causing the problem.
3. Export the logs and forward them to VOSS support.
4. Toggle the log level back to `Info`.

Note: When setting transaction log level to `Verbose` or `Debug`, notes and warnings are shown to remind admins that the retention period of such logs is due to their increased size, which consequently reduces the date range of available logs for troubleshooting.

Transaction Details

This Detail column of the list of transactions in the transaction log user interface shows information according to the type of entity and the operation carried out by the transaction.

The rules listed below should be considered when creating a transaction filter and specifying the value of the filter text.

The following conditions apply to content in the Detail column:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Action	Entity	Comment
Create, Update, Clone and Delete	all models	Detail will only contain the name on the model
Execute	DataSync, Workflow, Event, Scheduler	Detail will contain the instance name
Bulk operations on Modify, Delete, Move	all models	• The parent transaction detail contains: "[no. of succeeded / no. of total] were [updated / deleted / moved to destination_hierarchy] successfully." • Bulk move from different hierarchies to one hierarchy show the destination hierarchy name in the parent transaction detail. • Each child transaction detail will contain the name of instance that is deleted.
Data Import	all models	Detail shows only the imported file name.
Device Import	all devices	Detail shows host name or device address
All operations	all models	The following attribute values are considered first for inclusion in the Detail column: `country_name`, `DialPlanName`, `name`, `ip`, `host`, `address`, `description`, `username`, `type`, `entity_id`, `userid`, `pattern`, `RoleCurrent`. Otherwise, the Detail column will be empty.

Note that the contents of the Detail column of transaction lists are not localized.

Filter Transactions

Tip: *Use the Action search to navigate Automate*

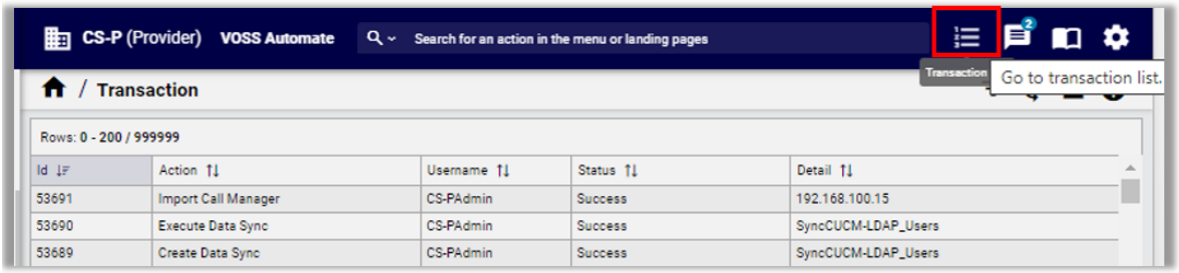
Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

A transaction filter is a logical *AND* operation based on column values in the **Transaction** log (list view), defined as search criteria in the **Filter Transactions** dialog.

Using filters to search for transactions

1. Log in to the Admin Portal.
2. Click the **Transaction Log** toolbar icon to open the **Transaction** list view.



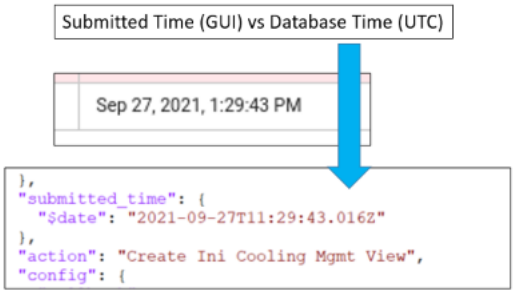
3. In the **Transaction** list view, inspect the list of parent transactions. You can click on a parent transaction to view details of the parent and its sub transactions.
4. Click the toolbar **Filter** icon to open the **Filter Transactions** dialog.
5. Specify filter criteria for the transactions you wish to view:

Field	Description
Transaction ID	• **Equals** (default): Filters only for an exact ID, and disables all other criteria. • **Range**: Filters for a range of IDs that match a **Start** and **End** value. Leave this input empty if a search is carried out using other matching criteria.
Include Sub Transactions	Apply filter criteria also to first level child transactions. Children of child transactions (sub-transactions directly below the parent) are excluded. By default, results show sub transactions above the parent (latest data on top)
Exclude System Transactions	Defines whether to exclude system-generated transactions (included by default); that is, where the **Username** column value is `system`.
Status	Filter by transaction status. Options are: Any, Failed, Success, Processing, Queued, or Success with Async Failures.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Date	Filter by date. Options are All, Last Day, Last Week, Last Month, or Custom (which allows you to select a date from a calendar date picker to specify a date range. When choosing one of the quick filters (Last Day, Last Week, Last Month), the next time the filter opens, the date selection displays as a Custom date range, since the range is then less than the selected interval. The filter date/time is based on the browser local timezone, for example GMT+0200. This time is converted to the UTC standard as used in the database. (Time Conversion)
Date Range	Displays when you select *Custom* from the **Date** field, and allows you to select a date from a calendar date picker.
Action	The action to filter on, for example, `Create user`, or start typing to filter values in the drop-down.
Rolled Back	Filter by transaction rolled back status. Options are Any, Yes, No.
Username	Case-insensitive field to filter on values in the **Username** column.
Detail	Case-insensitive field to filter on values in the **Detail** column.
Message	Case-insensitive field to filter by text values in the **Message** column. • Hover over the **Status** column to see a transaction message, or inspect it in the transaction detail view.

(Time Conversion)



Note: A filter timeout limits the filter search to 2 minutes. Try reducing the criteria to speed up filtering.

Once you've viewed filtered results, remember to cancel or clear the filter to display all transactions in the log. Filters are also cleared when you log out.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Filter Sub-Transactions and Logs

Some transactions have sub-transactions as well as a log list on the transaction detail view. The filtering of sub-transactions and logs works like the list view filter, in other words, a range of matching operators are available.

If a sub-transaction has further sub-transactions, click the Link in its Transaction column to carry out any filtering on nested sub-transactions. To navigate up the sub-transaction hierarchy, click the parent Link.

- In the Admin Portal, sub-transaction lists can be filtered by entering the filter value in the column header filter boxes of the list:
  - **Id**
  - **Action**
  - **Status**
  - **Submitted Time**
  - **Detail**

  More than one filter can be added - this will result in a logical AND of the filters. Filter values are matched case-insensitive and with match operator CONTAINS. To clear a filter, click the “x” in the column header filter box.
- In the Legacy Admin GUI, use the **Filter** button below the list of sub-transactions to add a filter in the pop up form. The following columns can be filtered:
  - **Action**
  - **Status**
  - **Detail**

  The following match operators are available: Contains, Does Not Contain, Starts With, Ends With, Equals, Not Equal. In addition, an **Ignore Case Value** check box is available to apply to each value. Multiple filters will result in a logical AND of the filters. When a filter is applied to a list, an “X” will show next to the **Filter** button to clear the filter.

The log columns to filter by, are:

- Severity
- Message
- Duration (some logs - only equals and not equals)

For more details on matching operators when filtering sub-transactions and logs, also refer to “Filtering Lists”.

Transaction Behavior

The VOSS Automate transaction engine ensures that configuration changes are made efficiently and reliably.

In the event of a transaction failure or error, VOSS Automate allows for transactions to be rolled back to a state preceding the failed transaction.

For example, where a workflow step fails, all successful steps prior to a failed step are rolled back.

Transactions are hierarchical and have parent-child relationships with other transactions. Sub-transactions are always executed sequentially and synchronously, in other words the child transactions of a workflow parent transaction are executed one after another.

Transaction behavior is different for the following actions in the system:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- API

  The API supports executing transactions in both synchronous and asynchronous modes. When executed in synchronous mode the API responds only once the transaction has completed. When executed asynchronously, the API responds immediately with a transaction ID so that the progress and status of the transaction can be polled.

- Bulk Loaders

  With bulk loading, the load of each row on a sheet is a separate transaction. These transactions are run in series. There is no rollback of rows that have loaded successfully prior to, or subsequent to, a failed transaction (a failed row on a sheet). Multiple bulk load sheets can be loaded in parallel.

- Data Import

  A single transaction is created for each record in the import file. If a single transaction fails, the import continues and does not roll back the preceding successful transactions.

- Data Sync

  A single parent transaction is created for a data sync action. The subsequent device API requests are not handled as sub transactions but are executed in-line.

- Events

  Events can be triggered as part of data sync operations or as triggers on operations performed on certain model types. The provisioning workflow executed when the event triggers is executed as a new parent transaction. Transaction failures with the workflow executed after an event do not affect the original transaction that triggered the event.

All transactions are placed on a queue before they are actioned. If the system queue service is restarted while a long-running transaction such as data sync or bulk load is running, all running transactions that are a part of this transaction will be marked as failed and finalized.

Parent transactions can run concurrently, but their subtransactions run serially. There is priority in parent transactions so that user input such as adding on a Admin Portal form will be prioritized over a running import or bulk load process.

Transaction Priority

Transactions can currently have two levels of priority: normal and low.

Normal priority transactions will be processed ahead of any low priority task in the queue.

Low priority transactions have a time limit associated with them. This means that if a low priority transaction is in the queue for more than a day, it will be processed as a normal priority transaction.

The following transactions have a low priority:

- Data sync
- Bulk load
- Data import (JSON import)

Any sub-transaction of these transactions also have a low priority.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Transaction Log Example

This section aims to examine the transactions, sub-transactions and logs that are displayed when an example wizard is executed.

The aim of the wizard is to to provide the user with a series of steps to allow input and choices. When the wizard is executed, a Workflow is run and this is displayed as an Action on the Transaction list.

The workflow executes tasks to:

- Add a hierarchy.
- Add devices at the created hierarchy if selected.
- Add a user to the system and if selected, add a user to devices and also LDAP and SSO users if selected.

After the wizard is run, the sub-transactions show the actions of the workflow. In the example, only the Unified CM is selected. The first action in the wizard is to execute a workflow, that results in three sub-transactions. The first sub-transaction is itself a workflow that carries out three actions:

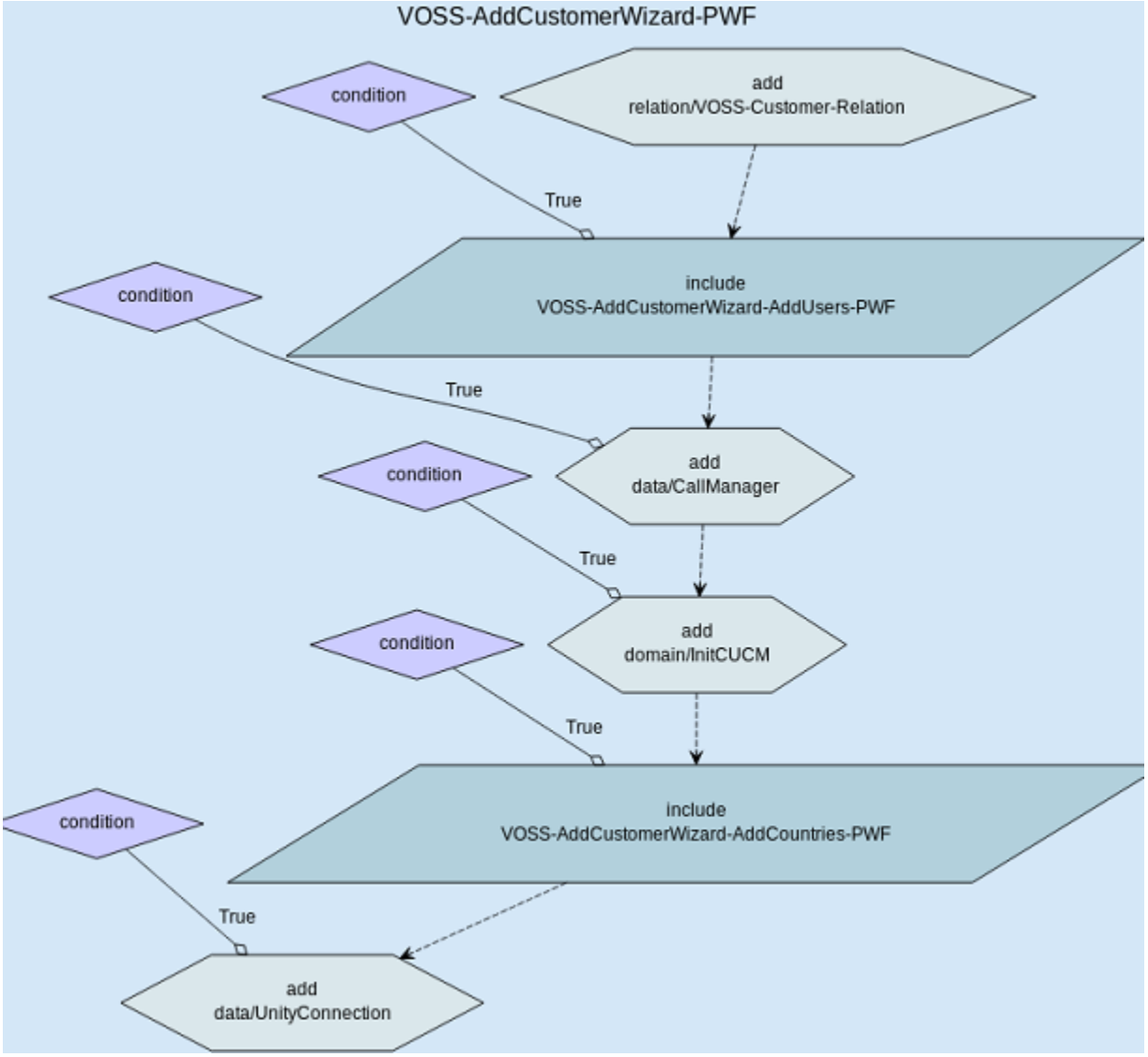
Execute : VOSS-AddCustomerWizard-PWF

1. Create Voss-Customer-Relation Execute : VOSS-Relation-Add-Customer-PWF
    a. Create Hierarchy Node
    b. Create Base Customer Dom
    c. Create Voss Cust Dp
2. Create User
3. Create Call Manager

The transaction log shows all the steps of all the workflows that are executed. The first log entry of the wizard is at the bottom of the log list. The first step of each workflow is marked as `Step 0`.

The figures below show the example wizard flow and the corresponding logs.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Transaction

Mar 27, 2014 15:26:1 SAST	info	Step 5 - Start include VOSS-AddCustomerWizard-AddCo
Mar 27, 2014 15:26:1 SAST	info	Step 4 - End
Mar 27, 2014 15:26:1 SAST	info	Step 4 - Condition unmet, skipping step.
Mar 27, 2014 15:26:1 SAST	info	Step 4 - Start add domain/InitCUCM
Mar 27, 2014 26:1 SAST	info	Step 3 - End
Mar 27, 201 6:1 SAST	info	Step 3 - Template (AddCustomerWizard_CUCM_CFT) aft
Mar 27, 20 1 SAST	info	Step 3 - Template (AddCustomerWizard_CUCM_CFT) be
Mar 27, 2 1 SAST	info	Step 3 - Template after merging AddCustomerWizard_Cl
Mar 27, SAST	info	Step 3 - Start add data/CallManager
Mar 27 AST	info	Step 1 - End
Mar 2 ST	info	Step 1 - End
Mar T	info	Step 1 - Template (AddCustomerWizard_User_CFT) after
Ma	info	Step 1 - Template (AddCustomerWizard_User_CFT) befo
M	info	Step 1 - Template after merging AddCustomerWizard_U
	info	Step 1 - Start add data/User
Mar 27 SAST	info	Step 0 - Executing workflow (dynamic_workflow) with th
Mar 27 SAST	info	Step 1 - Executing workflow for each [1]
Mar 27 SAST	info	Step 1 - Start add data/User
Mar 27 SAST	info	Step 0 - Executing workflow (VOSS-AddCustomerWizard-
Mar 27 SAST	info	Step 2 - Including_workflow, name: VOSS-AddCustomer
Mar 27 SAST	info	Step 2 - Start include VOSS-AddCustomerWizard-AddUs
Mar 27 SAST	info	Step 1 - End
Mar 27 SAST	info	Step 1 - Template (AddCustomerWizard_VOSS-Custome
Mar 27 SAST	info	Step 1 - Template (AddCustomerWizard_VOSS-Custome
Mar 27 SAST	info	Step 1 - Template after merging AddCustomerWizard_V
Mar 27, 2014 15:25:56 SAST	info	Step 1 - Start add relation/VOSS-Customer-Relation
Mar 27, 2014 15:25:56 SAST	info	Step 0 - Executing workflow (VOSS-AddCustomerWizard-
Mar 27, 2014 15:25:56 SAST	info	Step 0 - Executing workflow (VOSS-AddCustomerWizard-

Direction

Copyright © 2025 VisionOSS Limited. All rights reserved.

Device data sync errors in transactions

Overview

The data sync from a device has two steps:

1. A list request for all the resources of a specific type is made, for example for a user or a phone.
2. Requests for detailed information of each resource of the specific type.

Troubleshooting errors

The tables below show errors raised by devices and how these are handled or written to the transaction log by VOSS Automate. In the case of failed transactions, the tables point to possible causes of some errors.

Note:

- A number of CUCM device model errors are non-critical and will not fail data sync transactions.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUCM AXL handled by Automate (DataSync transaction final status is not failed)

Model	Operation	Device Error Message Match	VOSS Automate DataSync Action and/or error log
LocalRouteGroup	GET	No Search Criteria Defined	Ignored known error
LdapDirectory	GET	Item not valid: The specified LdapDirectory was not found	Ignored known error
UniversalDeviceTemplate	GET	Item not valid: The specified UniversalDeviceTemplate was not found	Ignored known error
LicensedUser	GET	Item not valid: The specified LicensedUser was not found','The endpoint reference (EPR) for the Operation not found is No License found for the specified user: Could not open database table	Ignored known error
LdapSyncCustomField	GET	Invalid ldapConfigurationName	Ignored known error
EndpointReleaseKey	GET	Column (name) not found in any table in the query (or SLV is undefined)','The endpoint reference (EPR) for the Operation not found is	Ignored known error
DirNumberAliasLookupandSync	GET	Item not valid: The specified DirNumberAliasLookupandSync was not found	Ignored known error
DeviceSerialNumber	GET	endpoint reference (EPR) for the Operation not found is	Ignored known error
LicenseCapabilities	GET	The endpoint reference (EPR) for the Operation not found is	Ignored known error
PhoneTypeDisplayInstance	GET	Wrong value for Protocol. Please enter a valid value.	Not all Phone Types have Vendor Config Rules. Ignored.

CUCM device errors not handled by Automate (DataSync transaction final status is failed)

Model	Operation	Model Error	Possible Cause
(All model types)	GET	Resource not found	A workflow in VOSS Automate deleted an item between the DataSync LIST operation and the GET operation
(All model types)	GET	AXL Error [-1]	This is a non-specific error raised by CUCM. Follow up with the CUCM team.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUC device errors not handled by Automate (DataSync transaction final status is failed)

Model	Operation	Model Error	Possible Cause
(All model types)	GET	Resource not found	A workflow in VOSS Automate deleted an item between the DataSync LIST operation and the GET operation
ImportUser	GET	Resource not found	1. A sync between CUC and LDAP is running at the same time as the VOSS Automate sync to CUC. If the User is disabled or deleted on LDAP, then the User would removed as an Import User on CUC. 2. A workflow on VOSS Automate promoted a user from Import User to User by creating a Voicemail Box for that User, which also causes the user to be removed as Import User and created as a full User.

Export a transaction

Tip: *Use the Action search to navigate Automate*

Overview

Administrators can export upper level parent transactions. This will include their child sub-transactions as well as the associated transaction log entries in JSON format.

The exported files may also be requested by VOSS support operators for troubleshooting purposes.

1. From the **Transaction** list view, select a parent transaction.
2. From the transaction details view, choose **Export** from the toolbar. A `.zip` archive file is downloaded by the browser.

Transaction export files and format

The `.zip` archive filename format:

export-tx-<Transaction ID>_<YYYY>-<MM>-<DD>T<HH_MM_SS>.json.zip

Example: `export-tx-20705_2019-01-22T06_18_15.json.zip` for parent transaction ID 20705.

The `.zip` archive contains two files in JSON format:

- The Transaction Detail file - containing transaction (parent and sub-transaction) details as on the Admin Portal - upper level and **Sub Transactions** table entries (maximum 20000 entries) in JSON format:

  export-tx-<Transaction ID>_<YYYY>-<MM>-<DD>T<HH>:<MM>:<SS>.json

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The Transaction Log file - containing entries as on the table of **Log** entries of a transaction on the Admin Portal (maximum 10000 entries) in JSON format:

  export-tx-logs-<Transaction ID>_<YYYY>-<MM>-<DD>T<HH>:<MM>:<SS>.json

Transaction detail file format

The example snippet below shows transaction details data of the upper level parent.

- Upper level parent entries are identified by the same `pkid` and `top_level` values, with `"parent_pkid": null`.
- Child and descendant entries show different `pkid` and `parent_pkid` values. The tree of parent and child entries can be determined by inspecting these values.

```
"processor_host_name": "VOSS-voss-queue",
"pkid": "c0a03e99-0c93-4d85-8736-f05b54f8fe55",
"hierarchy": "5c46a8efce894e001453b2a8",
"submitted_time": "2019-01-22T06:18:15.804000Z",
"started_time": "2019-01-22T06:18:15.839000Z",
"detail": "[ 9\\/9 ] succeeded from [ 1 ] sheet in H2-5-VOSS4...
"top_level": "c0a03e99-0c93-4d85-8736-f05b54f8fe55",
"priority": "Normal",
"duration": 3.187191,
"submitter_host_name": "VOSS",
"txn_seq_id": "20705",
"parent_pkid": null,
"action": "Execute Bulk Load",
"message": null,
"completed_time": "2019-01-22T06:18:19.026000Z",
"operation": "execute"
```

Transaction log file format

The snippet below has been formatted for readability. The `transaction_id` in the two entries shown will correspond with `pkid` entries in the Transaction Detail file, so that the Log entries can be associated with the transactions and sub-transactions.

```
{
   "severity": "info",
   "format": "text",
   "log_id": "5c46b5a7ce894e0014569a0b",
   "time": "2019-01-22T06:18:15.871000",
   "message": "H2-5-VOSS4UC-HCS-Customer_Data_ClassOfService...
   "transaction_id": "c0a03e99-0c93-4d85-8736-f05b54f8fe55"
},
{
   "severity": "info",
   "format": "text",
   "log_id": "5c46b5abce894e0014569ab3",
   "time": "2019-01-22T06:18:19.012000",
   "message": "Summary for sheet: Sheet1, No errors",
```

(continues on next page)

Copyright © 2025 VisionOSS Limited. All rights reserved.

(continued from previous page)

```
    "transaction_id": "d7aa7333-f692-40b4-a637-80cf456c1f70"
},
```

Bulk Load

Bulk load

Tip: *Use the Action search to navigate Automate*

Overview

The bulk loader tools enable the quick and easy management of system data using pre-populated MS Excel formatted spreadsheets.

The system can generate a spreadsheet template for any resources in the system, either via the Admin Portal or via the API.

Data on the sheet includes column headers to indicate the hierarchy, action, search criteria, and attribute names of the model to which the data applies. Rows include the data for model individual instances.

Note: To carry out a bulk load, the selected model should allow add operations in the access profile for the user.

Use a single sheet in the file to manage multiple templates by adding additional header rows and data under them. A file can include multiple sheets with a single or multiple templates on each.

When the file is loaded, it can either be processed immediately or scheduled for a date and time. A scheduled bulk load file is listed on the **Schedule** list view as a *single execution* schedule type and with resource type of `data/BulkLoad`. Items on the **Schedule** list are deleted once the scheduled item has been executed. This means that after a scheduled bulk load has been executed, you will no longer see it in the list of schedules.

A single parent transaction is created for the entire bulk load. Unless a sheet is set to execute rows in parallel, each row in the bulk load sheet results in a separate sub-transaction that is executed sequentially and synchronously. If a single sub-transaction fails, the bulk load transaction continues and does not roll back the preceding sub-transactions. In the case where a bulk load sub-transaction has other sub-transactions - for example a provisioning workflow with multiple steps - failure in any of the steps may cause a roll back of all the steps in the bulk load sub-transaction.

If a sheet is set to process rows in parallel, then by default, 14 rows are processed in parallel. Refer to the topic on the bulk load sheet layout for more details.

If a file is processed and further files are loaded, they are processed in parallel. Thus, bulk load transactions are executed in parallel, as with all transactions. Bulk load transactions are executed immediately.

Transactions, once started, cannot be canceled.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Prevent duplicate numbers in the Core Feature Guide

Data export Overview

You can export data from Automate in two formats:

- JSON format
- Excel format (Microsoft Excel spreadsheets)

JSON format

Used for exporting and importing model instance operations such as:

- Add
- Modify
- Delete
- Export and import can be done via:
- Admin Portal
- API (refer to API documentation for request URLs and parameters)

Exported files are compressed:

- .JSON
- .JSON.zip
- .JSON.gz

Excel format

- Available in list or instance view of a model.
- Export can be done via:
  - Admin Portal
  - API (refer to API documentation for request URLs and parameters)
- Export options:
  - Excel (.xlsx)
  - Excel (formatted)
- Exported (formatted) Excel files reflect the Field Display Policy of the menu item, including:
  - Attribute titles and sequence
  - Group names
  - Hidden fields (except mandatory ones)

Copyright © 2025 VisionOSS Limited. All rights reserved.

Bulk export of model data

1. Choose the hierarchy to which the model belongs.
2. Choose the items to be exported from the List view and click **Export**.
3. From the **Export format** list, choose the required export format and export the selected items.

   The following file formats correspond with the selected item in the list:

File format	Description
JSON	An export containing data in JSON format as in the system database. Item properties such as strings that are empty or Boolean values that are not set, are not included. The export filename also contains a date stamp.
Excel	An export containing data and Excel columns for all fields as shown in the JSON export format. The export filename also contains a date stamp and reference to the export data type.
Excel(formatted)	An export containing data and Excel columns as arranged by any Field Display Policies that apply. The columns correspond with those of a Bulk Load Template export sheet. This sheet can therefore be used to modify and update data if required. The export filename also contains a date stamp and reference to the export data type.

4. If required, the export JSON file can be decompressed, and the JSON file (.json) can be opened in a text editor. The XLSX file can for example be opened in MS Excel.

Note: The bulk export of Device Model data will export locally *cached* data, not data on the device itself.

Bulk load template export

Overview

You can use the MS Excel format spreadsheet bulk load template of a model to easily create a template of a sheet from the user interface. See *Bulk load template sheet layout*.

The Automate multi-domain core supports the ability to generate a MS Excel format spreadsheet bulk load template for any of the resources in the system directly from the user interface.

You can populate the template sheet with data and then load it using the *Bulk Load* tool.

Excel bulk load operations using spreadsheets support multiple (tabbed) worksheets that are loaded in tab sequence. Defined configuration templates on the system can be referenced in the sheets and applied during the bulk load operation.

The field specific help of the product can be used to assist the user with populating the bulk loaders with the correct data. See *Bulk load template sheet layout*.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Perform bulk load template export

The export of a bulk load template of a model is available on the list view.

1. Choose the hierarchy where the model is available.
2. Choose the required form and choose the export option **Bulk Load Template**.

A MS Excel sheet is created that contains the bulk load template for the selected model. The sheet is available in the download directory of the browser application.

Use the bulk load template sheet to enter data.

Use the Bulk Load system tool to upload the bulk load template sheet.

Bulk load sheets

Tip: *Use the Action search to navigate Automate*

Overview

A bulk load template is a Microsoft Excel `.xlsx` format spreadsheet workbook that contains a single sheet, and is used for bulk loading data into Automate.

A tabbed workbook may contain two or more template sheets (one sheet per model). When using a tabbed workbook, bulk load transactions are carried out from left to right, starting with the far left tab, and ending at the far right tab. For example, when adding a site under a customer in a bulk load, ensure you add the customer sheet to the left of the sheet containing details of the associated site, so that the customer detail is loaded before the site.

You can use any filename for the bulk load workbook, but since the same file can be loaded multiple times, it is recommended that you use unique names to differentiate bulk uploads.

Bulk load limitations

Automate's bulk load automation templates employ advanced features, such as configuration templates (CFTs), customizable field display policies (FDPs), and GUI rules.

For some resources, generated bulk load templates won't produce the provisioning results that may be achieved when using the GUI to upload and configure data. This topic provides an overview of the bulk load limitations to consider for such scenarios.

Note: See the Bulk Load Reference Guide for more information around the specific resources where these limitations apply, the impact of the limitations, and for best practice advice for using generated loaders for various resources.

The list below describes the general bulk load limitations:

- Certain fields link together different resources

  These fields might be hidden in the GUI, or they may be read-only. In generated bulk load templates, these field are currently exposed as mandatory fields. The fields and the specific conventions that are

Copyright © 2025 VisionOSS Limited. All rights reserved.

used in the template to link the fields together are highlighted in notes specific to the resource. For example, the value for remote destination name should be specified as `RDP-<username>`.

- Certain fields are derived from other system data

  Notes specific to the resource highlights where to obtain possible values for such fields. Examples are key-value type fields of a phone's vendor configuration settings.

- Restricting data to a specific set of fields on a sheet for modification purposes may not always succeed. Instead, use all the data for a bulk loader where possible.

  Exporting an instance as a bulk loader and changing the relevant columns is advisable for most complex cases.

  Due to the workflows and logic included with relations when using a modify loader, the loader may not only include the field(s) that you wish to change.

  For instance, `relation/MicrosoftSubscriber` does work with this approach. If you need to create a modify loader on a relation, test your use case by using only the fields you want to change and validate that the resulting configuration is correct.

  If the use case is not supported, you can potentially modify the data or device model(s) that make up the relation instead. However, be aware that you are not changing a field that has dependencies on the workflow updating related entities (like assigned numbers and number inventory).

  If you have any questions, please contact your local VOSS teams or VOSS support for assistance.

- GUI rules defined in the user interface that aren't replicated in the backend workflow must be considered in the loader to achieve the same provisioning results as the GUI.

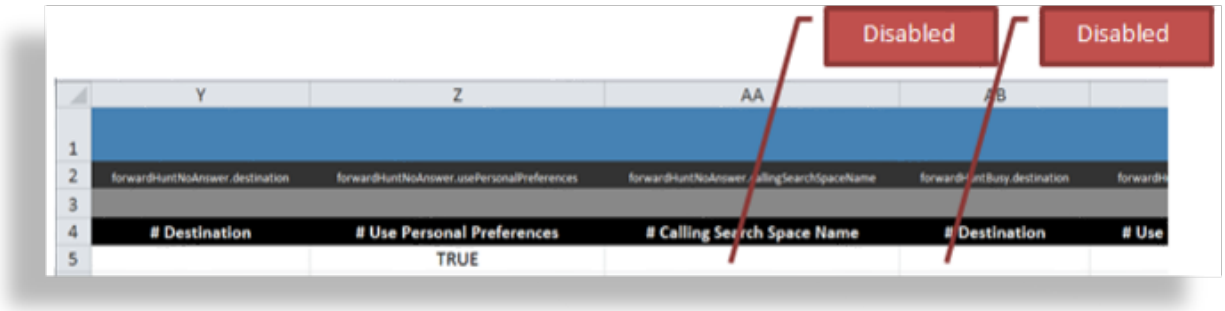
  Examples - GUI rules may:

  – Set a default value for a visible field (fixed value or derived from other data in the system). Include this column and corresponding value in the loader for this to be provisioned.

  – Set a value for a hidden field. Include the column and corresponding value in the loader for this to be provisioned. Note that this means that fields may be included in the loader that would not be visible in the user interface.

  – Make a field visible depending on some condition such as the value of another field (for example, a checkbox being selected). Include the column in the loader, and populate it under the appropriate conditions.

The image shows that a GUI rule may, for example, disable input fields based on the state of a checkbox. On the worksheet, the selected checkbox is represented as TRUE in the column. Columns associated with the disabled fields should not be filled.



Note: A set of sample bulk load sheets can be obtained from your VOSS account manager. These may assist with complexities around the use of the bulk load feature. These generated sheets allow users to get

Copyright © 2025 VisionOSS Limited. All rights reserved.

started quickly and to leverage recommended best practices for bulk loading.

Bulk loading files

This procedure uploads two or more `.xlsx` worksheets in a bulk upload.

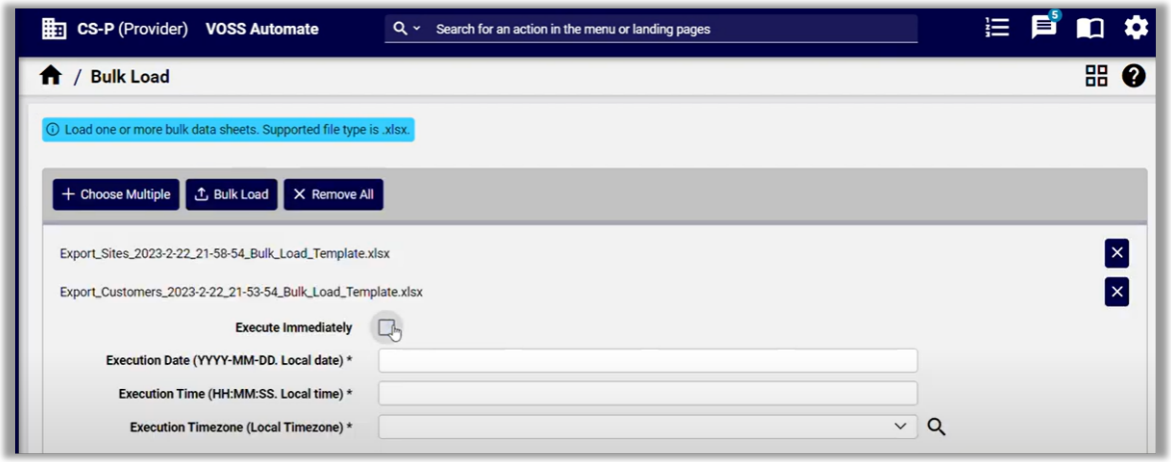
Prerequisites:

- File formats must be `.xlsx`.
- Ensure any referenced configuration templates are available.
- Verify details in each file, and ensure they contain all required information.
- Remove any comments from the worksheets, for example, comments showing as a marker in the cell with a pop-up.
- To send empty values, in the relevant cell of the value column:
  - type `<NULL>` in the cell

Note: Spreadsheet formulas in data are ignored, for example: `'=7+2'`

To bulk load files

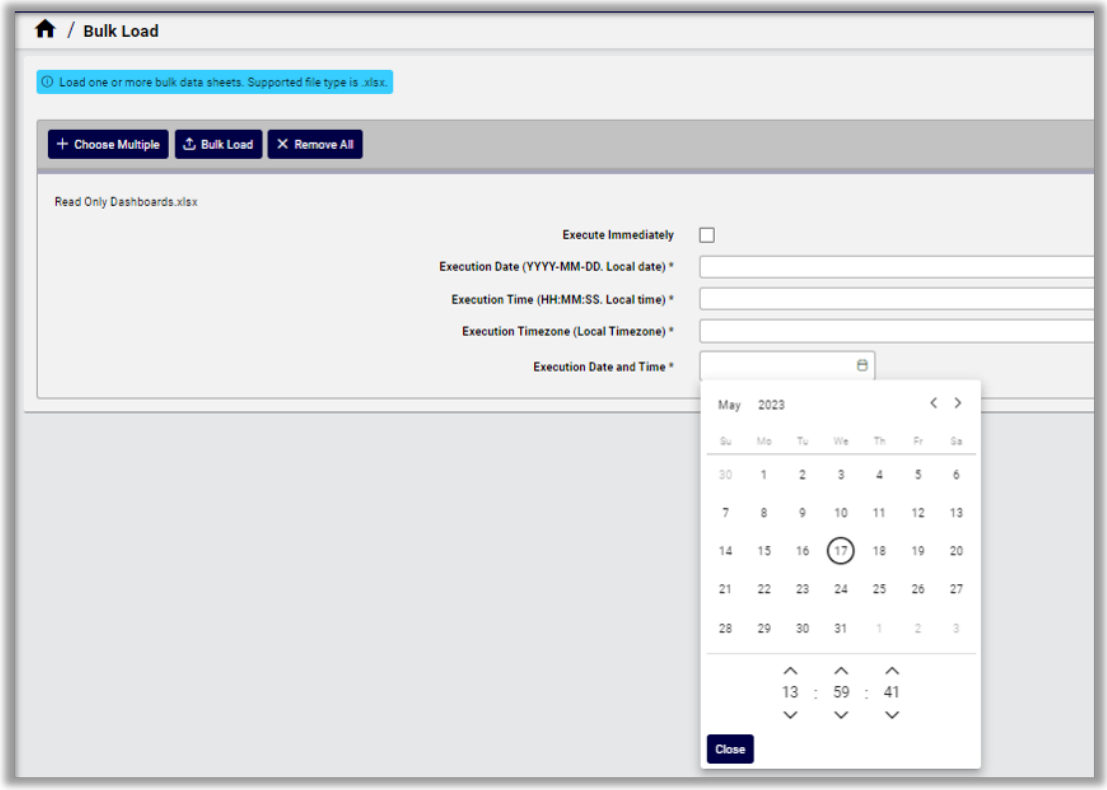
1. In the Admin Portal, go to the **Bulk Load** page.
2. Set the hierarchy to the level where you want to add bulk data.
3. On the **Bulk Load** page, click **Choose Multiple**; then, browse to the files you wish to upload.



4. Choose an option:
   - To remove any files, click the **X** icon adjacent to the filename.
   - To remove all files, click **Remove All**, and if required, choose alternative files.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- To execute the bulk load transaction immediately, select **Execute Immediately**, else, clear the checkbox and specify an execution date, time, and timezone.



5. Click **Bulk Load**.
6. Wait for the transaction to complete, then view results.

Note:

- The **Execute Bulk Load** sub-transaction list will show the transaction for each row of the sheet.
- If the transaction is scheduled for a future date, you'll need to check on it at the scheduled execution date and time. Scheduled bulk loads display in the list view of the schedule, with the name and upload date of the sheet.
- The **Bulk Load** button is temporarily disabled until the sheets that have been bulk loaded and are in progress have completed. To continue bulk loading while sheet loading is in progress, clear (remove) the current sheet or choose **Remove All** and select a new sheet to load.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Sample bulk loaders

Sample loaders enable a quick start by providing working examples of the most frequently used loaders. These can be be customized according to user requirements and data.

Furthermore, sample bulk load sheets incorporate best practices for using bulk loaders; ensuring rapid customer and user on-boarding.

Note that the sample loaders are built according to the default Field Display Policies and configuration templates that are shipped with the product. Since these are configurable, the use of non-default Field Display Policies or configuration templates may result in a change of the sample loaders. For example, if an additional field is exposed by the Field Display Policy, it needs to be added if it is to be managed in the loader.

The latest sample bulk loaders can be obtained from your account team.

Bulk load template sheet layout

Overview

This topic describes a typical generated sheet when using the Export Bulk Load Template menu option.

Colors and styles are applied to the exported sheet:

Header rows	Dark colors
Base group titles	Yellow text
Mandatory fields	Title text headers are red
Optional fields	Text headers are white

- dark colors style for header rows
- yellow text for base group titles
- mandatory fields have red title text headers
- optional fields text headers are in white

Although an attribute that has nested attributes may be optional, if this attribute has mandatory nested attributes, then the containing attribute becomes mandatory. If a field is mandatory, it is shown on the sheet regardless of any Field Display Policy instruction to hide it.

The Field Display Policy that applies to a menu item from which a Bulk Load Template Export is carried out, is applied to the exported sheet as follows:

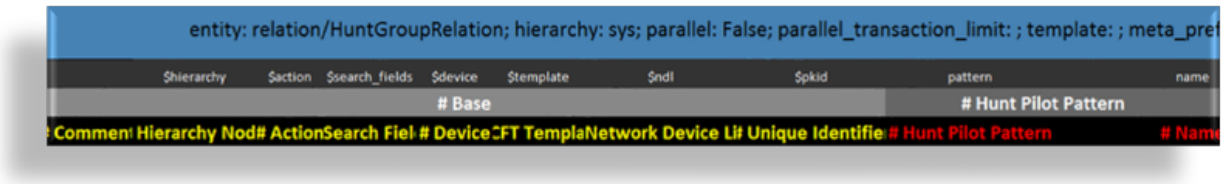
- Titles of attributes
- Sequence of the attributes
- Group names
- Hidden fields, with the exception of mandatory fields.

Note:

- Macros can be included in the loader to either be loaded as text or evaluated as part of the load. See documentation in this guide around *evaluate_macros* header for more details on macro behavior in the loaders.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- A single sheet of a file can be used to manage multiple templates by adding additional header rows and data under them. A workbook file can include multiple sheets with single or multiple templates on each.



Refer to the example sheet snippet. A bulk load sheet contains the following information:

- Sheet name (tab on spreadsheet workbook)
- Row 1 - Resource and instructions
- *Row 2 - Base columns (grouped by # Base in Row 3)*
- Row 2 - Column names
- Row 3 - Group or description
- Row 4 - Title
- Data rows

Sheet name (tab on spreadsheet workbook)

Any name can be provided on the tab or sheet If the name is prefixed with a hash (#) on the tab, the sheet is ignored during loading.

Row 1 - Resource and instructions

The exported bulk loader template will have the resource as target entity (model) as well as the hierarchy shown on the top row of the sheet. Verify the entity in the first row of an exported sheet. The reference data in the first row is of the format shown below, with variable values indicated in curly brackets `{}`:

```
entity: {entity name}; \
hierarchy: {hierarchy}; \
parallel: {True | False}; \
parallel_transaction_limit: {n}; \
template: {config_template}; \
meta_prefix: {c}; \
evaluate_macros: {True | False}
```

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Variable
entity	*{entity name}*: the name of the model, in the format *{modeltype}/{model name}*, for example `data/User`
hierarchy	*{hierarchy}*: the hierarchy, in the format *{level1}.{level2}.{level3}*, where *{level1}* is the first system level. Verify the hierarchy at which the bulk load should take place.
parallel	True or False. By default, the value is False and rows are processed sequentially. If multiple templates are entered on a single sheet, they should all *only have a single value*: True or False. Sheet rows can be processed in parallel. The sheet should then not contain multiple, sequence dependent models. If there are a large number of rows for complex models on the sheet, the duration of a bulk load transaction is significantly reduced by parallel processing. By default, 14 rows are processed in parallel, since bulk loads are low priority transactions that are limited to 50% of the maximum allowed parent transactions, which is by default set to be 30 per unified node. The default value supposes that one slot is used by the parent bulk load transaction itself. The maximum allowed parent transaction limit can be modified from the Command Line Interface (CLI) using the command: `voss workers <number>`
parallel_transaction_limit	The maximum number of rows that can be processed in parallel by the bulk load at any given time. The minimum value that can be set is 1 and the maximum is 100.
template	The configuration template *{config_template}* that is associated with the user's menu item for the *{entity_name}* from which the export was carried out. The exported sheet will show a row of values from the configuration template. When a sheet is created to bulk load, the configuration template should be available on the target system and it will only apply to rows on the sheet that has **add** specified in the `# Action` column. Note that this header item is not used when configuration templates are loaded.
meta_prefix	By default, the value is $. The # character cannot be used, as it is used for comments. The character is prefixed to the `# Base` group of columns in Row 2. See *Row 2 - Base columns (grouped by #Base in Row 3)* *Row 2 - Base columns (grouped by # Base in Row 3)* The purpose of the prefix is to distinguish a special set of base columns from the entity attributes on bulk load sheets. Note that the bulk load sheets will fail to load if the hash (#) character is used as prefix. An error message will be shown in the transaction log.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Variable
evaluate_macros	By default, the value is `False`. When set to `True`, named macros can be added as values to be evaluated before the sheet is loaded. Otherwise, the value is a string. The format of the macro is *{{ fn.bulkload_evaluate macro.NamedMacro }}*, where *NamedMacro* is the name of an existing `data/Macro` instance. The function prefix `fn.bulkload_evaluate` is required in the value for the macro to be evaluated. See for example *Bulk load sheet macro evaluation*. Note that `fn.bulkload_evaluate` is not available via the Macro Evaluator. For testing purpose using the Macro Evaluator, please use the `fn.evaluate` function prefix.

Related topics

- *Bulk load sheet macro evaluation*
- *Row 2 - Base columns (grouped by # Base in Row 3)*

Row 2 - Base columns (grouped by # `Base` in Row 3)

The table describes column values with the default value of `meta_prefix`, that is, column names by default prefixed by `$`.

The columns provide more detailed instructions or overriding data for a row.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Value
Comments	Any row containing a hash (#) in column A is considered a comment row and is ignored. Empty rows are also ignored. Column A - the first column is also a `# Comment` column, so that any value entered in it is considered a comment. If all rows on a tab are commented, but the tab name itself is not commented, the tab sheet load will fail.
`$hierarchy`	A hierarchy column with the name `# Hierarchy Node` is also available so that individual rows of a sheet can be loaded to a specified hierarchy. If a hierarchy is specified in this column for the row, it takes precedence over the hierarchy in the first row. The format for the hierarchy in the row is the same as for the first row: the full hierarchy, with levels separated by dots.
`$action`	Any row that contains an action in the `# Action` column : **add**, **delete**, **modify**, **execute**, **purge** or a custom action name, will have the action carried out. The action values in the column are case insensitive. If no action is entered, the **add** action is carried out. The list below shows the functionality for the values entered in the row. Also refer to the Search Fields entry below: • **add** or empty - the data in the attribute columns is added. Any values in the `# Search Fields` column are ignored. • **delete** - the row matching the unique criteria in the `# Search Fields` column is deleted. • **modify** - the row matching the unique criteria in the `# Search Fields` column is updated with values in the attribute columns. Refer to the Search Fields entry below. • **execute** - if the action is available for the model, the row matching the unique criteria in the `# Search Fields` column is executed, using any values entered in attribute columns. • custom action name - if the custom action is defined for the model, it is carried out for the row matching the unique criteria in the `# Search Fields` column.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Value
`$search_fields`	The column applies to rows where the action is not **add** and consists of a colon-separated list of attribute names and values, for example, `fullname:'John Smith',username:jsmith`. Note that if present, the `pkid` field takes precedence over search fields criteria when locating a resource. If search field criteria should apply to locate the resource, remove the `pkid` value of the resource from the sheet. • **delete** - the search fields and corresponding attribute values uniquely identify the model instance to delete. • **modify** - the search fields and corresponding attribute values uniquely identify the model instance to modify, with the values to modify in the attribute columns. • **execute** - the search fields and corresponding attribute values uniquely identify the model instance to execute. **Note:** Where the sheet is for a Relation model, only the left model attributes in the Relation can be in the Search Fields column. This is the standard search behavior for Relations. If it is necessary to carry our a search on relation data, the search can be applied to the underlying models for the purposes of bulk loading or export.
`$device`	The column is used when a sheet includes attribute columns that belong to a device model. This column then contains the comma-separated list of business keys of the device model, as well as its hierarchy. These values narrow the search for the device to which the data in the sheet applies. Examples of such sheets would contain device models or relations that have device model attributes in the left hand association of the relation. The format of the values in this column is: `<business_key1>,<business_key2>,...,<business_keyn>,<device_hierarchy>` For example, if a CM instance in a model `data/CallManager` has `host` and `port` as business keys, the value would for example be: `10.120.2.175,8443,sys.Varidion.InGen.Tokyo`
`$template` (Configuration Template)	If a row that contains a Configuration Template name that applies to the model, this template is applied to the row when it is loaded. Upon bulk loading, values in this column will override any value for `template` in the sheet header.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Column	Value
`$ndl` (Network Device List)	The column is used when a sheet includes attribute columns that belong to a device model. This column then contains the name of the Network Device List that includes the required device in the list of devices. The NDL can be filled in as either the business key friendly name or in the NDL business key format, for example *["322-CL1-NDL", "hcs.MTLAB.Ops.IBM"]*. The friendly name ("322-CL1-NDL") will then be used during the bulk load. If the Device column is also filled in, then the value in the Network Device List column overrides it.
`$pkid` (Unique Identifier)	On modify, delete, execute, and custom action operations, this `pkid` is used to identify the resource represented in the row data. Note that if present, the `pkid` field takes precedence over search fields criteria when locating a resource. If search field criteria should apply to locate the resource, remove the `pkid` value of the resource from the sheet. The `pkid` is unique to the resource on the particular database and cannot be relied upon when attempting to manipulate an identical resource on a different database.

Note: Macros inserted into the Base columns will not evaluate. See: *Bulk load sheet macro evaluation*.

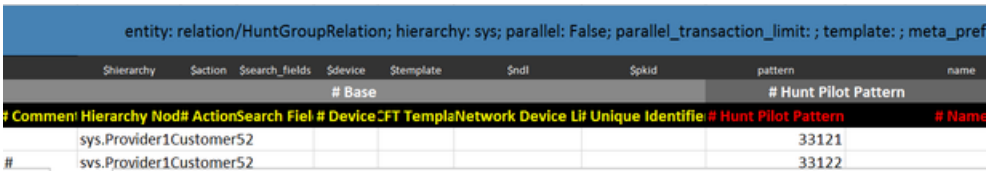
Row 2 - Column names

- base column names (prefixed by the `meta_prefix` character and listed above)
- attribute names. Entity attribute names show as column header data in the spreadsheet.

Columns can be in any order in a row. Nested object attribute names follow a dot notation.

Array objects will be sorted, so that attributes with names such as `filter_fields.<number>.xx` will be in sequence: `filter_fields.0.xx`, `filter_fields.2.xx`, and so on - before further ordering (represented by `.xx` here) is applied.

- If a column header starts with a #, the column will not be loaded.
- If a column header is blank, this indicates the end of the sheet header. Subsequent columns will not be loaded.



	$hierarchy	$action	$search_fields	$device	$template	$ndl	$pkid	pattern	name
			# Base					# Hunt Pilot Pattern	
# Commen	Hierarchy Nod	# ActionSearch Fiel		# Device	FT Templa	Network Device Li	# Unique Identifie	# Hunt Pilot Pattern	# Name
	sys.Provider1Customer52							33121	
#	sys.Provider1Customer52							33122	

Copyright © 2025 VisionOSS Limited. All rights reserved.

Row 3 - Group or description

The row provides a description of a column or columns (as for example `# Base` for the sheet base columns), or else the group name of attributes that are grouped on the GUI as tabs on the detail or input GUI form.

A group is specified in the row by merging the group name across all the columns of the group. For attributes that are required and are not grouped in the GUI (or may be hidden in the GUI), the group name: Not Grouped Fields is given on the sheet.

"Default" values of attributes in this group need to be removed from an exported sheet before the sheet is used to bulk load rows.

Row 4 - Title

Title of:

- the reference for base column names (hierarchy, action and so on)
- the column attribute as on the GUI. This title may be modified by a Field Display Policy.

Data rows

The exported template contains no data.

Important: As a part of bulk loader sheet design, attention should be paid to the API payload posted to the system. The data entered in the loader sheet columns should correspond with the API payload.

GUI drop-down lists may contain user-friendly titles, while the actual value sent to the API may differ.

Export data sheet layout

This topic explains formatted and unformatted exported sheets containing data.

General structure

- **Header and columns**: The header and column layout of formatted and unformatted sheets correspond with the bulk load template sheet.
- **# Comment column**: Displays "Exported data" in green for each row of data.
- **# Hierarchy Node column**: Indicates the source hierarchy of each exported row.
- **Sheet header (hierarchy)**: Shows the hierarchy used during export.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Key columns

- **# Device**: Lists the device's business key (for example, host, port, hierarchy) if device data is exported.
- **# CFT Template**: Displays the name of the applied configuration template (if used), also shown in the header. For example, if it applied to the Admin Portal form, the *# CFT Template* column will show this name for each row, as well as the *template* value in the sheet header. If the sheet is used for loading, row values override header values.
- **# Unique Identifier (pkid)**:
  - Identifies the exported resource in each row.
  - Used for modify, delete, execute, and custom actions to identify the resource instance on the database represented in the row data.
  - Takes precedence over search fields.
  - Unique to the resource on the particular database. Cannot be reused across different databases.

Sheet types

- **Formatted Excel Export**: Columns match the bulk load template sheet.
- **Unformatted Excel Export**: Columns reflect the properties of an exported JSON file (only non-empty strings and boolean values are included).

Reusability

- Formatted, export sheets can be used as bulk load templates to bulk load data
- For other actions, complete the **# Search Fields** column. Refer to *Bulk load template sheet layout*.
- Remove *Default* values from ungrouped fields before bulk loading.

Limitations

- Excel cell content is limited to the maximum length allowed in a Microsoft Excel cell (32 767 characters).
- Longer property values will be truncated in the exported sheet.

Bulk load sheet macro evaluation

Bulk load sheets can be configured to allow for macro evaluation.

The first row of a bulk load sheet has a variable to enable or disable macro evaluation (see *Bulk load template sheet layout*.:

```
evaluate_macros: {True | False}
```

- If the variable is set to `True`, macros in a sheet will be evaluated upon loading. In this case, it is important that:
  1. The macro be prefixed with `fn.bulkload_evaluate`.
  2. A named macro must be used, in other words, a `data/Macros` instance. Macro functions (`fn.<name>`) cannot be used here.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. If the named macro that is used evaluates to a boolean or integer value, it will be evaluated and the sheet will be processed with that value.

For example:

1. If the sheet is used to update a site at its hierarchy, and the `evaluate_macros:` value is set to `True` in the first row, then:
   - The macro `{{ fn.bulkload_evaluate macro.SITENAME }}` will be evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - The macro `{{ fn.evaluate macro.SITENAME }}` will be *not* evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - The macro `{{ macro.SITENAME }}` will be *not* evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - The macro `{{ input.sitename }}` will be *not* evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - Rows containing entries with a *combination* of the type `{{fn.bulkload_evaluate <named macro> }}` and other types macros will *only evaluate* the former type and load others as plain text.
   - Macros (in any format above) entered into the Base columns of a sheet will *not* evaluate - for details on the Base columns, see *Bulk load template sheet layout*.
2. If the sheet is used to update a site at its hierarchy, and the `evaluate_macros:` value is set to `False` in the first row, then *all* macros entered will be inserted as plain text.

Note: If the named macro needs to be tested with the macro evaluator, the format is {{ fn.evaluate macro.SITENAME }}.

- See the topic on macros in VOSS Automate documentation for named macro examples.
- For further details, also refer to the Advanced Configuration Guide and Named Macro Reference.

Import

Import

Overview

Model definitions and instances can be imported using JSON files. These can be compressed (`.json.zip`) or be uncompressed files with extension `.json`.

The format of the JSON files should correspond with the JSON schema for the model or instance that is imported. Typically, a model instance is exported as a JSON file in order to obtain such a schema. The export can then for example be edited as required.

For each model instance in a JSON file, if it contains the same values for a business key as an existing model instance, then the import will update the existing instance. Otherwise, the import will add a model instance. The business key of a model is specified on its design form and can be seen in the Add Form schema of the Model API Help Reference.

When exporting items that belong to a package, all hierarchy information will be removed from item meta business keys so that the packages have no hierarchy.

The importing process will still adhere to the hierarchy specified in the meta of each item except for a data/Package instance, which will be imported at the import hierarchy (breadcrumb hierarchy). For items

Copyright © 2025 VisionOSS Limited. All rights reserved.

other than Packages, the hierarchy where the items is loaded can be overridden (to the same or lower hierarchy level only) by specifying the hierarchy in the meta of the item.

If no hierarchy is found in the meta of the item, then the hierarchy will be taken from the import hierarchy (breadcrumb hierarchy).

Import a File

1. Choose the hierarchy level for the import (not applicable to packages - see *Import* for more details).
2. Go to the **Import** page (default menus **Administration Tools > Import**).
3. Choose the file (`.json`, `.json.tar.gz`, or `.json.zip`) that you want to import. Wait until the file name is displayed on the form.

   Note: An archive file may *only contain one* JSON file.

4. Click **Import** to import the file to the hierarchy.

Alerts

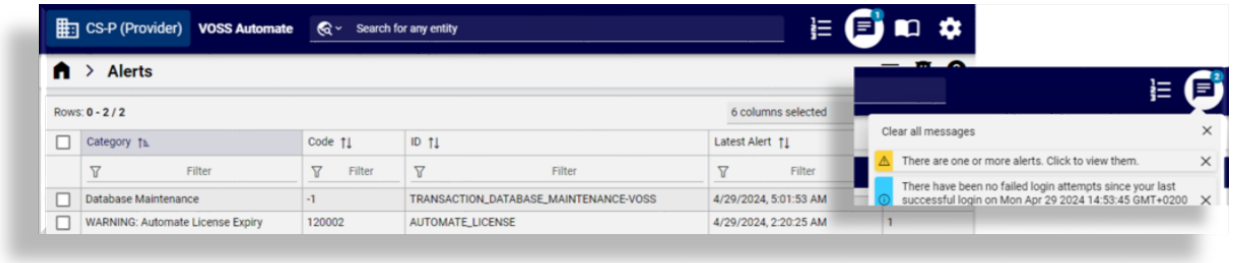
Alerts

Overview

Alerts in Automate are messages that are triggered by back-end processes when certain conditions are met. While alerts typically indicate that the system is in an error state, the conditions that trigger alerts can be related to system performance, task completion, or any metrics that are important to the functioning of the system.

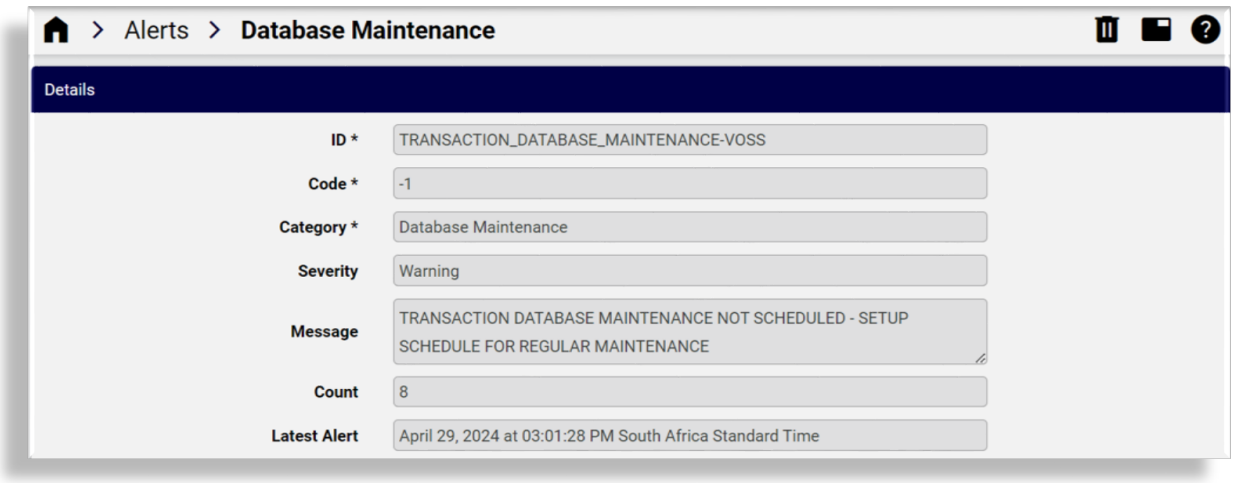
Note: You'll only be able to view alerts if your access profile permissions allow it (read permissions on `data/Alert`).

Alert notifications display via the **Messages** icon, and all active alerts are listed on the **Alerts** page. You can click the icon to open the list, or use the **Search** bar to locate the **Alerts** page in your system.



You can click on an alert in the list on the **Alerts** page for more information about the alert.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Alerts can be customized for the needs of the organization to ensure that relevant parties are notified promptly when specific events occur.

Alerts are enabled by default for the following functionality:

- Database maintenance
- Licensing
- Change notifications
- Number inventory availability

Provider admins can view all alerts, including alerts related to the database or licensing. Once any user clicks on an alert link via the Messages icon, the flag no longer displays in the notifications lists of other users. The alert will appear in the list until its deleted.

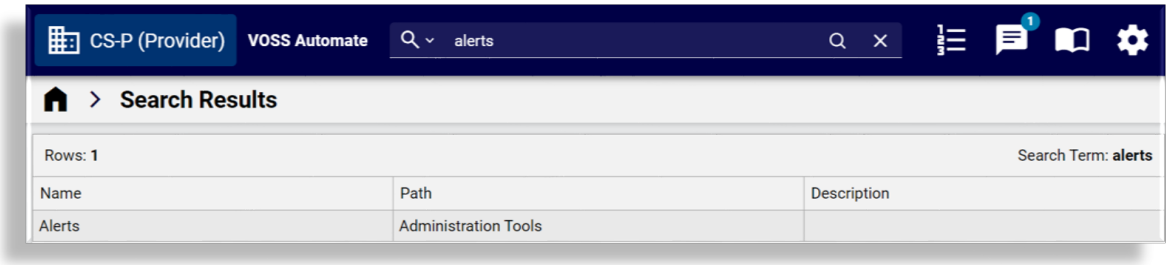
Related topics

- Cisco UCM Change Notification (CNF) Alerts in the Core Feature Guide
- Error Messages in the Platform Guide

View alerts

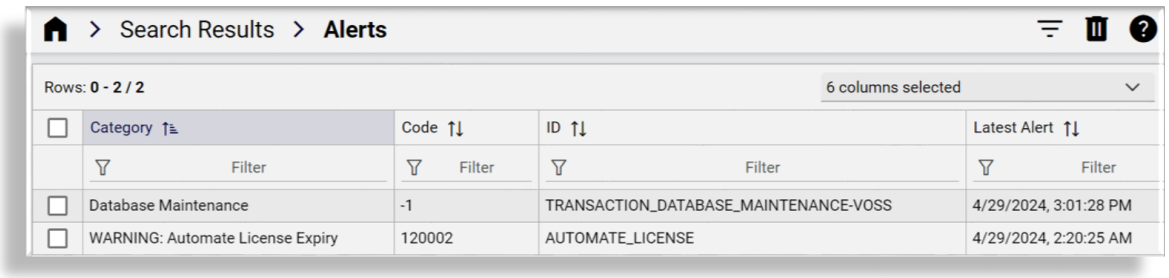
This procedure displays the alerts page list, and allows you to inspect the details of a selected alert.

1. To open the **Alerts** page, click the toolbar **Messages** icon, or locate the page via the **Search** bar.



2. On the **Alerts** page, review currently active alerts.

Copyright © 2025 VisionOSS Limited. All rights reserved.



The table describes the columns on the **Alerts** page summary list view:

Column	Description
Category	The alert category - either Database Maintenance, Licensing, Change Notification, or Number Inventory
Code	The error or warning code associated with the alert.
ID	The unique identifier, referencing the source of the alert.
Latest Alert	A timestamp for the last time this alert occurred.
Count	The number of times the same alert has occurred for a specific device. Alerts with the same ID and code updates the count of this alert as well as the last time that the alert occurred. This means that a single alert is shown on the list for each alert with the same ID and code.

3. Click on an alert that you want to inspect to open its **Details** page.
4. View the alert severity level (either Error, Warning, or Info), and in the **Message** field, view information around how to resolve the alert, for example, to renew a license, or to schedule database maintenance.
4. Once you've resolved the issue that raised the alert, you can delete the alert from the **Alerts** list.

Alert types

For alert codes also see:

the Error Messages topic in the Platform or API Guides and SNMP Traps in the Platform Guide.

Database maintenance alerts

If database maintenance schedules have not been set up from the Command Line Interface (CLI), alerts are shown *at the provider level hierarchy* for each required schedule.

The schedules are required to periodically:

- Archive or delete database transaction logs (CLI: **voss transaction archive** or **voss transaction delete**)

Refer to the Platform Guide topic "Enable Database Scheduling " for details.

The format of the alert is:

- ID: A generated identifier:
  - `TRANSACTION_DATABASE-<hostname>`

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: The `<hostname>` will be a primary unified node. These are where alerts are generated.

- Code: An error or warning code associated with the alert. (`-1`)
- Alert category: `Database Maintenance`
- Severity: `Warning`
- Message:
  - `TRANSACTION DATABASE MAINTENANCE NOT SCHEDULED`
- Count: Displays the number of times the alert has occurred.
- Latest Alert: Displays the last time this alert occurred.

Alert Code	Alert ID	Alert Category
-1	TRANSACTION_DATABASE-<hostname>	Database Maintenance
-1	CACHE_DATABASE-<hostname>	Database Maintenance

Licensing alerts

Alert Code	Alert ID	Alert Category
36200	Hierarchy Resolution Failure	Licensing
36100	License Audit File Transfer or data/SmtpDestination, data/HttpDestination, etc.	License Audit File Transfer

Change Notification (CNF) alerts

Alert Code	Alert ID	Alert Category
calling exception code: 40000-40006, 40008	device pkid OR business key	Device Change Notification Collector <model type>

Number inventory alerts

If alerts have been enabled on available number inventory numbers in global settings, alerts are raised when the availability threshold is exceeded. See: *Global settings*.

Alert Code	Alert ID	Alert Category
110000	Number Inventory Threshold of {{ pwf.INI_ALERT_THRESHOLD }}% Exceeded . . .	Number Inventory

Copyright © 2025 VisionOSS Limited. All rights reserved.

In the GUI, the alert **Message** field also provides details on the INI threshold, availability, hierarchy, count and a CSV list of nodes and numbers, as shown in the alert message template below. (Long message strings are truncated). For details on macro references, refer to *Email HTML templates*:

```
{{ pwf.INI_ALERT_HIERARCHY_NODE_TYPE }} [{{ pwf.INI_ALERT_HIERARCHY_NAME }}].
Hierarchy full path = {{ pwf.INI_ALERT_HIERARCHY }}
Total INI Available = {{ pwf.INI_ALERT_TOTAL_INI_AVAILABLE }}
Total INI count = {{ pwf.INI_ALERT_TOTAL_INI_COUNT }}
Total percent available = {{ fn.as_string pwf.INI_ALERT_TOTAL_PERCENT_AVAILABLE }}%

{{ pwf.INI_ALERT_NODES_EXCEEDED_THRESHOLD_DATA_ALERT }}
```

Important:

- If alerts have been enabled, a schedule called "InternalNumberInventoryAlert" is also created that is by default set to run daily if the availability threshold in the global settings is exceeded. For schedule management, see *Schedules*.

Cisco UCM Change Notification (CNF) alerts

Overview

The Cisco UCM Change Notification Feature (CNF) is enabled to display alerts.

CNF alerts don't need to be manually configured in Automate. Admin users receive alerts when the collector process is in an error state.

Admins can view and delete alerts at the hierarchy they're logged in at and at lower hierarchies. For example, Provider, Reseller, and Customer administrators can view alerts raised at the Customer level (sys.hcs.provider.reseller.customer), but a Site admin cannot view such alerts.

When a CNF alert is raised, you're notified of the alert via the toolbar Messages icon in the Admin Portal. Click the **Messages** or **Notifications** toolbar button to view the alerts, or go to **Alerts**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CNF alert properties

Change notification (CNF) alerts have the following properties:

Property	Description
ID	A generated unique identifier of the target device of the collector. For CUCM, the ID displays the host name, port, and hierarchy.
Code	An error or warning code associated with the alert.
Category	The alert category - Device Change Notification Collector
Severity	Automate displays severity codes and messages as follows ("{}" indicate device or number placeholders in the messages). Each alert has some properties, for example, severity (Error, Warning or Info), the number of times that the same alert has been raised, and the time stamp of the last alert instance.
Message	Displays error message description and the statement to fix the error.
Count	Displays the number of times the alert has occurred for a specific device.
Latest Alert	The last time this alert occurred.

Note: Administrators can filter alerts by any of the alert fields.

CNF error scenarios

Automate displays CNF alerts for the following error scenarios:

- Warning:

  45000: Unprocessed changes at 75% of limit for device {}. Please configure and run the necessary data syncs.

- Error:
  - 40000: Device change notifications are not supported for device {}.
  - 40001: Device change notification data for device {} has been lost. Tracking data has been repaired and collector process will continue. Some changes may have been lost, please run a full sync on the device.
  - 40002: Device change notification tracking data for device {} has become corrupted. Tracking data has been repaired and collector process will continue. Some changes may have been lost, please run a full sync on the device.
  - 40003: Device change notification tracking DB write for device {} failed. The collector process will continue to attempt DB writes. Please investigate the database write failure.
  - 40004: Device change notification data DB write for device {} failed. The collector process will continue to attempt DB writes. Please investigate the database write failure.
  - 40005: Unable to repair device change notification tracking data for device {}.

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - 40006: Too many unprocessed changes recorded for device {}. No new changes will be recorded until at least {} changes are processed. Please configure and run the necessary data syncs.
  - 40008: Could not update pending changes data for device {}. {}.

The administrator reads, inspects, acts on (for example, run a full sync on the device), and then manages alerts of the CNF collection service. The administrator can delete the alert from the list only when the issue that raised the alert has been resolved.

Note: If the Administrators forget to remove the CNF alert after resolving it, the alert will still be shown when they log in to Automate. We strongly recommend removing the alert after resolving it.

Alerts field reference

- The field Title is indicated in bold. An asterisk * indicates the field is mandatory.
- If the field Type is an array, its the Field Name has a .[n] suffix, where n is the array index placeholder.
- Object and array names are listed to provide the context of fields.
- If a field belongs to an object or an array, the full name is in dot separated notation.
- Where cardinality is shown, the range is [MinItems..MaxItems].
- If a field has a Default value, the value is shown.
- If a field has a Pattern, the regular expression pattern is shown.

Copyright © 2025 VisionOSS Limited. All rights reserved.

ID *	
Field Name	alert_id
Description	The unique ID of the alert
Type	String
Code *	
Field Name	alert_code
Description	The code of the alert
Type	String
Category *	
Field Name	alert_category
Description	The category of the alert
Type	String
Severity	
Field Name	alert_severity
Description	The severity of the alert
Type	String
Choices	[“Error”, “Warning”, “Info”]
Message	
Field Name	alert_message
Description	The message describing the alert
Type	String
Count	
Field Name	alert_count
Description	The number of times this alert has occurred
Type	Integer
Latest Alert	
Field Name	alert_timestamp
Description	The last time this alert occurred
Type	String
Format	date-time

Dashboard Exports

Schedules

13.2.3. Overbuild Tools

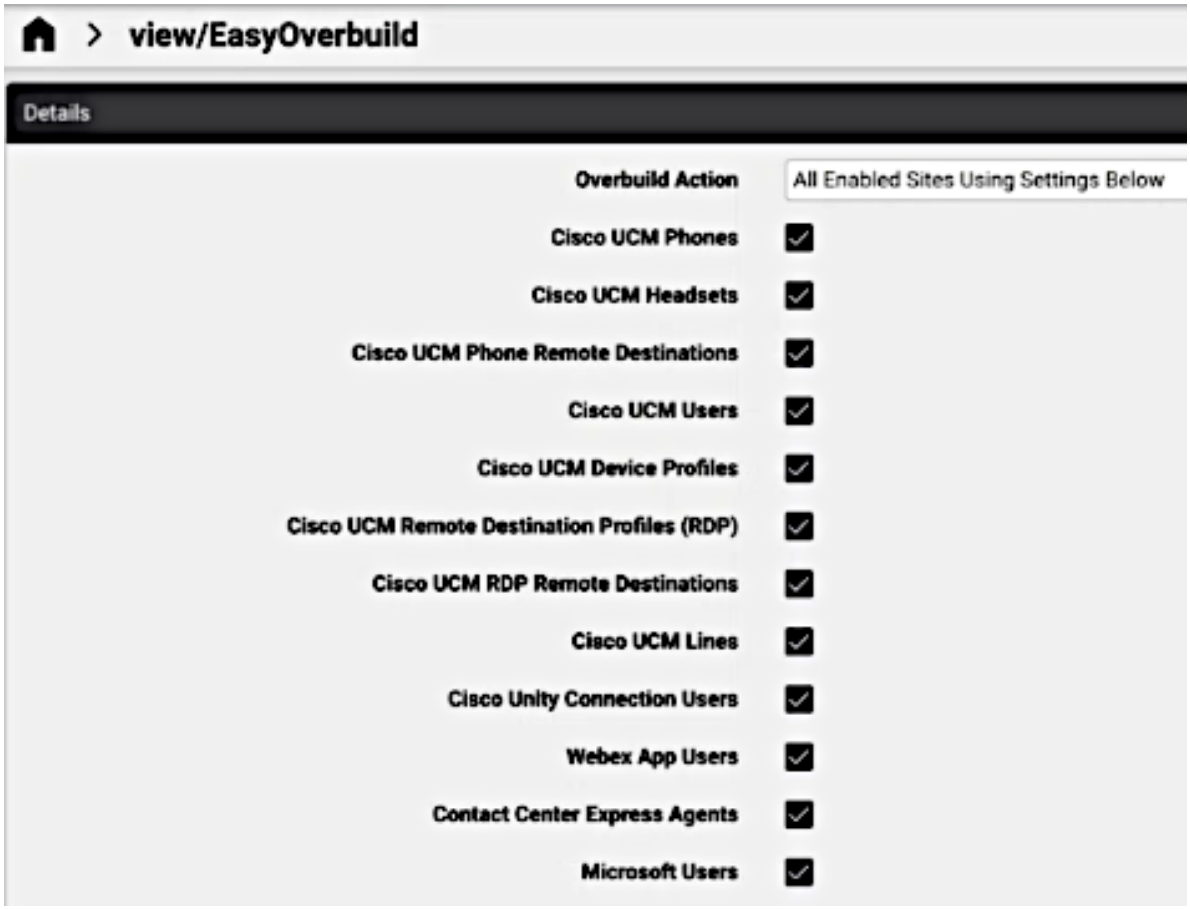
Introduction to overbuild

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overview

Automate's overbuild tool allows Provider and Reseller administrators to integrate vendor system components into Automate, without re-provisioning, if required.

- Sites must be included in an overbuild via the site's *Site Default* settings.
- The available options on the interface are in accordance with features enabled in **Global Settings** - see: *Global settings*.



- For users of **Microsoft Defender** in Automate, the overbuild tool to use applies Model Filter Criteria - see: *Overbuild with Microsoft Defender - by Model Filter Criteria*.

Related topics

- *Overbuild for Microsoft*
- *Overbuild with Microsoft Defender - by Model Filter Criteria*
- *Overbuild for Cisco*
- *Run overbuild*
- *Run dial plan overbuild*
- *Overview tool*
- *Device Models*

Copyright © 2025 VisionOSS Limited. All rights reserved.

- *User phone associate tool*
- *Overbuild Analog Gateway*
- *Filter calling search spaces and assign a class of service*
- *Move Phones*
- *Move users*
- *Overbuild Defaults tab*
- *Number inventory*
- *Number inventory audit*
- *Customer Onboarding Quick Start Guide (Multiple Vendors)*
- *Microsoft Quick Start Guide for Automate*

Scheduling overbuild

The first time you run the overbuild, an overbuild schedule is automatically created for a customer in Automate. You can configure the schedule to run at a predefined interval, instead of running it manually.

Typically, this is done if you're expecting a consistent stream of additions of resources in the underlying applications.

The scheduled overbuild allows the system to move the new resources that are synced in to the correct site if they match the overbuild criteria. This is the same as running the overbuild manually.

The default schedule (named "Overbuild_CustomerSchedule") is disabled. You can review the schedule details, update the frequency and other schedule details, and then activate it if you would like to schedule it to run.

The scheduled version of overbuild executes the overbuild process for the customer, using the overbuild settings in the site's site defaults, with the same result as manually invoking overbuild in the Admin Portal (via the Run Overbuild action, "All Enabled Sites Using Site Defaults Doc Overbuild Settings").

Moving model instances

If "move" is enabled for a model, instances can be moved from their current hierarchy to another hierarchy. "Move" can be enabled for data models, device models, and relations.

For lists of objects impacted by a move, refer to:

- For data and device models: *Dial plan elements moved to the site hierarchy*
- For user management models: *Move user management models*

Instances can only be moved up in the hierarchy if the administrator is at a higher hierarchy. For example, for an instance at level cust1.site1 and the level cust1.site2 also exists, then the user needs to be at level cust1 to carry out a move of this instance 'sideways' to cust1.site2 by going up and back down the hierarchy levels.

The move is typically used in conjunction with data sync, which pulls the entities in, for example users, phones, dial plan, and so on. By default the entities reside at the level of the cluster, so the move feature allows them to be allocated to a different hierarchy (if needed).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Move rules

From the user interface, the following move rules apply:

- On the Admin Portal, the only option shown on the drop-down is to move an item to a lower hierarchy.
- For the core application and the Overbuild tool:
  - LDAP device models can be moved to a hierarchy that is at or below the hierarchy where the device is located, regardless of the Network Device List Reference (NDLR).
  - Non-LDAP device models can be moved to a hierarchy where the device is located.
  - Non-LDAP device models can be moved to a hierarchy where the NDLR references the associated device.
  - Other instances at a hierarchy node can only be moved to a hierarchy that is below their current hierarchy.

Once the resource is moved, the metadata of all the resources at the moved hierarchy and below is updated to indicate the latest changes in the hierarchy path.

Note: For User Management local administrators and users, where the language is derived from the default hierarchy language, the default language is recalculated based on the new hierarchy tree location.

Move user management models

Administrators have permissions to manually move these user management models:

- Lines
- Voicemail
- WebEx
- Webex App
- Hunt Groups
- Call Pickup Groups

It is recommended that you use the dedicated tools to move users and phones between customer and site hierarchy levels.

Moving user management list view items

1. Log in as a customer administrator or higher.
2. Choose the relevant hierarchy at the user management functionality where you want to move an item.
3. From the list view, select items to move.
4. Click **Action > Move**. Select the target hierarchy.
5. Click **OK**.

The items are moved to the selected hierarchy, and will then be shown in their new hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Cisco Overbuild

Overbuild for Cisco

Cisco

Tip: *Use the Action search to navigate Automate*

Overview

Automate's overbuild feature allows Provider and Reseller administrators to integrate an existing, deployed Cisco Unified Communications Manager (Cisco UCM) system into Automate without re-provisioning, unless required.

This option is available for single-cluster dedicated deployments only.

Overbuild tools allow an administrator manage data synced from existing configurations in Cisco UCM and Cisco Unity Connection (CUC).

Important: It is recommended that VOSS services are engaged during the initial use of the overbuild feature to help ensure optimized processes and guidance.

Although a deployed Cisco UCM system does not contain Automate components such as hierarchies or users, the relationship between Cisco UCM components makes it possible to, for example, create an Automate user at a site hierarchy during the overbuild process. The necessary workflows, macros and brownfield move processes are available for this purpose. You will not need to access these tools directly; they are part of the **Run Overbuild** user interface.

The table summarizes the overbuild logic:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Component	Description
Cisco UCM Phones	This is based on the device pool of the phone. It will be moved to a site based on the device pool matching one of the device pools set up under the site defaults for a site.
Dual Mode Remote Destinations	This will move the remote destination to the site of the dual mode device.
Cisco UCM Phone Remote Destinations	(Provider deployment). This will move the remote destinations to the site of the associated phone.
Cisco UCM Users	If the user has an associated phone, that user is moved to the same site as the phone. A user without an associated phone must be manually moved to the relevant site, using the **Move Users** menu (under either **User Management** or **Overbuild**). It is recommended that you do this prior to the overbuild, so that all their related services are moved during overbuild, or you will need to run the overbuild again, after moving the user, to handle their related services.
Cisco UCM Device Profiles	This will move the device profile to the same site as the user associated to the device profile.
Cisco UCM Remote Destination Profiles	This logic is the same as phones, based on the device pool of the RDP. It will be moved to a site based on the device pool matching one of the device pools setup under the site defaults for a site.
Cisco UCM RDP Remote Destinations	This will move the remote destination to the same site as the associated remote destination profile.
Cisco UCM Lines	This will move the line to the same site as the phone/device profile/RDP it is associated to.
Cisco Unity Connection Users	This will move the voicemail user to the same site as the base user.
Webex App Users	This will move existing Webex App users that are synced into Automate to the same site as the base user (if it finds a matching email address).
Contact Center Express Agents	This will move contact center express agents to the same site as the base user (if it finds a matching Cisco UCM user ID).

Overbuild workflow

provider-admin

reseller-admin

The table describes the general steps for overbuild:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Component	Description
1. Initial setup	Step 1 involves the initial setup and configuration on Automate; the provisioning of the business hierarchy. Identify the business information of the existing, deployed system, and add these details to Automate. This can be done manually, or via bulk load. • Create the hierarchy, with customers, sites, and site codes to generate the initial configuration data, such as site dial plan (Provider deployment only), and site defaults data. • Modify the data, if required, according to Cisco UCM data, so that overbuild processing can move the data to required sites. For example, the default, generated Automate Site Defaults for a site have the site name as the device pool name. Since the Site Defaults are used in the overbuild, this name should be modified to match the device pool name on the imported phones before the overbuild is run. Automate allows Provider and Reseller Administrators to modify Site Defaults update the configuration of an overbuild. While customers and sites have access to the Site Defaults under the **Site Management** menu, the **Overbuild Defaults** tab in Site Defaults is only visible to Provider and Reseller Administrators.
2. Create shell dial plan schema	Provider deployment only. Associate a shell schema group with the customer, then add a custom dial plan under *Advanced Configuration* (Optional at the site hierarchy). In this step, you will need to create a shell dial plan schema group at the Customer hierarchy. The shell schema group enables Partners, Resellers, and Provider Administrators to access customers that have existing or deployed dial plans without having to use the pre-packaged type 1-4 dial plans. The shell schema groups only contain two default values: • Device Pool • Cisco UCM Group The rest of the fields are blank for customization. This enables administrators to “over-build” Automate operations on top of customers’ existing dial plans. See “Provider HCS Dial Plan Management Support Guide”.
3. Configure network device connections	Identify and create network device connections, associate these with a Network Device List (NDL) and import. This includes Cisco UCM and CUCX clusters. This step involves provisioning Cisco UC applications, NDLs, and NDL references. Once the UC applications are configured, the sync from Cisco UCM is scheduled and executed. Caution: Whenever this data is synced in, it becomes managed by Automate and, as a result, would be deleted by any hierarchy delete. One Cisco UCM typically belongs to a customer and resides in a cluster, so this device import takes place at the created customer hierarchy. The device can also be associated with a NDL on Automate that is mapped to a created hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Component	Description
4. Choose device pools and devices	Choose the device pool and devices for the site on both the General tab and on the Overbuild Default tabs in the Site Defaults.
5. Run overbuild	Run the overbuild to move the imported UC applications data into the site hierarchy that corresponds with the existing deployed site. • Select **User** on **Run Overbuild** to move users exposed in **User Management** to the site of their associated phones (as specified in the Site Defaults Doc Device Pools). Users without phones are not moved and can be moved separately. Note that the user's role is not changed when moving to the site. The following model instances are moved from customer level to the site level: – `data/User` – `device/cucm/User` • If the **Lines** checkbox is selected on **Run Overbuild**, lines are moved to the relevant site, and marked as *in use* in the Directory Number (DN) inventory. If a matching DN inventory entry does not exist then one is created. DN entries are created at site by default unless the Create Internal Number Inventory at Customer option is selected (in Site Defaults > Overbuild Defaults tab). Note: Adding Directory Number inventory at Customer level is only possible if the dial plan is non-SLC, if no dial plan is in use. The **Run Overbuild** tool selects which data to move based on device pool configurations. You can run the tool for all sites, or a particular site. The existing system's provisioned phones that have been imported should have their device pools matched with Site Default data values on each specific site. Imported elements are moved according to overbuild Move workflows, which are triggered by the **Run Overbuild** tool. These workflows identify imported network device data and move it to the site hierarchy that corresponds to the existing deployed site.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Component	Description
6. Verify data	Use **Overbuild > Overview Tool** to verify the number of UC elements at the selected hierarchy and below. You can manually validate and modify the overbuild run by reviewing the moved items, using the Overview Tool. Use Device Models and/or Relations to move, update, delete, and in a few limited cases, add instances of device types for the selected hierarchy. Optionally, review the device model types listed with hierarchy in the Device Models or User Management menu.
7. Post-move	• Move any users who were not moved during the overbuild • Add your E.164 inventory (optional). See Add an Inventory of E164 Numbers in the Core Feature Guide. • Filter calling search spaces and assign a class of service (optional). See Filter Calling Search Spaces and Assign a Class of Service in the Core Feature Guide. • Perform Self-service authentication provisioning steps for non-LDAP, LDAP, and SSO-enabled scenarios. See User Authentication in the Core Feature Guide. • Add additional internal number inventory for future lines. See Number Management.

Run overbuild (Cisco)

Cisco

The Run Overbuild tool processes Cisco UCM imported objects for all sites in the current customer.

Run Overbuild must be run at the customer hierarchy. A device model is moved to a site on condition that there is a Network Device List Reference (NDLR) referencing the device at the site.

Note: The line goes to the first site that the Run Overbuild tool finds. The site selection is not deterministic.

The table lists the conditions for creating or updating the internal number inventory (INI) during overbuild:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Given	Then
• INI exists at site. • Site Defaults “Create Internal Number Inventory at Customer” checkbox is clear.	The lines in the INI at the site are updated to “Used”.
• INI exists at customer. • Site Defaults “Create Internal Number Inventory at Customer” checkbox is clear.	The lines in the INI at the customer are updated to “Used”.
• No INI exists. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear.	The INI is created at the site.
• INI exists at customer. • Site Defaults “Create Internal Number Inventory at Customer” checkbox is selected.	The lines in the INI at the Customer are updated to “Used”.
• INI exists at Site. • Site Defaults “Create Internal Number Inventory at Customer” checkbox is selected.	The lines in the INI at the Site are updated to “Used”.
• No INI exists. • Site Defaults “Create Internal Number Inventory at Customer” checkbox is selected.	The INI is created at the Customer.

Objects moved during the overbuild

The overbuild processes imported Cisco UCM objects for selected sites in the current customer. During overbuild, some objects are moved to the site hierarchy, while others remain at the customer hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Objects moved to the site during overbuild

The table describes objects moved to the site during the overbuild:

Object	Description
Cisco UCM models	device/cucm/Line device/cucm/Phone device/cucm/RemoteDestinationProfile device/cucm/RemoteDestination device/cucm/DeviceProfile device/cucm/User
Cisco Unity Connection models	device/cuc/User device/cuc/UserPassword device/cuc/UserPin device/cuc/AlternateExtension device/cuc/SmtpDevice device/cuc/SmsDevice device/cuc/PagerDevice device/cuc/PhoneDevice device/cuc/HtmlDevice device/cuc/CallHandler device/cuc/CallhandlerMenuEntry device/cuc/CallhandlerTransferOption device/cuc/Greeting device/cuc/MessageHandler
Voicemail-related models	device/cuc/User device/cuc/UserPassword device/cuc/UserPin device/cuc/AlternateExtension device/cuc/SmtpDevice device/cuc/SmsDevice device/cuc/PagerDevice device/cuc/PhoneDevice device/cuc/HtmlDevice
Self-care models	device/cuc/Callhandler. By default, one CallHandler entry is created when a Cisco Unity Connection user is created. device/cuc/CallhandlerMenuEntry

- Contact Center

  After the initial sync, agents will be located at the customer hierarchy level. The overbuild tool will attempt to move these agents to the correct site hierarchy levels, based on matching Cisco UCM users. This matching is done according to the Cisco UCM user ID and the agent user ID.

Contact Center models	device/uccx/Team device/uccx/Skill device/uccx/ResourceGroup device/uccx/Agent

Data models affected when the user is moved during overbuild:

Copyright © 2025 VisionOSS Limited. All rights reserved.

- data/User

Objects remaining at the customer during overbuild

The table describes objects that remain at the customer hierarchy during the overbuild:

Object	Description
Cisco UCM models	device/cucm/DevicePool device/cucm/Region device/cucm/Location device/cucm/VoiceMailPilot device/cucm/VoiceMailProfile device/cucm/Css device/cucm/RoutePartition device/cucm/HuntList device/cucm/HuntPilot device/cucm/LineGroup device/cucm/CallPickupGroup device/cucm/DirectedCallPark device/cucm/CallPark device/cucm/CtiRoutePoint
Cisco Unity Connection models	operator undeliverablemessagesmailbox
CallHandler device models	Goodbye Opening Greeting Operator operator undeliverablemessagesmailbox
Call Pickup Groups	no objects moved

Related topics

- *Move users*
- *Site defaults*
- *Run overbuild*
- *User authentication*
- *Number range management*
- *Bulk loading files*
- *Run overbuild*
- *Overview tool*
- *Device Models*
- Add an inventory of E164 numbers in the Core Feature Guide
- Filter calling search spaces and assign class of service in the Core Feature Guide

Copyright © 2025 VisionOSS Limited. All rights reserved.

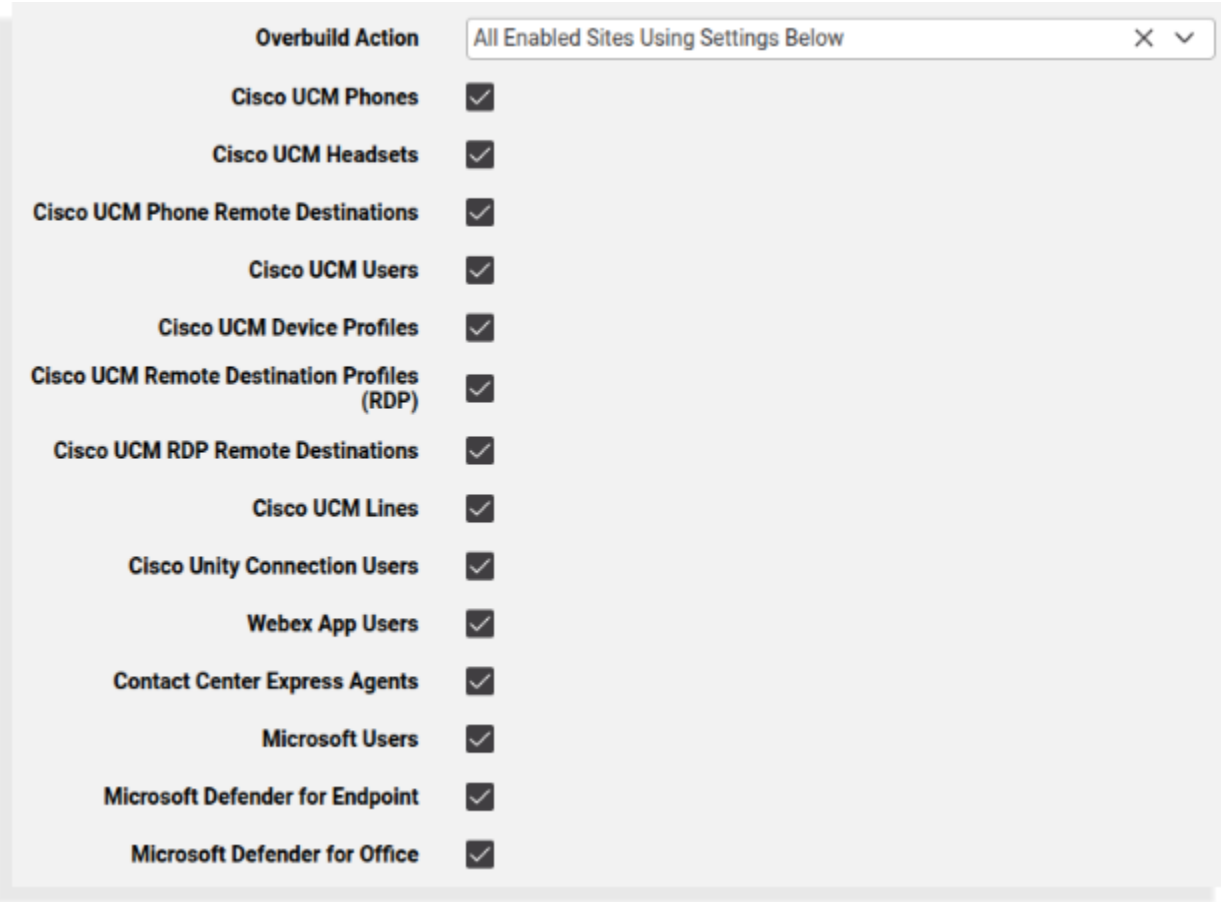
Run overbuild

Tip: *Use the Action search to navigate Automate*

Overview

The *Run Overbuild* tool imports objects.

Note: To access the Run Overbuild tool, go to **Run Overbuild**.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Overbuild action

The table describes options available for **Overbuild Action** on the **Run Overbuild** page

Overbuild action	Description
All Enabled Sites Using Settings Below	• Includes all devices selected on the form. • Includes all sites that have their site defaults doc configured to include the site in overbuild • An internal number inventory is created at customer level when Create Internal Number Inventory at Customer setting is selected, else, it's created at the site (if lines are included). • Device pools are from the General Defaults tab in the Site Defaults, and additional device pools are from the Overbuild Defaults tab. • The devices that display when **Limit Move Devices** is selected on the **Overbuild Defaults** tab are ignored. Runs Overbuild for all sites, and uses the devices selected on the **Run Overbuild** page. When Run Overbuild executes with this option, it applies to all sites and uses devices selected on the **Run Overbuild** page. Run Overbuild devices supersede the devices selected in **Limit Move Devices**.
All Enabled Sites Using Site Defaults Doc Overbuild Settings	• Hides and ignores selected devices on the Run Overbuild page. Moves all selected devices (when Limit Moved Devices is selected on the Overbuild Defaults tab in the Site Defaults) • Includes sites that are included for overbuild in their Site Defaults doc. • Creates internal number inventory at Customer level (when Create Internal Number Inventory at Customer option is chosen, else at site level (if lines is selected). • Device pools are from the General Defaults tab in the Site Defaults, and Additional Device Pools are used from the Overbuild Defaults tab in the Site Defaults.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Overbuild action	Description
Single Enabled Site Using Settings Below	• Overbuild is applied to the single site you choose. • The only sites available for selection are sites included for overbuild via their Site Defaults. • Includes all devices you choose on the page • Creates internal number inventory at Customer (if Create Internal Number Inventory at Customer option is selected); else, only at site (if Lines are included) • Device pools are from the General Defaults tab in the Site Defaults doc, and Additional Device Pools from the Overbuild Defaults tab. • Devices displayed when the Limit Move Devices option is selected on the Overbuild Defaults tab are ignored. Runs Overbuild for the selected site, and uses the devices selected on the **Run Overbuild** page. When the Run Overbuild tool executes with this option, it applies to the selected site only, and uses devices selected on the Run Overbuild page. Run Overbuild devices supersede the devices selected in **Limit Move Devices**.

Available device types

The available device types are shown in accordance with enabled services in Global settings (see: *Global settings*), for example:

- Cisco CUCM
- Cisco CUCX
- Cisco WebEx
- Cisco Webex App(Teams)
- Cisco UCCX
- Microsoft
- Defender for Office
- Defender for Endpoint

Available device types include:

- Phones
- Phone Remote Destinations
- Users (`device/cucm/User`)
- Device Profiles
- Remote Destination Profiles (RDP)
- RDP Remote Destinations

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Lines (a number inventory entry is also added for all `device/cucm/Line`) instances that are in the system at the customer or site level)
- CUC Users
- Webex App Users
- Pexip Users
- Contact Center Agents
- Microsoft Users
- Microsoft Defender for Endpoint
- Microsoft Defender for Office

Affected device models

The following device models are affected by the overbuild move:

- device/cuc/User
- device/cuc/UserPassword
- device/cuc/UserPin
- device/cuc/AlternateExtension
- device/cuc/ExternalServiceAccount
- device/cuc/SmtpDevice
- device/cuc/SmsDevice
- device/cuc/PagerDevice
- device/cuc/PhoneDevice
- device/cuc/HtmlDevice
- device/cuc/Callhandler
- device/cuc/CallhandlerMenuEntry
- device/cuc/CallhandlerTransferOption
- device/cuc/Greeting
- device/cuc/MessageHandler
- device/cucm/Phone
- device/cucm/User
- device/cucm/DeviceProfile
- device/cucm/RemoteDestinationProfile
- device/cucm/RemoteDestination
- device/cucm/Line
- device/pexip/Conference
- device/spark/User
- device/uccx/Team

Copyright © 2025 VisionOSS Limited. All rights reserved.

- device/uccx/Skill
- device/uccx/ResourceGroup
- device/uccx/Agent
- device/msexchangeonline/SafeAttachmentPolicy
- device/msexchangeonline/SafeLinksPolicy
- device/msexchangeonline/QuarantinePolicy
- device/mssecurity/Machine
- device/msgraphsecurity/Alert
- device/msgraphsecurity/Incident

Related topics

- Microsoft Defender for Office security management and policies in the Core Feature Guide
- Microsoft Defender for Endpoint security management and policies in the Core Feature Guide

Affected data models

The following data models are affected when moving a user during overbuild:

- `data/User`

Device types available for selection depend on the status of other device type check boxes. For example:

- The following device types are only available if you've selected **Phones**:
  - Dual-Mode Remote Destinations
  - Users
  - Lines
- The following device types are only available if you've selected **Users**:
  - Device Profiles
  - Remote Destination Profiles
  - CUC Users

Overbuild and failures

Overbuild workflows do not stop on any transaction failures and no transaction rollback takes place on errors. For example, device instance move operations to sites continue for all selected devices. Inspect the transaction log for errors.

In the Transaction log, sub-transactions of a successful overbuild workflow show their status as "Fail" if a model (such as a User) already exists. The sub-transaction logs also show details of the duplicate model and an "ignore error code" information message.

If a number already exists and the global setting *Prevent Duplicate Number* is enabled, the sub-transaction to create a duplicate of an existing number fails.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Related topics

- Prevent duplicate numbers in the Core Feature Guide

Overview tool

Tip: *Use the Action search to navigate Automate*

The overview tool validates your *run overbuild* process.

Overbuild users can use individual device models to ensure that the required Cisco UCM elements have been moved to the right hierarchy.

Note: To access this feature, go to **Overview Tool**.

You can use the *Overview Tool* at the customer or site hierarchy. The report shows the numbers of each Cisco UCM customer-specific data, for example phones, lines, users, etc., at the selected hierarchy and below. This is displayed in the format “current hierarchy/below.” For example, “390/20” means that 390 elements are at the current hierarchy and 20 elements are at hierarchies below the current hierarchy. Change the hierarchy to inspect the overbuild overview at that hierarchy.

When running the *Overview Tool* at site level, the number on the right will always show as 0, since site is the lowest Automate hierarchy level.

To verify the individual device models after running Overbuild, search for the model name for the device mode. The hierarchy where each device model instance exists will be listed in the far right column in the list view of the device model.

Run dial plan overbuild

provider

Cisco

Overview

The dial plan overbuild process moves specific dial plan elements, imported from Cisco UCM, to a specified site, based on the Automate location name and location ID.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Move dial plan elements to a site

Prerequisites

You must know the following Automate location details:

- Location name
- Location ID
- Location dial plan country code

1. Log in as a provider administrator or higher.
2. Enter the **Location Name**, **ID**, and **Dial Plan Country Code** to identify the location from which you want to move the elements.
3. From the **Destination Site Name** drop-down, choose the site to which you want to move the elements.
4. Click **Save**.

Dial plan elements moved to the site hierarchy

The table describes the dial plan elements moved when running a dial plan overbuild:

Model Type	Model Field	Condition	Filter Text
device/cucm/Region	name	endswith	phone-{{ input.v8_siteid }}
device/cucm/Region	name	startswith	{{ input.v8_sitename }}
device/cucm/Line	shareLineAppearanceCssName	endswith	CSS{{ input.v8_siteid }}
device/cucm/Line	shareLineAppearanceCssName	startswith	{{ input.v8_sitename }}
device/cucm/Location	name	endswith	-{{ input.v8_siteid }}
device/cucm/Location	name	startswith	{{ input.v8_sitename }}
device/cucm/DevicePool	name	endswith	pool{{ input.v8_siteid }}
device/cucm/DevicePool	name	startswith	{{ input.v8_sitename }}
device/cucm/DevicePool	regionName	endswith	-{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Calls{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	CallsCLIR{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	-{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Enh{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Std{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Rst{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Service{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Internal{{ input.v8_siteid }}

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

Model Type	Model Field	Condition	Filter Text
device/cucm/RoutePartition	name	endswith	Features{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	LclManagers{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	PT{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Site{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Plus{{ input.v8_siteid }}
device/cucm/RoutePartition	name	startswith	{{ input.v8_sitename }}
device/cucm/Css	name	endswith	CSS{{ input.v8_siteid }}
device/cucm/Css	name	endswith	LBO{{ input.v8_siteid }}
device/cucm/Css	name	startswith	{{ input.v8_sitename }}
device/cucm/CtiRoutePoint	callingSearchSpaceName	endswith	CSS{{ input.v8_siteid }}
device/cucm/CtiRoutePoint	devicePoolName	endswith	{{ input.v8_siteid }}
device/cucm/CtiRoutePoint	devicePoolName	startswith	{{ input.v8_sitename }}
device/cucm/VoiceMailProfile	voiceMailPilot.cssName	endswith	CSS{{ input.v8_siteid }}
device/cucm/VoiceMailPilot	cssName	endswith	CSS{{ input.v8_siteid }}
device/cucm/VoiceMailPilot	cssName	startswith	CSS{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	endswith	Feature{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/DirectedCallPark	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/DirectedCallPark	routePartitionName	endswith	Feature{{ input.v8_siteid }}
device/cucm/DirectedCallPark	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/CallPickupGroup	name	startswith	{{ input.v8_sitename }}
device/cucm/CallPickupGroup	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/CallPickupGroup	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/CallPickupGroup	routePartitionName	endswith	AllowCallFeatures{{ input.v8_siteid }}
device/cucm/HuntPilot	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	-{{ input.v8_siteid }}

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

Model Type	Model Field	Condition	Filter Text
device/cucm/TransPattern	routePartitionName	endswith	-{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Plus{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	isexactly	AllowEmerCalls{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	isexactly	AllowInternal{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Enh{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Std{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Rst{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	-PT{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/RoutePattern	routePartitionName	isexactly	SNRRRPT{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	isexactly	AllowVMCalls{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	endswith	EmerCalls{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	isexactly	AllowInternal{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	endswith	-PT{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/RouteList	name	endswith	-{{ input.v8_siteid }}
device/cucm/RouteGroup	name	endswith	-{{ input.v8_siteid }}
device/cucm/CallingPartyTransformationPattern	routePartitionName	endswith	PT{{ input.v8_siteid }}
device/cucm/CalledPartyTransformationPattern	routePartitionName	endswith	PT{{ input.v8_siteid }}
device/cucm/VoiceMailProfile	description	endswith	location{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	isexactly	AllowCallFeatures{{ input.v8_siteid }}
device/cucm/GatewaySccp Endpoints	callingSearchSpaceName	endswith	-CSS{{ input.v8_siteid }}

continues on next page

Copyright © 2025 VisionOSS Limited. All rights reserved.

Table 1 – continued from previous page

Model Type	Model Field	Condition	Filter Text
device/cucm/GatewayEndpointAnalogAccess	callingSearchSpaceName	endswith	-CSS{{ input.v8_siteid }}
device/cucm/H323Gateway	callingSearchSpaceName	endswith	-CSS{{ input.v8_siteid }}
device/cucm/MeetMe	routePartitionName	endswith	Site{{ input.v8_siteid }}

User phone associate tool

Tip: *Use the Action search to navigate Automate*

Overview

Cisco

Automate uses the associated or controlled devices value on the Cisco UCM user (user in Automate) to determine which phones are associated to that user.

The **User Phone Associate Tool** verifies that UCM phones in the system with the ownerID value set are correctly associated to the UCM user (user), for correct association in Automate.

For example, you may have phones synced in from an existing environment for overbuild, where the ownerID on the phones were set, but these were not associated from the UCM user perspective. In this case, check whether you can see the phones in the user view, but it appears they are owned by the user. In this scenario, you can run the **User Phone Associate Tool** to correct the association.

Note: When adding phones and users from *within* Automate, the phone-user relationship is bi-directional.

Run the user phone associate tool

Cisco

1. Navigate to the hierarchy of the UCM and choose it from the **UCM** drop-down list.

   The **Number of Phones that will be checked** value that is displayed is the number of phones on the UCM, at the hierarchy, that have been synced in to Automate and have an ownerID set, but cannot be found to be an associated device of any user at the hierarchy, or lower.

2. To run the **User Phone Associate Tool**, click **Save**.

   The tool searches in Automate for users that match the ownerID, and, if found, their associated devices will be updated with the phone.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Re-run the tool for the selected UCM. For any of the checked phones that were set as associated devices, the **Number of Phones that will be checked** value will decrease accordingly.

Note: If a user already has other associated devices, any new associated devices will be appended to the existing list.

Overbuild Analog Gateway

Overview

VOSS Automate offers management of analog gateways (FXS ports) using the SCCP and MGCP protocols. This feature also provides an overbuild capability.

VG2XX and VG3XX models are supported providing a range of port capacities from 2 – 160 ports. VG400 (8 ports max) and VG450 (144 ports max) models are also supported.

Using Overbuild Analog Gateway

This feature is initiated via the **Overbuild Analog Gateway** form (accessed via the default menu location **Overbuild > Overbuild Analog Gateway**).

The only required attribute is the **CUCM IP Address**, which is selected from a drop-down list. When executing the overbuild, all MGCP and SCCP gateways are discovered.

For each gateway not already at site level, a new IOS device is created, and the gateway and ports are moved to the site level based upon the device pool found on the first port. The gateway can then be managed in the normal way.

Note: Since the device pool associated with the first gateway port is used to identify the location of the gateway, a gateway with no configured ports cannot be moved.

Device Models

Cisco

From the Overbuild's **Device Models** menu, you can view details about the devices, by model, in the selected hierarchy. Like the **Overview Tool**, this can be useful to indicate where devices have moved as a result of an overbuild.

When choosing a device model type from this menu, the list view displays data about the devices of that model type in the hierarchy, such as:

- Device names or identifiers
- Their device pools
- Their hierarchies at and below the currently selected hierarchy
- Data related specifically to the selected device model

Copyright © 2025 VisionOSS Limited. All rights reserved.

In a device model you can select individual devices to modify, delete, and export them. You can also bulk change settings for all the devices in a device model by selecting the **Select All** checkbox at the top of the table in the list view, then choose **Action > Bulk Modify**.

> **Caution:** It is strongly recommended that you do NOT directly edit the device models via this menu. Instead, use other menus in Automate, such as the Subscriber Day 2 menus. The **Device Models** menu items should be used for manually moving device models that the **Overbuild Tool** can't move or that need additional manual moves after **Run Overbuild** is executed.

For CUC models, two system users (`operator` and `undeliverablemessagesmailbox`) remain at the Customer level. All associated CUC device models for the two system users will remain at the Customer hierarchy and will show in the device model counts and device model lists at the Customer hierarchy.

For call handler device models, there are 5 default instances that remain at the Customer hierarchy:

- Goodbye (a CUC system default call handler)
- Opening Greeting (a CUC system default call handler)
- Operator (a CUC system default call handler)
- operator (the system user 'operator' call handler)
- `undeliverablemessagesmailbox` (the system user `undeliverablemessagesmailbox` call handler)

These 5 call handlers remain at the Customer hierarchy and appear in the device model count and device model lists for call handlers at the Customer hierarchy.

These device models also allow you to add device instances. However, it is not recommended to add device instances in the **Overbuild** menu.

- CUCM CtiRoutePoint
- CUCM DirectedCallPark
- CUCM Phone
- WebEx User

Locate a user associated with a CUC device model

Cisco

Tip: *Use the Action search to navigate Automate*

The CUC device models use internal UUID references to the CUC user objects. As a result, most CUC device models do not have a field showing the ID of the user associated with the device model. You can use Search in Automate to find the associated user information.

1. Go to **Device Models**.
2. Click the desired CUC device model in the menu, then view the list of CUC device models that display.
3. Click the relevant device model instance.
4. In the CUC device model output, find the field Subscriber Object ID.
5. Search for the following string in the Automate Admin Portal. See *Search in Automate*

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
device/cuc/User WITH object_id like 9b16c8ce-edd9-43c4-9262-c25296d3560b
```

where 9b16c8ce-edd9-43c4-9262-c25296d3560b would be replaced with the output of the Subscriber Object ID.

The equivalent Automate API request would be:

```
https://<host-or-proxy>/api/tool/Search/?
format=json&
device%2Fcuc%2FUser%20
 with%20object_id%20like%20
  9b16c8ce-edd9-43c4-9262-c25296d3560b
```

Filter calling search spaces and assign a class of service

Cisco

provider

Tip: *Use the Action search to navigate Automate*

This procedure filters calling search spaces (CSS) so that drop-down lists contain only the CSSs that are relevant to the selected devices and lines. Additionally, you can flag a CSS as a class of service (CoS).

Note: For the overbuild, Automate does not filter the Calling Search Space (CSS) fields that are used for various lines and devices in the user interface.

1. Enable CSS filtering.
   a. Log in to Automate as provider, reseller or customer administrator.
   b. Choose the customer hierarchy.
   c. Go to the **Dial Plan** page.
   d. Click the dial plan.
   e. Select the **Enable CSS Filtering** check box.
   f. Click **Save**.
2. Move CSSs from the customer hierarchy to the site hierarchy.
   a. While still at the customer hierarchy, Go to **CUCM CSS**.
   b. Select the check box to the left of each CSS that you want to move.
   c. Click **Action > Move**.
   d. From the **Move Resources to Hierarchy** drop-down, choose the site to which you want to move the CSS.
   e. Click **OK**.
   f. Repeat steps b through e if you want to move more CSSs.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Identify the CSSs that you want to appear in the filtered drop-down lists for the devices, services, and lines.
   a. Choose the site hierarchy.
   b. Go to **Class of Service**.
   c. Click **Add**.
   d. From the **Class of Service Name** drop-down, choose the CoS that you want to associate with the CSS.
   e. Click **Save**.
   f. Repeat steps b through e for each CoS that you want to associate with a CSS.
4. Verify that the CSS field is filtered correctly.
   a. While still at the site hierarchy, go to the **Lines** page.
   b. Click **Add**.
   c. From the **Calling Search Space** drop-down, verify that the items in the list are the CSSs that you flagged as CoS.
5. (Optional) Remove the CoS flag from a CSS.
   a. Log in to Automate as provider, reseller or customer administrator.
   b. Choose the site hierarchy.
   c. Go to **Class of Service**.
   d. Click the required Class of Service Name.
   e. Click **Action > Exclude from CoS**.

   Note:

   Ensure that you exclude the CSS from the CoS when you want to remove the CoS flag. If you delete the CoS instead, the CSS is deleted from CUCM.

Microsoft Overbuild

Overbuild for Microsoft

Tip: *Use the Action search to navigate Automate*

Automate provides an overbuild tool for each of:

- *Automate with Microsoft enabled (not Microsoft Defender)*
- *Overbuild with Microsoft Defender - by Model Filter Criteria*

Copyright © 2025 VisionOSS Limited. All rights reserved.

Automate with Microsoft enabled (not Microsoft Defender)

Overview

The Overbuild feature enables Provider and Reseller administrators to integrate existing, deployed Microsoft tenants into Automate without re-provisioning, unless required.

Important: It is recommended that Automate training and/or VOSS Services are engaged during the initial use of the feature to help ensure optimized processes and guidance.

In Automate, a Microsoft tenant shows the combined and specific details of a MS Office 365 and MS Teams tenant.

Overbuild provides tools to help the administrator manage Microsoft Tenant data synced from existing configurations.

While a Microsoft Tenant does not contain such Automate components as a hierarchy or a user, the relationship with Microsoft tenant components makes it possible to, for example, create an Automate user at a site hierarchy during the Overbuild process. The necessary filters can be set up and workflows, macros, and brownfield move processes are available for this purpose.

After overbuild is run for the first time, a schedule is created in Automate that can be set up to run at a selected interval.

Overbuild logic for handling users:

- Microsoft Users

  The synced in Microsoft tenant user is moved to the site, based on the MS 365 model filter criteria selected for the site in the site overbuild defaults. To allow this, ensure you select **Include Site for Overbuild** and **Microsoft Users** (on the **Overbuild Defaults** tab in the site defaults).

  To view the number of Microsoft users at the hierarchy level (MS 365 users, MS Teams users, and MS Exchange users), go to **Overbuild > Overview Tool**. A Microsoft tenant user can be set up with services using Quick User.

Note: Microsoft Guest users (Msol users external to the tenant) are synced in, but their group details (information about which groups they're associated with) won't be included in the sync.

Related topics

- *Microsoft Quick User*

Configure overbuild site defaults for Microsoft Users

Pre-requisite:

- *Sync to customer, then to site*

Note:

- Ensure the NDLs are configured for the overbuild by adding tenant details, including MS Exchange details if you wish to move mailboxes to the site in the overbuild.

Copyright © 2025 VisionOSS Limited. All rights reserved.

- All Microsoft elements must be moved to customer level in a sync before running the overbuild, which moves these elements to the sites.

To configure a site for overbuild:

1. In the Automate Admin Portal, go to **Site Defaults**.

Note: Alternatively, go to **Defaults** and select the **Overbuild Defaults** tab. You can also fill out the search term, *Site Defaults*, in the Automate Admin Portal **Search** field to locate **Site Defaults**.

2. In the **Site Defaults** list view, click on a site to open its site default settings.
3. On the **Overbuild Defaults** tab, configure the following:
   - Enable **Include Site for Overbuild**
   - At **Overbuild Device Control**, choose **Limit Moved Devices**.
   - Select **Microsoft Users** to enable Microsoft users.
4. For **Microsoft Users**, on the **Move Filter Criteria** tab, configure the following:
   - At **MS 365 User Model Filter Criteria**, select the relevant filter.

     Note: For more information about filters, see *Model filter criteria*.

   - If required, select **Move by Number**.

     Note: User data is moved to a site using **Move by Number** only if the synced in Microsoft Teams user's LineURI matches a pre-loaded internal number at that site.

     If you've selected a filter for **MS 365 Model Filter Criteria** and you've enabled **Move by Number**, the overbuild first processes **MS 365 Model Filter Criteria**, and then processes **Move by Number**.

     For more information about options on the **Move Filter Criteria** tab, see *Site defaults* in the Core Feature Guide.

Related topics

- Site defaults in the Core Feature Guide
- *Model filter criteria*

Run overbuild

1. In the Automate Admin Portal, go to **Run Overbuild**.
2. Choose the site.
3. In a Microsoft-only environment without MS Defender, select only **Microsoft Users** to include in the overbuild.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: This allows Microsoft users to move to the site. Automate looks at the MS user, and checks whether it has MS Teams and MS Exchange, and moves these elements to the sites along with the user.

4. Save your changes to run the overbuild.

Note: For *Microsoft Users**, the overbuild moves assigned numbers to the number inventory, flagged with the user's name, location (customer or site), number status (**Used** when assigned, else, **Available**), and the relevant vendor (Microsoft, in this case).

The number management step occurs on sync, overbuild, as well as in a number audit. You can run a number audit anytime to verify that numbers are correctly flagged as used or available (via **Number Management > Audit Number Inventory**) - see *Number inventory audit*.

Related topics

- Sync Microsoft users to sites in the Core Feature Guide
- Model Filter Criteria in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide
- *Number inventory audit*

Overbuild with Microsoft Defender - by Model Filter Criteria

Overview

The Overbuild by Model Filter Criteria feature makes it possible to move resources across hierarchies in accordance with defined Model Filter Criteria (MFC) instances where the MFC **Usage** is set to **Overbuild**. See: *Model filter criteria*.

Microsoft Defender overbuild options:

- Microsoft Defender for Endpoint

  This will move Microsoft Defender for Endpoint device data and alerts down to lower hierarchy levels using Model Filter using Model Filter Criteria.

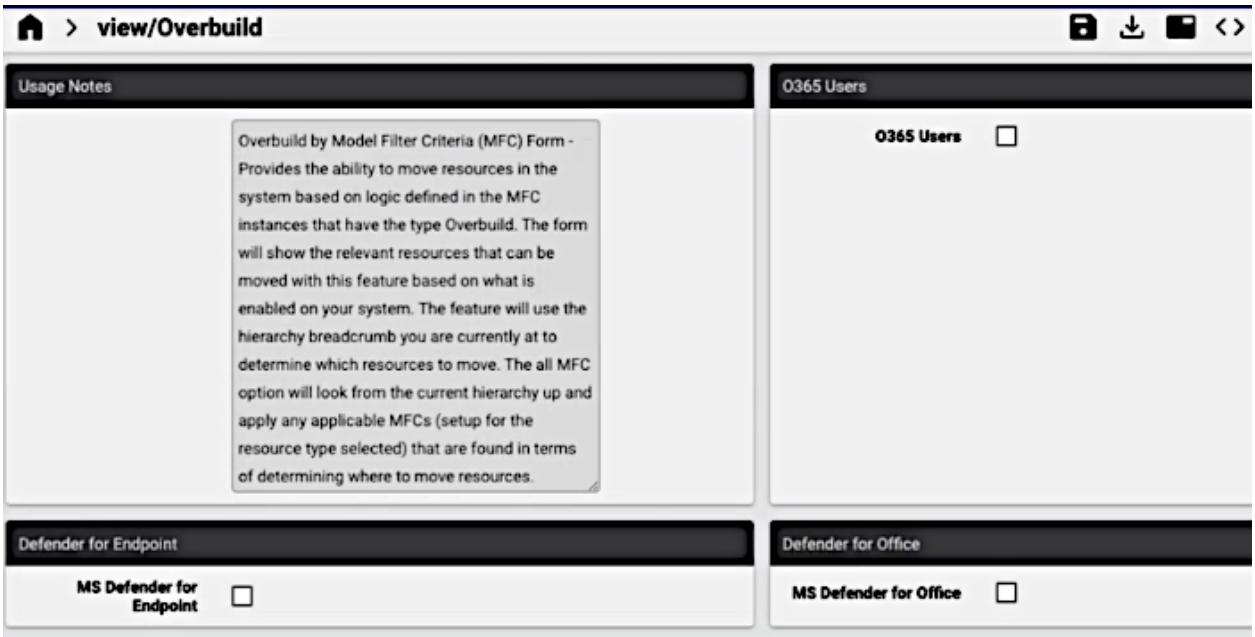
- Microsoft Defender for Office

  This will move Microsoft Defender for Office attachments, links and quarantine policies for Office down to lower hierarchy levels using Model Filter Criteria.

The feature presents a form showing available overbuild options based on the global settings enabled on your system - see: *Global settings*.

For example, in the image below, **Enable Defender for Office** and **Enable Defender for Endpoint** are available, since these are enabled.

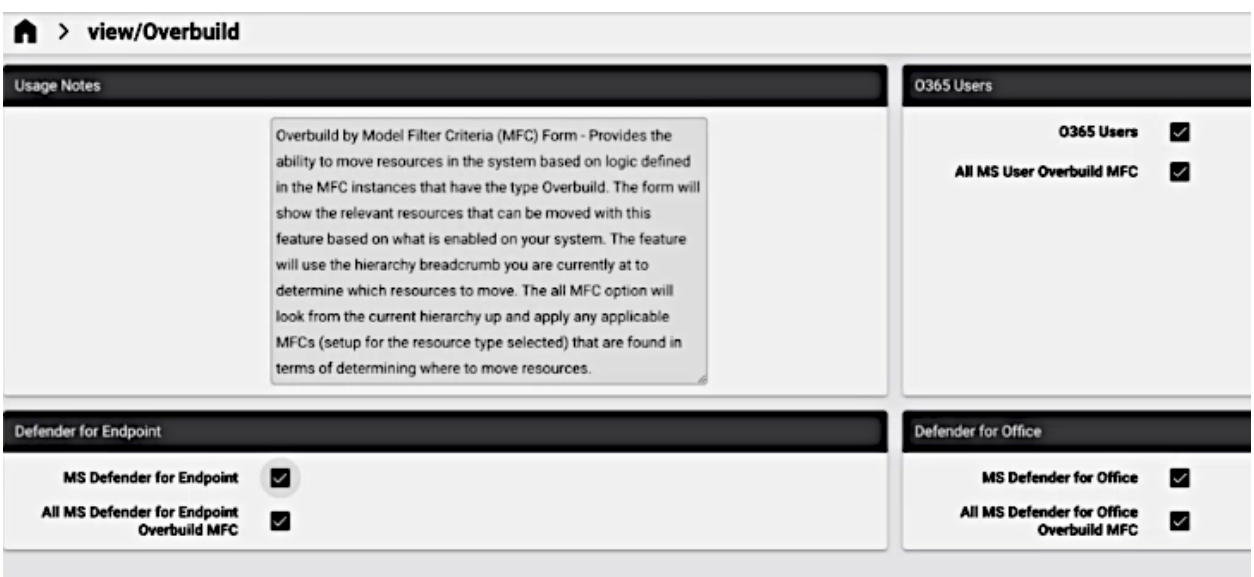
Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: If on *Global settings*, the **Enabled Solutions** setting **Enable Voice Automation Solution** is enabled, Overbuild by Model Filter Criteria will skip the move of `device/msgraph/MsolUser` and that this data will be moved by standard settings - as implied by the setting.

Option selection

Upon selecting the initial overbuild option available according to your global settings, an *all* and *specific* choice will then be available for the option. By default, the *all* option is enabled. If this option is deselected (un-tick checkbox), the *specific* options are shown.



- When selecting the *all* MFC option, the current hierarchy upwards (up to Provider level) is be checked for relevant MFCs that have been set up for the selected option. The listed instances are MFC instances

Copyright © 2025 VisionOSS Limited. All rights reserved.

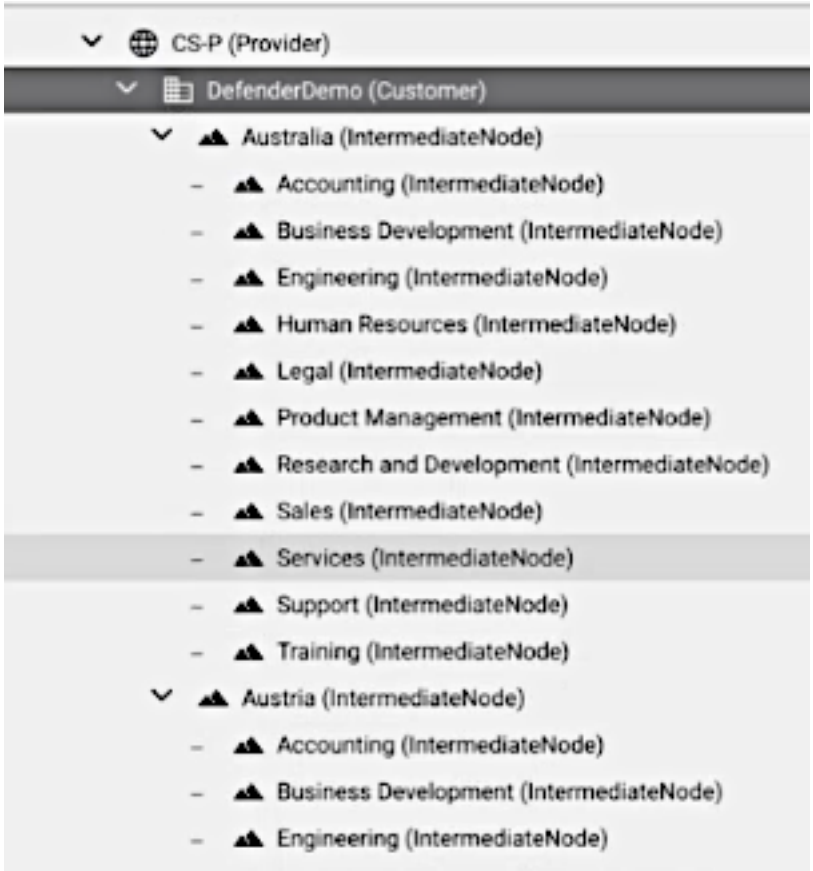
where **Automated Overbuild** setting has been enabled.

- When selecting an option to specify *specific* MFC instances, the form displays *all* the MFC resources up to the `sys` hierarchy - *including* instances where the **Automated Overbuild** setting has been disabled - in an **Available** list of a transfer box that can then be selected by moving these to the **Selected** list. The inclusion of instances with **Automated Overbuild** disabled here allows you to run selected MFCs without running them automatically by accident.

Note:

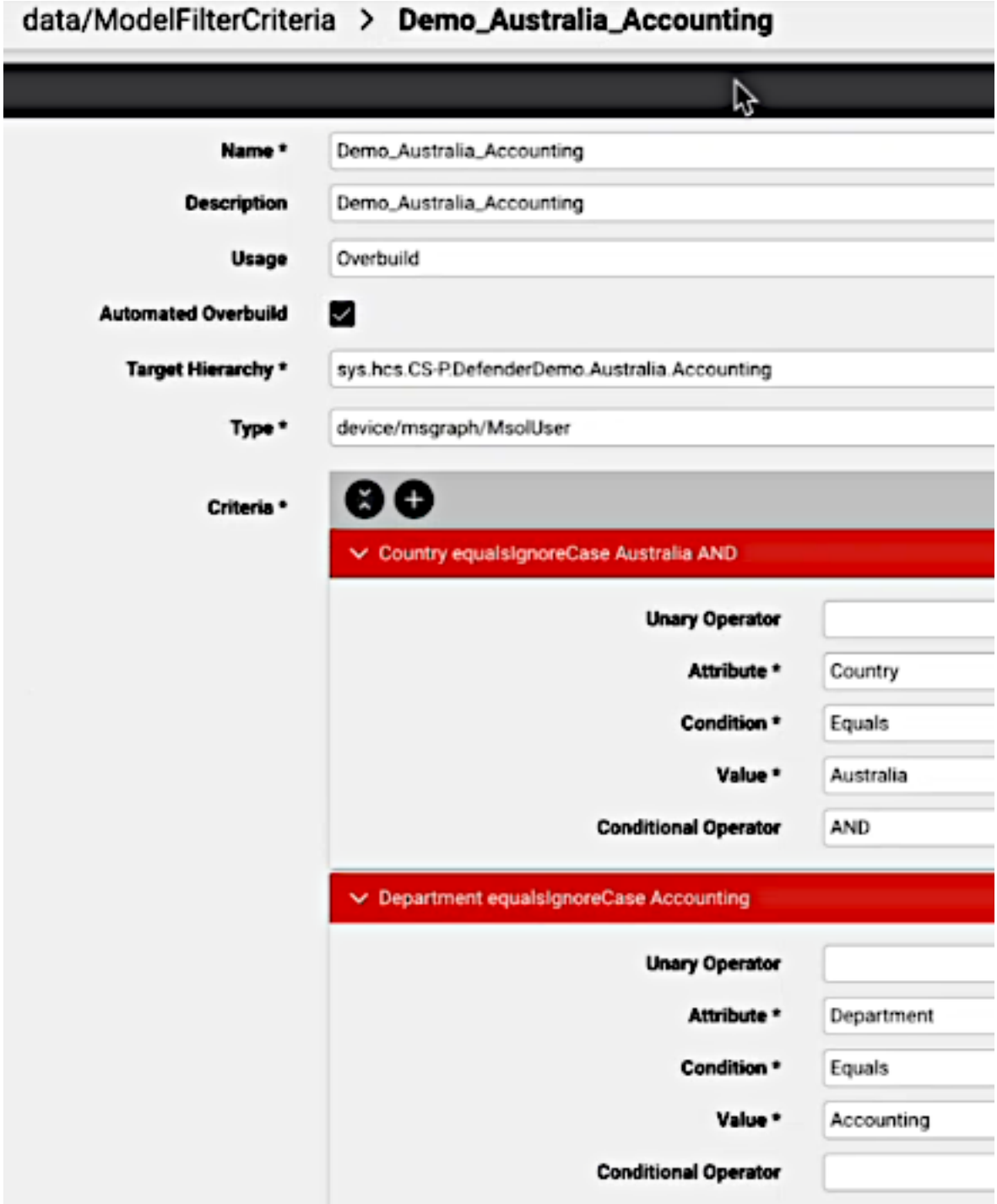
- The current hierarchy where the feature is used determines which resources specified in the MFC to move to the **Target Hierarchy** as specified in the MFC. This target hierarchy is thus not only limited to sites, but can be any created intermediate nodes representing an organizational structure.

  Example hierarchies:



  Example MFC:

Copyright © 2025 VisionOSS Limited. All rights reserved.



- When specific MFCs are selected, the overbuild move sequence will be carried out according to the MFC order in the **Selected** list (top-down).

The following list shows overbuild options (not all may be enabled in your settings) and the conditions of their selection or de-selection:

- **O365 Users**: checkbox. If checked, then either:
  - **All MS User Overbuild MFC**: checkbox (enabled by default)

Copyright © 2025 VisionOSS Limited. All rights reserved.

or disabled, then:

  - **Specific MS User MFC**: transfer box

- **MS Defender for Endpoint**: checkbox. If checked, then either:
  - **All MS Defender for Endpoint Overbuild MFC**: checkbox (enabled by default)

  or disabled, then:
  - **Specific Defender for Endpoint Machine MFC**: transfer box
- **MS Defender for Office**: checkbox. If checked, then either:
  - **All MS Defender for Office Overbuild MFC**: checkbox (enabled by default)

  or disabled, then:
  - **Specific Defender for Office Quarantine Policy MFC**: transfer box
  - **Specific Defender for Office Safe Links Policy MFC**: transfer box
  - **Specific Defender for Office Safe Attachment Policy MFC**: transfer box

  An example of option selection is show in the image below:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Microsoft Defender models and move rules

The items below indicate which Microsoft Defender models are moved and by what rules they are moved during overbuild.

Type models move via Model Filter Criteria (MFC) for the policy where **Usage** is **Overbuild** to **Target Hierarchy** according to **Criteria**. See: *Model filter criteria*.

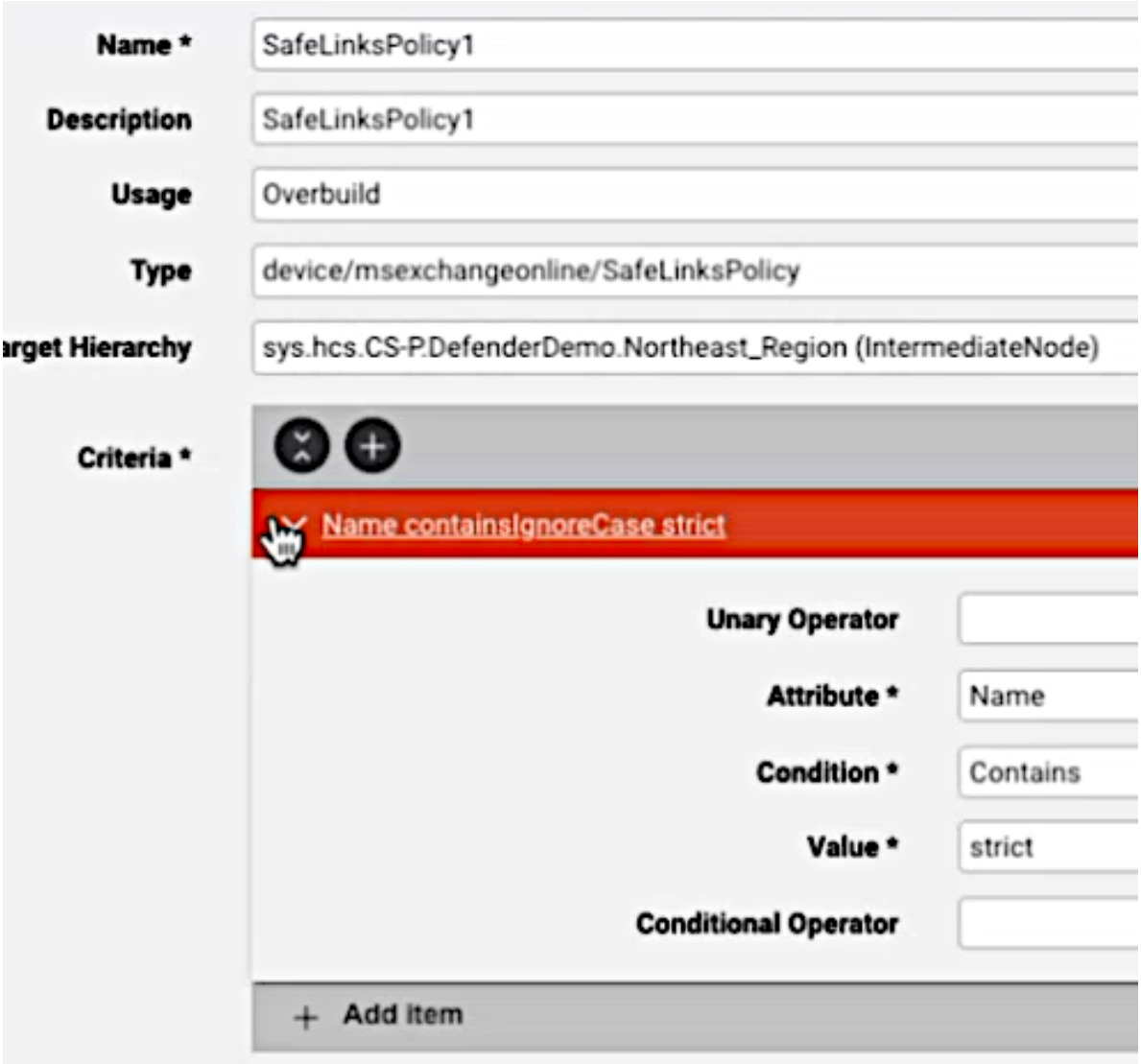
- Office

  If Microsoft Defender for Office is enabled as a service in global settings and the tenant configuration has synced collection data to the tenant hierarchy, overbuild moves attachments, links and quarantine policies according to the specified criteria for the **Type**:

  - `device/msexchangeonline/SafeAttachmentPolicy`: move according to Model Filter Criteria
  - `device/msexchangeonline/SafeLinksPolicy`: move according to Model Filter Criteria
  - `device/msexchangeonline/QuarantinePolicy`: move according to Model Filter Criteria
  - `device/msexchangeonline/QuarantineMessage`: move to the first recipient address on each instance if the `MsolUser` is at a lower hierarchy.

  Example MFC instance:

Copyright © 2025 VisionOSS Limited. All rights reserved.



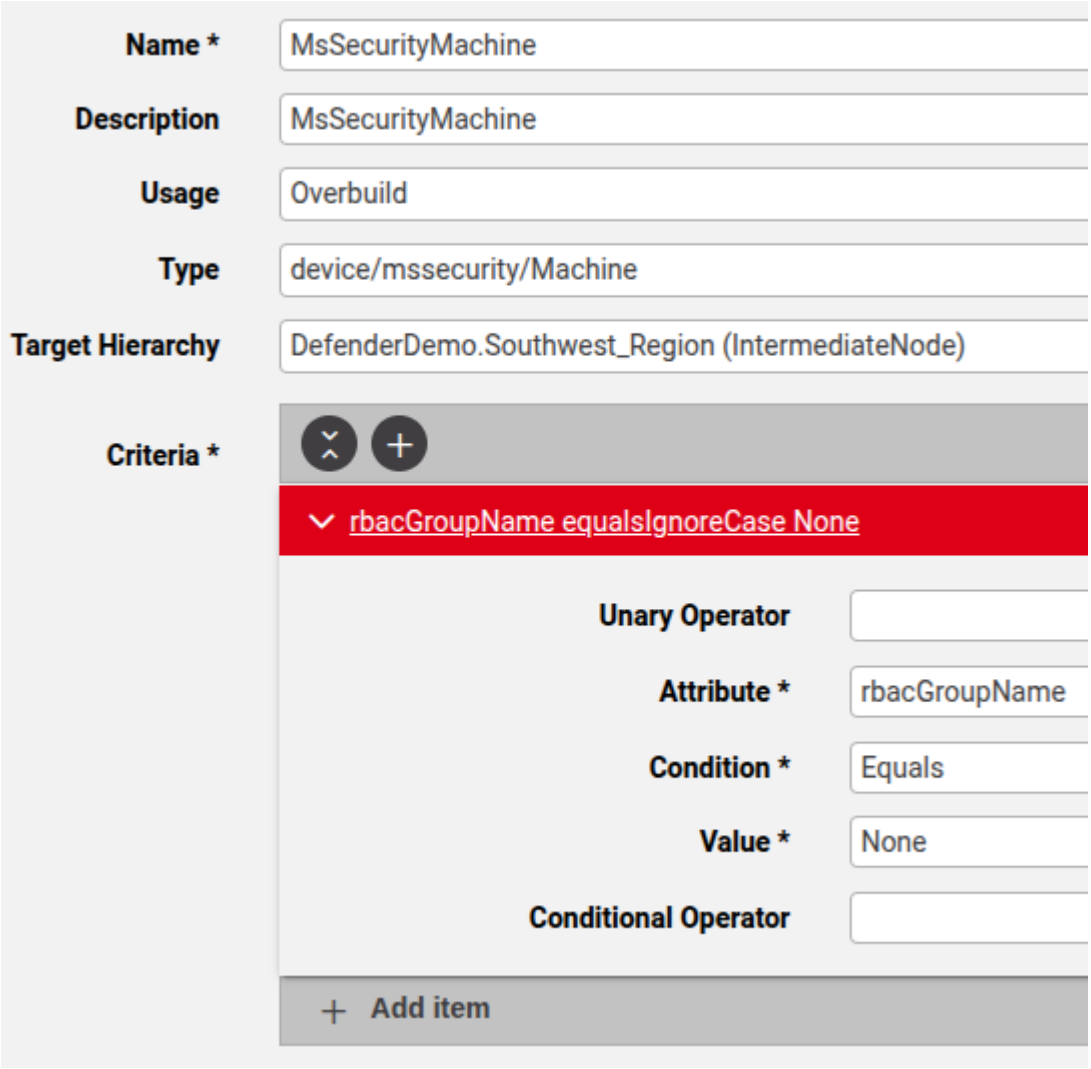
- Endpoint

  If Microsoft Defender for Endpoint is enabled as a service in global settings and the tenant configuration has synced collection data to the tenant hierarchy, overbuild moves attachments, links and quarantine policies according to the specified criteria for the **Type**:

  - `device/mssecurity/Machine`: move according to Model Filter Criteria instances that are set up.
  - `device/msgraphsecurity/Alert`: move Alert models based on hierarchy level of related Machine models at a lower hierarchy, since all the alerts follow a machine.
  - `device/msgraphsecurity/Incident`: move Incident models based on hierarchy level of related Alert models that are at a lower hierarchy, based on the incident IDs in the alert of the first matching alert. (Alert ID is referenced)

  Example MFC instance:

Copyright © 2025 VisionOSS Limited. All rights reserved.



Related topics

- *Model filter criteria*

13.2.4. Files and Logs

Create Model Report

Tip: *Use the Action search to navigate Automate*

System admins and and advanced admins can create and display reports on the data under a selected site hierarchy. The purpose of such a report is to show the model types: device and data models at a site as well as the number of instances of each model type.

You can create, list, view, and delete reports for a hierarchy.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Note: The relation data type is not displayed, but component data models are reported on.

1. Log in as system administrator.
2. Navigate to the hierarchy for which the report is to be created.
3. Go to **Create Model Report**
4. Verify that the hierarchy level value is the required hierarchy.
5. Choose the model types to be reported on:
   - DATA Models
   - CUCM Models
   - CUC Models
   - LDAP Models
6. Click **Save** to create the report.

   The time stamp of the report at the hierarchy is recorded. To see the progress of the report creation, go to **Model Reports** and from the list of reports, either inspect the value in the **Status** column or choose the report to see the status. The report is available when the status is **Done**.

Manage Model Reports

Reports can be viewed and deleted.

1. Log in as system administrator.
2. Choose **Advanced Tools > Model Report > Model Reports**
3. To view a report, click the report to view. Details for each model type are displayed on a tab.
4. The **Detail** tab shows:
   - the type of report
   - date of creation
   - hierarchy of the report

   The model tabs show Count value for each model type, if these were selected. If a model type has no instances, in other words a zero count, this is not shown.
5. To delete a report, choose the report and click **Delete**.

Create Line Reports for a Site

This procedure creates a report of all lines configured at a site.

Note: You can use the report information to determine which lines you must move before deleting the site.

The report shows:

- The hierarchy node of the line's corresponding DN inventory
- Whether the line is shared within the site
- A list of all the phones that reference the line

Copyright © 2025 VisionOSS Limited. All rights reserved.

- The owner and hierarchy node of each phone that references the line

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer for which you want to create a site line report.
3. Choose **Administration Tools > Reports > Create Line Report**.
4. From the **Site Hierarchy** drop-down, choose the site for which you want to create the line report.
5. Click **Save**.

A line report for each line in the selected site is generated.

Next Steps

View line reports.

View Line Reports

This procedure displays the line reports.

Perform the following steps:

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer for which you want to view line reports.
3. Choose **Administration Tools > Reports > Line Reports**.

   A list of line reports is displayed containing this information:

Column	Description
Pattern	Directory Number of the line.
Partition	The route partition of the line. The pattern combined with the partition defines the uniqueness of the line in CUCM.
Line Hierarchy	Hierarchy where the CUCM line with this pattern and partition is defined.
DN Inventory Hierarchy	Hierarchy where the DN inventory for the pattern is defined. If empty, no DN inventory exists for this pattern.
Device Count	Number of Phones, Device Profiles, and Remote Destination Profiles remote across all sites that are referencing this line.
Used Across Sites	Indicates whether at least one phone which exists in a different site references this line.
Shared Within Site	Indicates whether this line is shared between multiple phones within the site where the line exists.
Timestamp	Time when the report was generated.
Hierarchy	Hierarchy of the customer for which the report was generated.

4. To see additional information about Phones, Device Profiles, and Remote Destination Profiles related to a line, click the required line report. The **Line Reports** screen displays this information about Phones, Device Profiles, and Remote Destination Profiles:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Phones

Column	Description
End User	The user ID of the CUCM user who owns this phone.
Phone Name	Device name of the phone which references the line.
Hierarchy	Hierarchy where the phone exists which references the line.

Device Profiles

Column	Description
End User	The user ID of the CUCM user who owns this Device Profile.
Device Profile Name	Name of the Device Profile which references the line.
Hierarchy	Hierarchy where the Device Profile exists which references the line.

Remote Destination Profiles

Column	Description
End User	The user ID of the CUCM user who owns this Remote Destination Profile.
Remote Destination Profile Name	Name of the Remote Destination Profile which references the line.
Hierarchy	Hierarchy where the Remote Destination Profile exists which references the line.

Next Steps

To avoid letting too many line reports accumulate, delete them individually or select the check boxes on the **Line Reports** list view and click **Delete** to delete multiple reports.

Template customization audit tool

Overview

You can run the template customization audit tool on a selected hierarchy node to identify template definitions and instances that were not delivered in the standard template packages during an installation or upgrade.

The audit report includes custom model schema definitions as well as data, domain, and view instances created on the hierarchy node as a result of workflow execution.

Use the report to verify that there are no unexpected instances at the specified hierarchy node.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Run the template customization audit tool

1. Log in as a customer administrator or higher.
2. Set the hierarchy path to the level from which you want to run your audit.

   From a given hierarchy node, you can audit customized templates at the node, and at nodes directly above or below the node in the hierarchy tree.
3. Choose **Administration Tools > Reports > Audit Template Customization**.
4. Choose the hierarchy node for which you want to audit customized templates.
5. Click **Save**.

Next steps

View the audit report. See “View Template Customization Audit Reports”.

View template customization audit reports

1. Log in as provider, reseller, customer, or higher level administrator.
2. Choose **Administration Tools > Reports > Template Customization Reports**. A list of template customization audit reports is displayed.
3. Click a report to view the details. The message field shows how many customized templates were found at the hierarchy node. The details fields lists the model type and instance of each customized template.

Example template customization audit reports

The purpose of a Template Customization Audit Reports is to provide a record of changes as a result of workflow execution at a particular hierarchy, in particular:

- data, relation, and view instances of standard models that include for example Configuration Templates, Field Display Policies, Macros.
- custom model schema definitions that may have been created at the site (for example, instances of `data/DataModel`) as a result of a custom adaptation.

Consider an example customization report that was created at a Site hierarchy called: `LOC001`.

After the report is created from the **Administration Tools > Reports > Audit Template Customization** menu, it shows as an item in the list of reports on the **Administration Tools > Reports > Template Customization Reports** menu.

The report can be identified by checking the creation Timestamp and Message columns of the list. The message would contain the number of templates and the phrase that shows the Site hierarchy, for example:

```
544 customized templates were found at sys.hcs.CS-P.CS-NB.AAAGlobal.LOC001
```

The Details list in the report shows entries of the format:

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
Model Type: data/User, \
Instance: bkey(["QAS0003", "hcs.CS-P.CS-NB.AAAGlobal.LOC001"]), \
pkid(5949dd115da9aa9559aa2386)

Model Type: data/ConfigurationTemplate, \
Instance: bkey(["Reference CUCM User Template", \
                "device/cucm/User", \
                "hcs.CS-P.CS-NB.AAAGlobal.LOC001"]), \
pkid(5949dcd15da9aa9559aa1b2d)

Model Type: data/Macro, \
Instance: bkey(["CUSTOMER_INI_ENABLED", \
                "hcs.CS-P.CS-NB.AAAGlobal.LOC001"]), \
 pkid(5949db2a5da9aa9559aa01d9)
```

From the list details, it is possible to see the model instances created at the site - defined by type, business key and pkid.

This provides administrators with information when inspecting data at a hierarchy for troubleshooting or for reference when contacting support operators.

13.2.5. System Settings

Settings

sys-admin

Tip: *Use the Action search to navigate Automate*

Overview

sys-admin

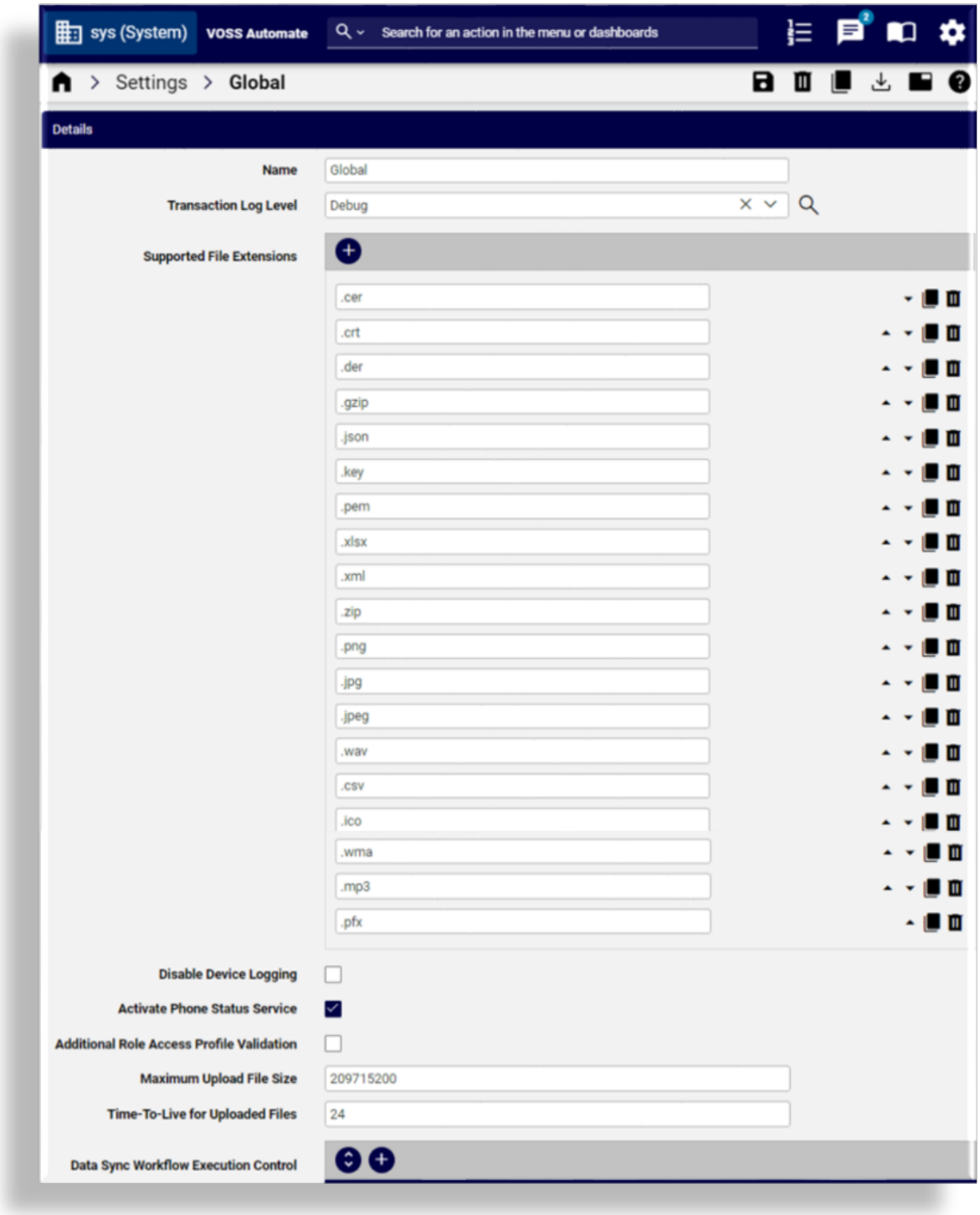
This topic describes the system level settings configurable via the **Settings** page, where a `sysadmin` user with access to the `data/Settings` model can view and modify the following global system level settings for Automate:

- Configure transaction log levels (See *Configure transaction log levels*)
- Add or remove supported file extensions (See *Supported file extensions*)
- Enable or disable system user audit (See System User Audit in the Core Feature Guide)
- Enable or disable device logging (See *Disable device logging*)
- Enable or disable the phone status active service (the service to periodically fetch Call Manager phone status). See *Activate phone status service*
- Enable or disable role access profile validation (See *Additional role access profile validation*)
- Specifying the maximum file upload size (See *File upload limitations*)

Copyright © 2025 VisionOSS Limited. All rights reserved.

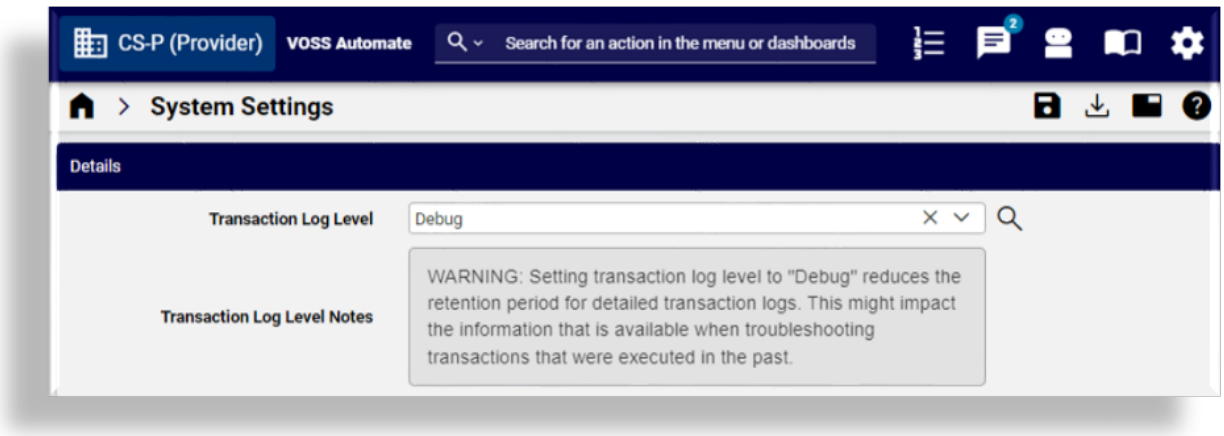
- Specify the time to live for uploaded files, in hours (See *Time-to-live for uploaded files*)
- Configure controls for data sync workflows on certain models via allowlist and denylist attributes (See *Data sync workflow execution control*)
- Configure device overwrite check exemptions on certain models via attributes (See *Device overwrite check exemptions*)
- Enable or disable Wingman at the system level (the Automate chat co-pilot)
- Choose when tooltips display (for accessibility)

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note: Provider admins and admins at `hcsadmin` have access to the **System Settings** page (`view/DataSettings`) for managing transaction log levels only, and is a limited version of `data/Settings`.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Configure transaction log levels

System transaction log levels refer to the configured verbosity level of the transaction logs in Automate. Available transaction log levels for Automate are as follows:

- Debug
- Verbose
- Info (default)
- Warning
- Error
- Disabled

Note: See *Transaction log levels* for details.

The following Automate admin users can view and modify transaction log levels in Automate:

- Provider admins and `hcsadmin` admins with access to the `view/DataSettings` model
- High level admins (`sysadmin`) with access to the `data/Settings` model

Supported file extensions

Users with system administrator privileges to the `data/Settings` model, typically, `sysadmin`, can manage valid file extensions in Automate.

By default, the following file extensions are specified as supported in the Global instance of `data/Settings`, which means that files with these extensions can be uploaded to Automate.

- `.cer`
- `.crt`
- `.der`
- `.gzip`

Copyright © 2025 VisionOSS Limited. All rights reserved.

- `.json`
- `.key`
- `.pem`
- `.xlsx`
- `.xml`
- `.zip`
- `.png`
- `.jpg`
- `.jpeg`
- `.wav`
- `.csv`
- `.ico`

The `sysadmin` user can add or remove file extensions. Unsupported files can't be uploaded or imported, and will trigger a system error.

Disable device logging

Users with system administrator privileges to the `data/Settings` model, typically, `sysadmin`, can enable or disable device logging.

When setting **Disable Device Logging** to enabled (on the **Settings** page), then UCM AXL (and other external calls) requests and responses aren't written to the transaction log, and neither are generic driver requests, responses, template evaluations, and macro evaluations. These details won't display for the relevant transactions (on the **Transaction Log** page).

Activate phone status service

High level admins (`sysadmin`) with access to the `data/Settings` model (**Settings** page) can view and update the **Activate Phone Status Service** checkbox, which is enabled by default.

When enabled, this setting indicates that the real-time information (RIS) data collector service is enabled and is polling the CUCM to obtain the latest phone registration status information for phone instances stored in the Automate database. The polling default interval is `43200` seconds (12 hours).

For details, see the *System Monitoring Configuration* (Metrics Collection) topic in the Advanced Configuration Guide.

However, When viewing a list of phones, the **status** action can be carried out by an administrator who has been assigned a role that has an access profile to enable this action. By default, an administrator *above* provider level can carry out this task via the **Access Profiles** page - in this case, for `relation/SubscriberPhone`.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Carrying out this operation fetches the UCM phone IP address and status *directly* from the UCM and displays the data on the **Phones** list view **Registration Status** and **IP Address** columns, updating any existing data shown.

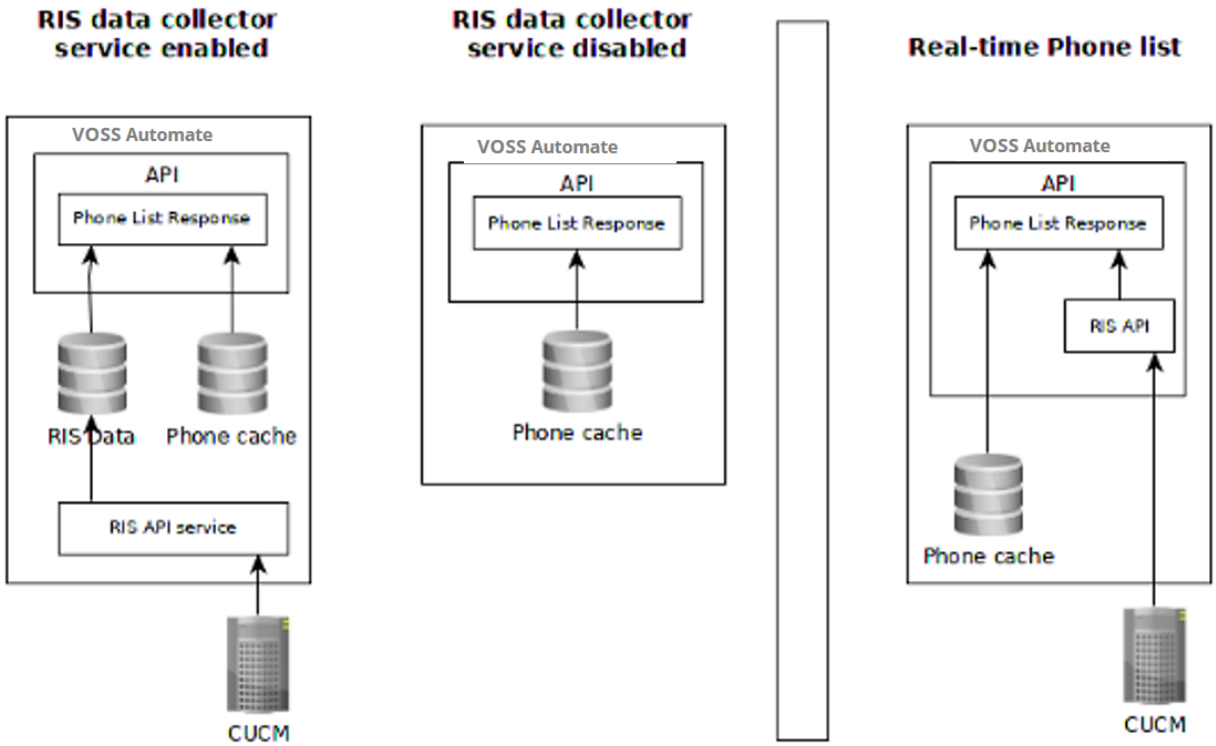
Important: Since the result of the **status** action is in real time, the current status of the list requires that the action carried out in order to see the latest values.

There is no caching of data resulting from this action. If any values show in the columns before carrying out this action, these would not be current, but are the cached values from the RIS data collector if it is enabled.

When carrying out the **status** action, the data in the **Registration Status** and **IP Address** columns can only be viewed.:

- The latest data only shows for the *current* list of phones on the GUI.
- The data in these columns is not stored in the database and *cannot be exported*.

Copyright © 2025 VisionOSS Limited. All rights reserved.



Note:

- Whether the real-time information (RIS) data collector service is enabled or disabled, if the **status** action is carried out from the phones list view, the operation will *always* fetch and display the current information for the displayed phones directly from the device.
- The administrator's access profile associated with the role needs to allow the administrator to carry out the **status** action.
- The carrier-integrated Mobile device type is automatically added to the **RIS API Excluded Device Types** and therefore not fetched by the service.

When clearing or enabling the check box on `data/Settings`, log in on the platform command line interface (CLI) and restart the service:

```
$ cluster run application app start voss-risapi_collector
```

Phone status service in the logs

When clearing this setting and then restarting the (RIS) data collector service, an `app.log` entry will show: `"message":"RIS API service disabled"`.

Refer to the Platform Guide for commands to inspect log files.

Example log entry below (line breaks added):

Copyright © 2025 VisionOSS Limited. All rights reserved.

```
2020-03-26T20:06:00.346577+00:00 VOSS-UN-2 deviceapi.background.risapi INFO
 {"process_id":24,
  "hostname":"VOSS-UN-2-voss-risapi-collector",
  "name":"deviceapi.background.risapi",
  "level":"INFO",
  "utc_iso_timestamp":"2020-03-26T22:06:00.346268",
  "request_uuid":null,
  "user_hierarchy":null,
  "user":null,
  "message":"RIS API service disabled",
  "line":330,
  "parent_process_id":1
 }
```

Additional role access profile validation

High level admins (`sysadmin`) with access to the `data/Settings` model (**Settings** page) can view and update the **Additional Role Access Profile Validation** setting to manage the available roles when an administrator creates access profiles.

The table describes how the system works when the **Additional Role Access Profile Validation** setting is enabled or disabled:

Enabled	An admin can only assign a role to a user if it is linked to an access profile with permissions that are in the subset of the admin's own access profile. Role drop-down lists will therefore be restricted. If the macro function `fn.filter_roles_by_user_access_profile` is used, the setting needs to be enabled for roles to be filtered. This validation check also applies when admins manage multi-role admin users - where the role is associated with an Authorized Admin Hierarchy.
Disabled	(Default) An admin can assign any role to a user, regardless of the admins own access profile. Role drop-down lists will therefore not be restricted. If the macro function `fn.filter_roles_by_user_access_profile` is used, the roles will *not* be filtered. This validation check also applies when administrators manage multi-role admin users - where the role is associated with an Authorized Admin Hierarchy.

Note: See the macro topic Filter Role Functions for details on the use of the `fn.filter_roles_by_user_access_profile` function.

Copyright © 2025 VisionOSS Limited. All rights reserved.

File upload limitations

High level admins (`sysadmin`) with access to the `data/Settings` model (**Settings** page) can view and update file upload size limitations and file time to live on the database.

By default, the following file limitations apply:

- Maximum Upload File Size: 209715200 bytes (200MB)
- Time-To-Live for Uploaded Files: 24 (clean up every 24 hours)

Note:

- Extending the Maximum Upload File Size to greater than the default can impact the platform system operation.
- The minimum setting for time-to-live hours is 1 hour

Files are uploaded to the system database during activities such as:

- Bulk Load
- JSON import
- Theme upload
- Any other file upload activity, *excluding*:
  - Themes
  - SSO certificates
  - SSO service provider metadata
  - Audio files (MoH)

The time-to-live value applies to uploaded files that have not been used, in other words, imported or processed. By default, a check is done every 24 hours for such files, after which time they are removed.

Time-to-live for uploaded files

High level admins (`sysadmin`) with access to the `data/Settings` model (**Settings** page) can view and update the time-to-live for uploaded files.

Note: Files uploaded from file management menus on the Automate GUI and listed as instances of `data/File` are not affected.

Uploaded bulk load files and imported JSON files are affected; however:

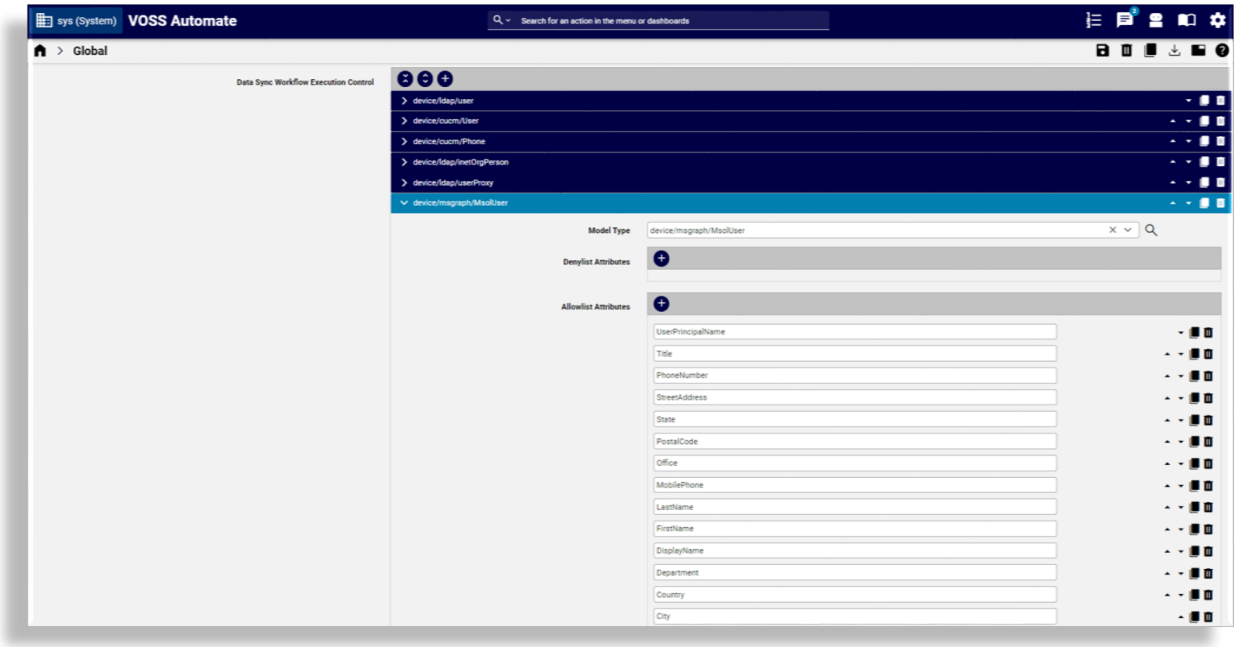
- For bulk load files, the file is kept for as long as there is an instance of `data/BulkLoad` attached to it. So a schedule that is more than 24 hours in the future is not impacted, because when we schedule a bulk load for the future, we create a `data/BulkLoad` instance. The instance is cleared when the bulk load is executed.
- Monthly license reports that are uploaded to the database by the internal schedule are not removed. For more details, refer to the License Guide.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Data sync workflow execution control

High level admins (`sysadmin`) with access to the `data/Settings` model (**Settings** page) can view and update lists of device attributes affected by data sync in the **Data Sync Workflow Execution Control** settings (allowlist and denylist attributes):

List	Description
Allowlist Attributes	When this list contains a field, then *only* a change in that field and not any other field will trigger data sync workflows, regardless of the list of the **Denylist Attributes**. In other words, this list takes precedence over the existing list of **Denylist Attributes**.
Denylist Attributes	Items in this list will *not* trigger any update workflows that may have been defined to execute during the data sync. These attributes are therefore excluded from data sync considerations. The reason for this list of attributes is that while data sync operations can have a performance impact, some data sync attribute changes do not require data sync workflows to be carried out. Note however that *the local device cache will still be updated with the updated attribute data*. No update workflows will be run, though. The transaction logs will indicate the updated device cache, but the transactions for these attributes instances will show as: *Device changes on denylisted attributes only. Updating cache, skipping workflows.*



Copyright © 2025 VisionOSS Limited. All rights reserved.

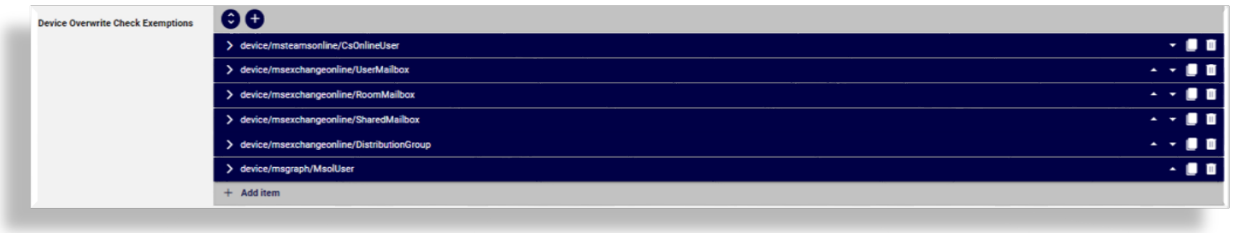
Related topics

- Allowlists and Denylists in the Core Feature Guide.
- Microsoft syncs in the Best Practices Guide.

Device overwrite check exemptions

High level admin users (`sysadmin`) with permissions to access the Global instance of the settings in the `data/Settings` model can create a list of fields to be excluded from device overwrite checking.

This means that if the field changes on the device, it will *not* be overwritten by data in Automate. The most common situation where this might be necessary is where a device field changes, but does not affect the data on Automate, because the data is treated as read only in Automate.

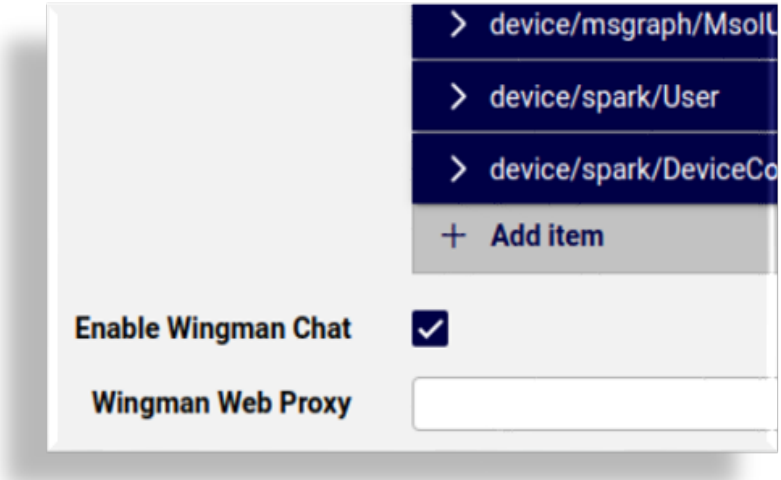


Enable Wingman chat

High level admin users (`sysadmin`) with permissions to access the *Global* instance of the settings in the `data/Settings` model (**Settings** page) can enable or disable the **VOSS Wingman** AI assistant or copilot.

By default, **Enable Wingman Chat** is enabled, and the **Wingman** icon displays on the Admin Portal toolbar, if the user role is associated with an access profile that has **Wingman Chat** enabled under the **Miscellaneous Permissions**.

See *VOSS Wingman* in the Core Feature Guide.



Copyright © 2025 VisionOSS Limited. All rights reserved.

Wingman web proxy

High level admin users (`sysadmin`) with permissions to access the *Global* instance of the settings in the `data/Settings` model (**Settings** page) can select a Web Proxy name that has been added as an instance on the **Web Proxy** menu and which will be used by VOSS Wingman on environments that require web proxy access to the internet.

Related topics

- "Set up a web proxy" in the Core Feature Guide.
- VOSS Wingman in the Core Feature Guide.

Portal Preferences

The **Portal Preferences** settings define system-wide settings for your environment.

The table describes the available settings:

Setting	Description
Application Insights	Enables/disables Automate product usage event tracking. Enabled by default. Clear the field to disable event tracking. When enabled, the system securely tracks and measures anonymized product usage events, such as login/logout actions, user hierarchy, platform ID, locality, and browser type. Additional tracked events include console errors, transaction types (add/update), transaction status (success/fail), and the names of dashboards, list views, and forms opened/closed. Event tracking in list views includes the number of results returned and filter operators used (for example, “contains”, “equals”), but not filter values. Wingman queries are excluded, with only the number of queries recorded. This data helps VOSS gain insights into product usage and improve user experience.
Tooltip Display Event	Defines the action (event) that allows tooltips to display. You can choose to have tooltips display for form elements only when using keyboard navigation (focus), or only with mouse-over (hover) over the form element, or for both hover and focus, or neither hover or focus (that is, no tooltips).

Copyright © 2025 VisionOSS Limited. All rights reserved.

Set up a Web Proxy

sys-admin

Web Proxies can be added from the **Web Proxies** menu:

- For licensing:

  If your licensing delivery method configuration includes a destination that allows for the selection of a web proxy.

  Add a web proxy to capture its connection details in the partner deployment.

  The web proxy **Name** will be available to select on file transfer destination input forms that have **Web proxy** drop downs, for example **VOSS Cloud Licensing Service**.

- For VOSS Wingman:

  To create a web proxy instance to be used in the **Wingman Web Proxy** setting available to `sysadmin` users (default menus, **Administration Menu > Settings**), thereby allowing VOSS Wingman to function in environments that access the internet via an HTTP proxy. The web proxy **Name** will be available to select in the **Wingman Web Proxy** dropdown.

  Note: The Web protocol setting must be `https`.

  Refer to the "Wingman Web Proxy" section of the Settings topic in the Core Feature Guide.

  Note: Ensure that the web proxy is created at a hierarchy level that is at or above the required level. This is necessary for the proxy to be available for requests. For example, if the proxy is created at a specific customer hierarchy level below a provider, it will not be available for another customer hierarchy that is also below the same provider.

1. From the menu, add an instance and complete the necessary fields:
   - Name
   - Web protocol (http/https)
   - Proxy protocol (http)
   - Proxy address
   - Proxy port
   - Username
   - Password
2. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

13.2.6. Northbound Notifications

Northbound Notification

The Automate Northbound Notification (NBN) functionality provides a mechanism to notify an Operations Support System (OSS) or Business Support System (BSS) when user data in Automate is created, updated, or deleted. Northbound Notifications can be customized to specify which events trigger notification and the destination of notifications.

The supported model types are:

- `data/User`

  Essential user information. Changes occur either from LDAP sync or manually in Automate.

- `relation/Subscriber`

  User information, such as assigned devices and services. Only changes made in Automate via User Management generates notifications. Changes to users made in Automate do not generate notifications.

All NBN events are post-execution so the notification is sent immediately after the data is changed in Automate.

Note: Failing changes to user data result in a pair of notifications, one for the attempted change and an opposite one for the rollback of the change. For example, a failing user add generates a create notification and a delete notification.

To suspend notifications for a given model type and operation, mark the event as 'inactive' and notifications will neither be sent nor stored while the event is inactive. Once the event is marked as 'active', subsequent notifications will be sent.

Notification Format

The Northbound Notifications are sent to a destination as HTTP or HTTPS POST requests. The message body is a JSON map that contains the notification data. The JSON map is in this format:

Key	Datatype	Operation
model_type	String	All
operation	String	All
pkid	String	All
hierarchy	String	All
new_data	Map	Create/Update
previous_data	Map	Update/Delete

The keys in the new_data and old_data maps are the attribute names for the given model type.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Example

See this example of a notification's message body triggered by updating a user:

```
{
   'model_type': 'data/User',
   'operation': 'update',
   'pkid': '5445310900698a11d83164e3',
   'hierarchy': '543c57ea00698a11d8305815',
   'new_data': {
      'username': 'jdoe',
      'email': 'jdoe@provider.com',
      'department': 'Finance'
   },
   'previous_data': {
      'username': 'jdoe',
      'email': 'jdoe@provider.com',
      'department': 'Admin'
   }
}
```

NBN Transaction Processing

Once an NBN event is triggered, it is handled in a new transaction independent of the original transaction that triggered the event. These transactions can also be queried through the transaction log. The result of the NBN transaction will be successful if a positive HTTP or HTTPS response code is received from the OSS/BSS. If no response is received (timeout) or a negative response code is received, the transaction will show as failed.

Northbound Notification Workflow

Perform the following procedures to configure northbound notification.

Perform these steps:

1. Configure Northbound Notification Destination to specify the destination for northbound notifications.
2. Configure Northbound Notification Event to specify an event to trigger the northbound notification.
3. Configure Northbound Notification Event Attributes to specify the list of attributes to be received in a notification for a specific event.

   Note:

   Steps 2 and 3 can be performed in either order, but after the list attributes are defined in Step 3 you will need to edit the event (Step 2) to add or update the Attribute Selector field.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Configure Northbound Notification Destination

Use this procedure to set the destination for Northbound Notifications of VOSS Automate events. Only one NBN destination can be configured.

Note: You cannot delete a destination until it is removed or disassociated from all events.

Perform these steps:

1. Log in as provider administrator.
2. Choose **Administration Tools** > **Northbound Notifications** > **Destination**.
3. Click **Add**.
4. Provide the following information for the destination:

Field	Description
Hostname/IP Address	Hostname or IP address of the OSS/BSS http server. This field is mandatory.
Port	The destination port. This field is mandatory.
Username	If the OSS/BSS http server has authentication enabled, specify the username to use.
Password	The password for the above username.
Secure	Use HTTPS send method for secure transport of the notification. Default = Selected. Clear the check box to use HTTP instead.

5. Click **Save**.

Configure Northbound Notification Event Attributes

Tip: *Use the Action search to navigate Automate*

You can use attribute selectors to define the attributes to be received in a notification for a particular event. Notifications contain only the specified fields and are not sent if none of the fields are chosen.

Note: You cannot delete an attribute selector until it is removed or disassociated from all events.

Important: It is possible to create an attribute selector through the API with 'invalid' attributes as there is no API validation on the list of attributes. We recommend using the Admin Portal or API to retrieve the list of attributes prior to creating an attribute list through the API. Refer to the API Reference Guide. If an invalid attribute is added to an attribute filter, the transaction will succeed but notifications will not contain the chosen field.

Perform these steps:

1. Log in as provider administrator.
2. Go to **Attributes**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

3. Click **Add**.
4. Enter a unique name.
5. Choose a model type: either `data/NormalizedUser` or `relation/Subscriber`.
6. Highlight one or more attributes and perform the following:
   - Click **Select** to add an attribute to the list of chosen attributes. You can also select multiple attributes at a time by highlighting them and clicking **Select**. The attributes move from the **Available** box to the **Selected** box.
   - Click **Remove** to remove an attribute from the list of chosen attributes. You can also remove multiple attributes at a time by highlighting them and clicking **Remove**. The attributes move from the **Selected** box to the **Available** box.

   Example: For the data/User model, you could select Username, First Name, Last Name, Phone Number, and Mail. Notifications are then sent when an event occurs that includes one or more of these attributes.
7. Click **Save**.

Next steps

Apply the event attributes to an event by adding or updating the event and choosing the desired attribute selector.

Configure Northbound Notification event

Tip: *Use the Action search to navigate Automate*

This procedure specifies an event to trigger Northbound Notifications.

Prerequisites:

- Set the Northbound Notification destination before you can configure events.

Perform these steps:

1. Log in as provider administrator.
2. Go to **Events**.
3. Click **Add**.
4. Provide the following information for the triggering event:

Copyright © 2025 VisionOSS Limited. All rights reserved.

Field	Description
Name	Event name. Must be unique. This field is mandatory.
Description	A description of the event
Active	Select to turn on notification.
Model Type	Choose either data/User or relation/Subscriber as the model type of the data that triggers the event. This field is mandatory.
Operation	Choose from the operations applicable to the selected model type. This field is mandatory.
Attribute Selector	Set an attribute selector to restrict (filter) the list of attributes sent in notifications for this event. This field is optional. To remove an existing attribute selector, backspace and delete it from the Attribute Selector field. If you do not specify an attribute selector, all possible attributes are sent in notifications for this event.
Destination	The provider's NBN destination. This field is read-only.

5. Click **Save**.

Copyright © 2025 VisionOSS Limited. All rights reserved.

14. Self-service Administration

14.1. Introduction to Self-service Administration

In addition to the administration and configuration of various components of the Self-service interface, an administrator also enables end user access to Self-service.

The items below provide an overview of this administration and configuration.

14.2. Self-service feature display policy

14.2.1. Overview

The Self-service feature display policy is used by an administrator to determine which features or services are available to the Self-service user on the Self-service UI. These are typically available on both the toolbar and dashboard.

Important: The configuration templates that are selected on the **Phones**, **Personal Phones** tabs may not contain macro values for Line Settings (nested Line Array fields), since these are not supported in Automate Self-service.

On the **Phones**, **Personal Phones** and **Voicemail** tabs, there are two similar check boxes (one associated with entitlement, the other not). For example, on the **Voicemail** tab, the first check box is labelled **User can enable Voicemail (Add a Voicemail Account)** and the second check box is labelled **User can enable Voicemail only if the user is entitled to Voicemail**.

If the entitlement feature is used, that is an entitlement profile is associated to the subscriber on the **Entitlement Profile** drop-down on the **Users** screen, then select the second check box. If an Entitlement Profile is not associated to the subscriber, then select the first check box, as the second checkbox is no longer applicable.

In a similar way, select the appropriate checkboxes on the the **Phones** and **Personal Phones** tabs.

Availability of features/services is configured using the following tabs on the **Self-service Feature Display Policy** screen:

- **Details**

  Shows/hides the **My Availability** and **Speed Dials**/**Busy Lamp Fields** areas and associated functionality. This controls the ability to add and manage speed dials and busy lamps.

The **Enable (CFWD Only) Minimal Mode** checkbox controls the user Self-service UI. If enabled, the user is presented with a minimal interface suitable for mobile devices with *only* the functionality to set call forwarding. For details on the minimal interface, refer to the topic on Minimal Mode in the Self-service Guide.

- **Phones**

  Shows/hides the **Your Company Phones** area and associated functionality. This controls the ability to add smart devices, as well as to manage company phones and associated lines.

- **Personal Phones**

  Shows/hides the complete **Your Personal Phones** area and associated functionality, or hides selected functionality only, such as setting up ring schedules or advanced timer options. Also controls the ability to enable own personal phone management (add remote destination profile).

- **My Information**

  Shows/hides one or more of the **My Information**, **My Credentials**, and **Webex Self-service** areas and the associated functionality.

- **Voicemail**

  Shows/hides one or more of the **Voicemail Settings**, **Alternate Numbers and Notification Devices**, and **Caller Input** areas, as well as the associated functionality. Also controls the ability to add own Voicemail account if required.

- **Call Forward**

  Shows/hides the complete **Call Forwarding** area and associated functionality, or selected advanced call forwarding functionality only, such forward calls to settings.

See *Self-service feature display policy field reference* for field descriptions.

See also topics under:

- “Entitlement Management” - for more details about the Entitlement feature.
- “General Subscriber Management Tasks” - for more details about associating an Entitlement Profile to a subscriber.

Copyright © 2025 VisionOSS Limited. All rights reserved.

14.2.2. Self-service feature display policy field reference

Title	Field Name	Description
Details	details	Configure Base features.
Name*	name	The name of the Feature Group.
My Availability	my_availability	Turn my availability on/off.
Automatically update Presence Status from calendar	update_presence_from _calendar	Allow users to manage the setting that automatically updates their presence status based on their calendar. The user must have 'IM and Presence' enabled, and Self-service 'My Availability' settings must be in 'Show' state.
Speed Dials	speed_dials	Turn speed dials on/off.
FMC (Fixed Mobile Convergence)	fmc	Turn FMC on/off
CLI (Calling Line Identification)	cli	Turn CLI on/off
Enable (CFWD Only) Minimal Mode	enable_minimal_mode	Display Call Forward settings only minimal mode.

Title	Field Name	Description
Phones	phones	Configure Phone features.
User can add own smart devices	own_phone_add	User can add own smart devices. Default: false.
User can add own smart devices only if the user's Entitlement Profile includes 'Voice'	own_phone_add_if _entitled	Default : false.
Limit the user's total number of phones the number allowed by the user's Entitlement Profile	own_phone_add_limit _entitlement	Default : false.
Device Configuration Templates for User Phone Add	device_type_list.[n]	See below.
Phone Management	phone_management	Turn phone management on/off.
Phone Line Management	phone_line_management	Turn phone line management on/off.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Device Configuration Templates for User Phone Add	device_type_list.[n]	Smart Device configuration.
Device Name	devicetype	Choose from the drop-down list; either: iPhone, iPad, or Android Phone or Tablet.
Device Name Prefix	device_name_prefix	Automatically populated depending on the device name selected above; either TCT, TAB, or BOT.
Configuration Template	config_template	Select from the drop-down list. We recommend that you select the default configuration template for each device.

Title	Field Name	Description
Personal Phones	personal_phones	Configure Personal Phone features.
User can enable Personal Phone Management (add Remote Destination Profile)	user_add_rdp	Default: false
User can enable Personal Phone Management / SNR only if entitled to SNR	user_add_rdp_if_entitled	Default: false
Device Configuration Template for End User Remote Destination Profile Add	rdp_config_template	Choose from the drop-down list. Default = Default CUCM RDP Template.
Personal Phone Management	personal_phone_management	Turn personal phone management on/off.
Mobile Id Management	mobileid_management	Turn mobile id management on/off.
Ring Schedules	ring_schedules	Turn ring schedules on/off.
Advanced Timer Options	advanced_timer_options	Turn advanced timer options on/off.
Line Association	line_association	Turn line association on/off.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
My Information	my_information	Configure My Information features.
User Data	user_data	Turn user data on/off.
User Language	user_language	Turn user language on/off.
Password	password	Turn password on/off.
Pin	pin	Turn pin on/off.
Minimum Pin Length	pin_min_length	Minimum length of Pin (0 to 64 characters).
Link to Webex Self-service portal	webex_link	Toggle whether end user portal users can see a link to their Webex Self-service portal. The user must have an associated webex account in order to have the link.

Copyright © 2025 VisionOSS Limited. All rights reserved.

Title	Field Name	Description
Voicemail	voicemail	Configure Voicemail features.
User can enable Voicemail (Add a Voicemail Account)	user_add_vm_account	Default: false
User can enable Voicemail only if the user is entitled to Voicemail	user_add_vm_account_if _entitled	Default: false
Device Configuration Template for End User Voicemail Account Add	voicemail_config_template	Choose from the drop-down list. Default = Default CUC User Template.
Voicemail Basic	voicemail_basic	Turn basic Voicemail on/off.
Voicemail Devices	voicemail_devices	Turn Voicemail devices on/off.
Phone Notification Device	phone_notification_device	Show/Hide Phone Notification Device management from end user.
SMS Notification Device	sms_notification_device	Show/Hide SMS Notification Device management from end user.
Voicemail Alternate Extensions	alternate_extensions	Show/Hide Voice Mail Alternate Extension management from end user.
Configuration Template for end user Alternate Extensions for Voicemail	cucaltext_config_template	Choose from the drop-down list. Default = cucalt-cft.
Configuration Template for end user add Phone Notification Devices	cucphonedevice_config_template	Choose from the drop-down list. Default = cucphone-cft.
Configuration Template for end user add SMS Notification Devices	cucsmsdevice_config_template	Choose from the drop-down list. Default = cucsms-cft.
Voicemail Caller Input	voicemail_callerinput	Turn Voicemail caller input on/off.
Voicemail Email Relay	voicemail_email_relay	Show/Hide Email Relay from end user.

Title	Field Name	Description
Call Forward	call_forward	Configure Call Forward features.
Call Forward Basic	call_fwd_basic	Turn basic call forwarding on/off.
Advanced Call Forward	call_fwd_adv	Turn advanced call forwarding on/off.

Copyright © 2025 VisionOSS Limited. All rights reserved.

14.3. End User Access and Authentication

Users with a "system user entry" may log in to the Self-service interface. A "system user entry" is created automatically when a user is added as a subscriber. Refer to the topics under "Subscriber Management".

You can grant a user access to Self-service by creating a user, with a **Self-service** role, directly in the system user interface. Such a user is not able to view devices or any services associated with the devices, nor can a manually added user view personal information such as first name, last name, address, department, and so on. Refer to *Add admin user*.

Self-service authentication is controlled by the administration interface using the same three authentication methods: Standard, LDAP, and SSO.

Consolidated password and PIN management for end users is available as follows, based on the Self-service authentication method configured for the end user:

- Standard VOSS Automate authentication: end users can change their password and PIN from the Self-service interface.
- LDAP and SSO authentication: end users cannot change their password and PIN from the Self-service interface.

To ensure the best user experience, it is recommended that all applications (Self-service and the UC applications) use the same authentication method.

14.4. Themes and Branding

The Self-service interface can be branded by configuring cascading style sheets, images, and logos. The same theme upload and download interface used for the Admin Portal is used.

The theme itself differs between the Admin Portal and the Self-service interface (based on the user role).

The Login page theme is also loaded from the URL:

```
https://<host>/selfservice/#/login?theme=<mytheme>
```

Refer to the topic "Download and Update a Theme".

14.5. Self-service Login Banner

The Self-service login banner corresponds with the administrator interface banner.

For details on banner configuration and specifications, refer to the topic on "Login Banner" in the "Advanced Configuration Guide".

Copyright © 2025 VisionOSS Limited. All rights reserved.

14.6. Personal Phones (Remote Destinations)

You must allocate a remote destination profile (RDP) to end users for them to manage their own personal phones and simultaneous ring settings.

If no RDP is associated to the end user, the Personal Phones management interface in the Self-service application is hidden.

Multiple RDP's per end user is not supported. The Personal Phones management interface in Self-service is also hidden if an end user has more than one RDP associated. Refer to the topics under "Subscriber Workflows".

14.7. Dual Mode Phones - Mobile ID

If users have a dual mode device associated, they can manage the phone number and simultaneous ring settings for the device.

If no dual mode device is associated, the relevant settings are hidden in the Self-service interface. Refer to the "Subscriber Workflows" topic.

14.8. Voicemail for Self-service

Voicemail settings are only visible in the Self-service interface if the user has a Voicemail box. Refer to the "Subscriber Workflows" topic.

14.9. Links Page

The contents of a user's Links page in the Self-service interface can be managed.

You can create one or more links to for example, Voicemail, WebEx, or downloadable content such as a User Guide.

Links on the page are associated to a user role and are managed using the Administration GUI Self-service Links interface.

Refer to "Create a Self-service Link".

Copyright © 2025 VisionOSS Limited. All rights reserved.

15. Dashboard and Menu Reference

15.1. Introduction to the default reference menus and dashboards

This reference guide contains high level details of the contents of the default set of shipped reference menus and dashboards.

Menus typically contain links to dashboards and model forms, and may contain sub-menus. Dashboards typically contain a set of widgets that provide an overview of data or easy access to related functionality. These widgets include:

- Counters: indicating counts of items at a hierarchy
- Charts: a variety of charts showing breakdowns or trends
- Tables: details of data at a hierarchy in a table format
- Quick links: a set of shortcuts to access related functionality directly from the dashboard.

While the set of menus and dashboards are provided as defaults, not all these may be available to you, since some access depends on available licenses as well as global settings.

Note that menus and dashboards can be created and modified, so that customization can be carried out according to specific needs. Refer to the relevant topics on menus and dashboards in the Core Feature Guide.

Related topics

- *Role-based dashboards and menus*

15.2. Default menus

15.2.1. Menu: Automate - Admin

Menu for the Automate - Admin role

- **Hierarchy Management**

  Hierarchy Management - Manage Sites, Customers, other hierarchy elements

- **Role Based Access**

  Administrator role settings

- **App Integration and Detailed Settings**

  Setup application to integrate with and managed advanced detailed settings

  - Microsoft Overview

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Overview

    General Microsoft Tenant settings and management
  - Microsoft Detailed Configuration

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Detailed-Configuration

    Detailed technical Microsoft Tenant settings and management
  - Webex Overview

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-UC-Integration-Webex-Overview

    General Webex tenant settings and management
  - Webex Detailed Configuration

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-UC-Integration-Cisco-Webex-Detailed-Configuration

    Detailed technical Webex settings and management
  - Webex Contact Center Configuration

    (Condition: MACRO: macro.is cisco webex contact center enabled)

    Dashboard name: Automate-UC-Integration-Cisco-Webex-Contact-Centre-Configuration

    Detailed technical Webex Contact Center settings and management
  - Cisco UCM Detailed Configuration

    (Condition: MACRO: macro.is cisco cucm enabled)

    Dashboard name: Automate-UC-Integration-Cisco-CUCM-Detailed-Configuration

    Detailed Cisco UCM (Unified Communications Manager) technical settings and management
  - Cisco CUC Detailed Configuration

    (Condition: MACRO: macro.is cisco cucx enabled)

    Dashboard name: Automate-UC-Integration-Cisco-CUC-Detailed-Configuration

    Detailed Cisco CUC (Unity Connection) technical settings and management
  - SBC Configuration

    (Condition: MACRO: macro.is session border control enabled)

    Dashboard name: Automate-UC-Integration-SBC-Management

    Setup and Manage SBC and related elements in the system

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Additional Apps

    Dashboard name: Automate-UC-Integration-Extended-UC-App-Configuration

    Additional app integration setup and detailed configuration e.g. LDAP
  - Data Sync Management

    Dashboard name: Automate-Additional-Admin-Functions-Data-Sync

    Manage Data Sync setup and schedules
  - Dialplan Tools

    Dashboard name: Automate-UC-Integration-Dialplan-Tools

    Manage and Use Dialplan orchestration tools in the system
- **Number Management**

  Multivendor number range inventory management
- **Users and Services**

  Users and Service Management
  - User Overview

    Dashboard name: Automate-Users-and-Services-User-Overview
  - User Details

    Dashboard name: Automate-Users-and-Services-User-Details
  - Microsoft User Services

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Users-and-Services-Microsoft-User-Management
  - Webex User Services

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-Users-and-Services-Webex-User-Services
  - Webex Contact Center User Services

    (Condition: MACRO: macro.is cisco webex contact center enabled)

    Dashboard name: Automate-Users-and-Services-Webex-Contact-Centre-User-Services
  - Cisco User Services

    (Condition: MACRO: macro.is cisco cucm enabled)

    Dashboard name: Automate-Users-and-Services-Cisco-User-Services
- **Call Groups**

  Call Groups - Hunt Group, Pickup Group, Call Queue, Auto Attendant
  - Microsoft Call Groups

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Call-Groups-Microsoft-Call-Groups

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Webex Call Groups

    (Condition: MACRO: macro.is cisco webex enabled)

    Dashboard name: Automate-Call-Groups-Webex-Call-Groups

  - Cisco Call Groups

    (Condition: ((macro.global setting service cisco cucm == fn.true)) <MACRO: fn.true > ((macro.is cisco cucx enabled == fn.true)) <MACRO: fn.true > <MACRO: fn.false >)

    Dashboard name: Automate-Call-Groups-Cisco-Call-Groups

- **Security Management**

  Management of Security elements - Microsoft Defender

  (Condition: MACRO: macro.IS SECURITY ENABLED)

  - Defender for Office Overview

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Overview

    Overview dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Office Actions

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Actions

    Action dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Endpoint Overview

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Overview

    Overview dashboard for Defender for Endpoint capabilities - devices, alerts, incidents and key metrics

  - Defender for Endpoint Actions

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Actions

    Action dashboard for Defender for Endpoint capabilities - view alerts, incidents, and devices as well as take a range of actions on devices

- **Insights Dashboards**

  A collection of dashboards providing insights into Microsoft

  (Condition: MACRO: macro.IS INSIGHTS ENABLED)

- **System Configuration**

  Provider platform settings

- **System Functions**

  Administration and associated support functions

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Transaction Overview

    Dashboard name: Automate-Additional-Admin-Functions-Transaction-Overview

    A dashboard providing an overview of key transaction metrics.
  - Tools

    Dashboard name: Automate-Additional-Admin-Functions-Admin-Tools

    Import, Bulk loader, auditing, logging and other admin support tools
- **About**

  Information on system software installation
  - Version

    (view/HcsVersionVIEW)
  - Patches

    (data/Patch)
  - Adaptations

    (data/adaptation log)
  - License

    (view/AboutLicense)
  - License Counts

    Dashboard name: Automate-VOSS-License-Overview

15.2.2. Menu: Automate - Admin - Microsoft Only

Menu for the Automate - Admin role - Microsoft only - tailored to MS only environments

- **Hierarchy Management**

  Hierarchy Management - Manage Sites, Customers, other hierarchy elements

  (Condition: MACRO: macro.ALLOW SITE MANAGEMENT)
- **Role Based Access**

  Administrator role settings
- **App Integration and Detailed Settings**

  Setup application to integrate with and managed advanced detailed settings
  - Microsoft Overview

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Overview

    General Microsoft Tenant settings and management
  - SBC Configuration

    (Condition: MACRO: macro.is session border control enabled)

    Dashboard name: Automate-UC-Integration-SBC-Management

Copyright © 2025 VisionOSS Limited. All rights reserved.

Setup and Manage SBC and related elements in the system

- Additional Apps

  Dashboard name: Automate-UC-Integration-Extended-UC-App-Configuration

  Additional app integration setup and detailed configuration e.g. LDAP

- Data Sync Management

  Dashboard name: Automate-Additional-Admin-Functions-Data-Sync

  Manage Data Sync setup and schedules

- Dialplan Tools

  Dashboard name: Automate-UC-Integration-Dialplan-Tools

  Manage and Use Dialplan orchestration tools in the system

- **Microsoft General**

  Overall O365 Tenant Management

  - Tenant Setup

    Dashboard name: Automate-UC-Integration-Microsoft-Overview

    General Microsoft Tenant settings and management

  - License Management

    Dashboard name: Automate-Microsoft-License-Management

    Microsoft License Management - inventory, allocations, and assignment actions

  - License Analysis

    Dashboard name: Automate-Microsoft-License-Management-Analysis

    Microsoft License Analysis dashboard for license managers

  - User Overview

    Dashboard name: Automate-Microsoft-User-Overview

    General User overview of services across the Microsoft stack

  - User Details

    Dashboard name: Automate-Users-and-Services-User-Details

    Detailed User report of services across the Microsoft stack and trend analysis

- **Microsoft Teams**

  Microsoft Teams Services

  - Detailed Configuration

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Detailed-Configuration

    Detailed technical Microsoft Tenant settings and management

  - User Management

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Microsoft-Microsoft-User-Management

Copyright © 2025 VisionOSS Limited. All rights reserved.

Manage Microsoft Teams Users and related settings

- Call Groups

  Dashboard name: Automate-Call-Groups-Microsoft-Call-Groups

  Microsoft Teams management of call groups - Auto Attendant, Call Queues and related setup

- **Microsoft Exchange**

  Microsoft Exchange Management

- **Microsoft Defender**

  Management of Security elements - Microsoft Defender

  (Condition: MACRO: macro.IS SECURITY ENABLED)

  - Defender for Office Overview

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Overview

    Overview dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Office Actions

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Actions

    Action dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Endpoint Overview

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Overview

    Overview dashboard for Defender for Endpoint capabilities - devices, alerts, incidents and key metrics

  - Defender for Endpoint Actions

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Actions

    Action dashboard for Defender for Endpoint capabilities - view alerts, incidents, and devices as well as take a range of actions on devices

- **Number Management**

  Multivendor number range inventory management

- **Insights Dashboards**

  A collection of dashboards providing insights into Microsoft

- **System Configuration**

  Provider platform settings

- **System Functions**

  Administration and associated support functions

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Transaction Overview

    Dashboard name: Automate-Additional-Admin-Functions-Transaction-Overview

    A dashboard providing an overview of key transaction metrics.
  - Tools

    Dashboard name: Automate-Additional-Admin-Functions-Admin-Tools

    Import, Bulk loader, auditing, logging and other admin support tools
- **About**

  Information on system software installation
  - Version

    (view/HcsVersionVIEW)
  - Patches

    (data/Patch)
  - Adaptations

    (data/adaptation log)
  - License

    (view/AboutLicense)
  - License Counts

    (data/LicenseAuditCounts)

15.2.3. Menu: Automate - Analyst

Menu for the Automate - Analyst role

- **Hierarchy Management**

  Hierarchy Management - Manage Sites, Customers, other hierarchy elements
- **Apps Overview**

  Overview dashboards for various technologies
  - Microsoft Overview

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Analyst-Microsoft-Overview

    General Microsoft Tenant settings and management
  - Webex Overview

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-Analyst-Webex-Overview

    General Webex tenant settings and management
- **Number Management**

  Multivendor number range inventory management

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Users and Services**

  User, Users and Service Management

  - User Overview

    Dashboard name: Automate-Users-and-Services-User-Overview

  - User Details

    Dashboard name: Automate-Users-and-Services-User-Details

  - Microsoft User Services

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Analyst-Users-and-Services-Microsoft-User-Management

  - Webex User Services

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-Analyst-Users-and-Services-Webex-User-Services

  - Webex Contact Center User Services

    (Condition: MACRO: macro.is cisco webex contact center enabled)

    Dashboard name: Automate-Analyst-Users-and-Services-Webex-Contact-Centre-User-Services

  - Cisco User Services

    (Condition: MACRO: macro.is cisco cucm enabled)

    Dashboard name: Automate-Analyst-Users-and-Services-Cisco-User-Services

- **Security Overview**

  Overview of Security elements - Microsoft Defender

  (Condition: MACRO: macro.IS SECURITY ENABLED)

  - Defender for Office Overview

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Overview

    Overview dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Endpoint Overview

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Overview

    Overview dashboard for Defender for Endpoint capabilities - devices, alerts, incidents and key metrics

- **Insights Dashboards**

  A collection of dashboards providing insights into Microsoft

  (Condition: MACRO: macro.IS INSIGHTS ENABLED)

- **Transaction Overview**

  Overview of transactions in the system

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **About**

  Information on system software installation

  - Version

    (view/HcsVersionVIEW)
  - License Counts

    Dashboard name: Automate-VOSS-License-Overview

15.2.4. Menu: Automate - License Manager

Menu for the License Manager role - focused on managing licenses and allocations in the environment

- **License Management**
- **License Analysis**

15.2.5. Menu: Automate - Service Desk

Menu for the Automate - Service Desk role

- **Hierarchy Management**

  Hierarchy Management - Manage Sites, Customers, other hierarchy elements
- **Role Based Access**

  Administrator role settings
- **App Integration and Detailed Settings**

  Setup application to integrate with and managed advanced detailed settings

  - Microsoft Overview

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Overview

    General Microsoft Tenant settings and management
  - Microsoft Detailed Configuration

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Detailed-Configuration

    Detailed technical Microsoft Tenant settings and management
  - Webex Overview

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-UC-Integration-Webex-Overview

    General Webex tenant settings and management
  - Webex Detailed Configuration

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-UC-Integration-Cisco-Webex-Detailed-Configuration

Copyright © 2025 VisionOSS Limited. All rights reserved.

Detailed technical Webex settings and management

- Webex Contact Center Configuration

  (Condition: MACRO: macro.is cisco webex contact center enabled)

  Dashboard name: Automate-UC-Integration-Cisco-Webex-Contact-Centre-Configuration

  Detailed technical Webex Contact Center settings and management

- Cisco UCM Detailed Configuration

  (Condition: MACRO: macro.is cisco cucm enabled)

  Dashboard name: Automate-UC-Integration-Cisco-CUCM-Detailed-Configuration

  Detailed Cisco UCM (Unified Communications Manager) technical settings and management

- Cisco CUC Detailed Configuration

  (Condition: MACRO: macro.is cisco cucx enabled)

  Dashboard name: Automate-UC-Integration-Cisco-CUC-Detailed-Configuration

  Detailed Cisco CUC (Unity Connection) technical settings and management

- SBC Configuration

  (Condition: MACRO: macro.is session border control enabled)

  Dashboard name: Automate-UC-Integration-SBC-Management

  Setup and Manage SBC and related elements in the system

- Additional Apps

  Dashboard name: Automate-UC-Integration-Extended-UC-App-Configuration

  Additional app integration setup and detailed configuration e.g. LDAP

- Data Sync Management

  Dashboard name: Automate-Additional-Admin-Functions-Data-Sync

  Manage Data Sync setup and schedules

- Dialplan Tools

  Dashboard name: Automate-UC-Integration-Dialplan-Tools

  Manage and Use Dialplan orchestration tools in the system

- **Number Management**

  Multivendor number range inventory management

- **Users and Services**

  Users and Service Management

  - User Overview

    Dashboard name: Automate-Users-and-Services-User-Overview

  - User Details

    Dashboard name: Automate-Users-and-Services-User-Details

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Microsoft User Services

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Users-and-Services-Microsoft-User-Management
  - Webex User Services

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-Users-and-Services-Webex-User-Services
  - Webex Contact Center User Services

    (Condition: MACRO: macro.is cisco webex contact center enabled)

    Dashboard name: Automate-Users-and-Services-Webex-Contact-Centre-User-Services
  - Cisco User Services

    (Condition: MACRO: macro.is cisco cucm enabled)

    Dashboard name: Automate-Users-and-Services-Cisco-User-Services
- **Call Groups**

  Call Groups - Hunt Group, Pickup Group, Call Queue, Auto Attendant
  - Microsoft Call Groups

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Call-Groups-Microsoft-Call-Groups
  - Webex Call Groups

    (Condition: MACRO: macro.is cisco webex enabled)

    Dashboard name: Automate-Call-Groups-Webex-Call-Groups
  - Cisco Call Groups

    (Condition: ((macro.global setting service cisco cucm == fn.true)) <MACRO: fn.true > ((macro.is cisco cucx enabled == fn.true)) <MACRO: fn.true > <MACRO: fn.false >)

    Dashboard name: Automate-Call-Groups-Cisco-Call-Groups
- **Security Management**

  Management of Security elements - Microsoft Defender

  (Condition: MACRO: macro.IS SECURITY ENABLED)
  - Defender for Office Overview

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Overview

    Overview dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies
  - Defender for Office Actions

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Actions

    Action dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Defender for Endpoint Overview

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Overview

    Overview dashboard for Defender for Endpoint capabilities - devices, alerts, incidents and key metrics
  - Defender for Endpoint Actions

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Actions

    Action dashboard for Defender for Endpoint capabilities - view alerts, incidents, and devices as well as take a range of actions on devices
- **Insights Dashboards**

  A collection of dashboards providing insights into Microsoft

  (Condition: MACRO: macro.IS INSIGHTS ENABLED)
- **System Functions**

  Administration and associated support functions
  - Transaction Overview

    Dashboard name: Automate-Additional-Admin-Functions-Transaction-Overview

    A dashboard providing an overview of key transaction metrics.
  - Tools

    Dashboard name: Automate-Additional-Admin-Functions-Admin-Tools

    Import, Bulk loader, auditing, logging and other admin support tools
- **About**

  Information on system software installation
  - Version

    (view/HcsVersionVIEW)
  - License Counts

    Dashboard name: Automate-VOSS-License-Overview

15.2.6. Menu: Automate - Service Desk - Microsoft Only

Menu for the Automate - Service Desk role - for Microsoft Only - streamlined and tailored menu to a MS environment only.

- **Hierarchy Management**

  Hierarchy Management - Manage Sites, Customers, other hierarchy elements

  (Condition: MACRO: macro.ALLOW SITE MANAGEMENT)
- **Role Based Access**

  Administrator role settings

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Microsoft General**

  Overall O365 Tenant Management

  - Tenant Setup

    Dashboard name: Automate-UC-Integration-Microsoft-Overview

    General Microsoft Tenant settings and management
  - License Management

    Dashboard name: Automate-Microsoft-License-Management

    Microsoft License Management - inventory, allocations, and assignment actions
  - License Analysis

    Dashboard name: Automate-Microsoft-License-Management-Analysis

    Microsoft License Analysis dashboard for license managers
  - User Overview

    Dashboard name: Automate-Microsoft-User-Overview

    General User overview of services across the Microsoft stack
  - User Details

    Dashboard name: Automate-Users-and-Services-User-Details

    Detailed User report of services across the Microsoft stack and trend analysis
- **Microsoft Teams**

  Microsoft Teams Services

  - Detailed Configuration

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Detailed-Configuration

    Detailed technical Microsoft Tenant settings and management
  - User Management

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-Microsoft-Microsoft-User-Management

    Manage Microsoft Teams Users and related settings
  - Call Groups

    Dashboard name: Automate-Call-Groups-Microsoft-Call-Groups

    Microsoft Teams management of call groups - Auto Attendant, Call Queues and related setup
- **Microsoft Exchange**

  Microsoft Exchange Management
- **Microsoft Defender**

  Management of Security elements - Microsoft Defender

  (Condition: MACRO: macro.IS SECURITY ENABLED)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Defender for Office Overview

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Overview

    Overview dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Office Actions

    (Condition: MACRO: macro.is microsoft defender for office enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Office-Actions

    Action dashboard for Defender for Office email capabilities - Quarantine email, safe link, and safe attachment policies

  - Defender for Endpoint Overview

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Overview

    Overview dashboard for Defender for Endpoint capabilities - devices, alerts, incidents and key metrics

  - Defender for Endpoint Actions

    (Condition: MACRO: macro.is microsoft defender for endpoint enabled)

    Dashboard name: Automate-Security-Management-Defender-for-Endpoint-Actions

    Action dashboard for Defender for Endpoint capabilities - view alerts, incidents, and devices as well as take a range of actions on devices

- **Number Management**

  Multivendor number range inventory management

- **Insights Dashboards**

  A collection of dashboards providing insights into Microsoft

- **System Functions**

  Administration and associated support functions

  - Transaction Overview

    Dashboard name: Automate-Additional-Admin-Functions-Transaction-Overview

    A dashboard providing an overview of key transaction metrics.

  - Tools

    Dashboard name: Automate-Service-Desk-Additional-Admin-Functions-Admin-Tools

    Import, Bulk loader, auditing, logging and other admin support tools

- **About**

  Information on system software installation

  - Version

    (view/HcsVersionVIEW)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - License Counts
    (data/LicenseAuditCounts)

15.2.7. Menu: HcsAdminMenu

- **Hierarchy Management**
  - Localization Language
    (data/LanguageDefault)
- **Provider Management**
  - Providers
    (relation/HcsProviderREL)
  - Delete Provider
    (view/HcsDeleteProviderVIEW)
- **User Management**
  - Admins
    (relation/User)
- **Role Management**
  - Roles
    (data/Role)
  - Authorized Admin Hierarchy
    (data/AuthorizedAdminHierarchy)
  - Themes
    (tool/Theme)
  - Menu Layouts
    (data/MenuLayout)
  - Menu Diff Tool (Portal only)
    (view/MenuDiff)
  - Dashboards
    (data/Dashboard)
  - Dashboards Permission Groups
    (data/DashboardPermissionGroup)
  - Dashboard Value Mapping
    (data/DashboardValueMapping)
  - Access Profiles
    (data/AccessProfile)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Access Profile Merge Tool
    (view/AccessProfileTool)
  - Credential Policy
    (data/CredentialPolicy)
  - Default Credential Policy
    (data/HierarchyDefault)
  - Business Admin Portal Profiles
    (data/InterfaceBusinessAdminPortal)
  - Self Service Feature Display Policy
    (data/SelfServiceFeatureDisplayPolicy)
  - Self Service Links
    (data/SelfServiceLinks)
  - Privacy Policy Configuration
    (data/PrivacyPolicy)
  - Delete Unused Roles
    (view/DeleteUnusedRoles)
- **Flow Through Provisioning Configuration**
  - User Profiles
    (data/SubscriberProfile)
  - Model Filter Criteria
    (data/ModelFilterCriteria)
  - FTP Provisioning Criteria
    (data/FlowThroughProvisioningCriteria)
  - Global Settings
    (view/GlobalSettings)
  - Site Defaults Settings
    (data/SiteDefaultsDoc)
- **Entitlement**
  - Device Types
    (data/HcsDeviceTypeDAT)
- **Customizations**
  - Global Settings
    (view/GlobalSettings)
  - Field Display Policies
    (data/FieldDisplayPolicy)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Configuration Templates
    (data/ConfigurationTemplate)
  - Business Admin Portal Profiles
    (data/InterfaceBusinessAdminPortal)
  - Self Service Feature Display Policy
    (data/SelfServiceFeatureDisplayPolicy)
  - Self Service Links
    (data/SelfServiceLinks)
  - Move Phones
    (data/HcsMovePhoneCustomizationsDAT)
  - User Profiles
    (data/SubscriberProfile)
  - Phone Configuration Mapping
    (data/PhoneConfigMapping)
  - DeviceProfile Configuration Mapping
    (data/DeviceProfileConfigMapping)
  - Line Configuration Mapping
    (data/LineConfigMapping)
- **Number Management**
  - Number Inventory
    (relation/NumberInventoryREL)
  - Number Range Management
    (view/NumberInventoryRangeMgmtVIEW)
  - Cooling and Reservation
    (view/IniCoolingMgmtVIEW)
  - Audit Number Inventory
    (view/NumberInventoryAudit)
  - Purge Number Inventory
    (view/INI Purge Tool View)
  - E164 Inventory
    (Condition: MACRO: macro.IsProviderDeploymentMCR)
    (data/HcsDpE164InventoryDAT)
  - Add E164 Inventory
    (Condition: MACRO: macro.IsProviderDeploymentMCR)
    (view/HcsE164InventoryMgmtView)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - E164 Associations (N to N DN)
    (Condition: MACRO: macro.IsProviderDeploymentMCR)
    (relation/HcsDNE164AssociateREL)
  - E164 Associations (N to 1 DN)
    (Condition: MACRO: macro.IsProviderDeploymentMCR)
    (relation/HcsDNMultiE164AssociateREL)
- **Dial Plan**
  - Dial Plan Schema
    (data/HcsDpDialPlanSchemaDAT)
  - Dial Plan Schema Group
    (data/HcsDpDialPlanSchemaGroupDAT)
- **Administration Tools**
  - Import
    (tool/DataImport)
  - Bulk Load
    (tool/BulkLoad)
  - Alerts
    (data/Alert)
  - Transaction Overview
    Dashboard name: Automate-Additional-Admin-Functions-Transaction-Overview
    A dashboard providing an overview of key transaction metrics.
  - Transaction
    (tool/Transaction)
  - Overview Tool
    (Condition: MACRO: macro.IsEnterpriseDeploymentMCR)
    (view/OverbuildOverview)
  - Macro
    (data/Macro)
  - Macro Evaluator
    (tool/Macro)
  - Model Type Lists
    (data/ModelTypeList)
  - Model Instance Filters
    (data/ModelInstanceFilter)
  - Data Sync
    (data/DataSync)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Scheduling
    (data/Schedule)
  - Bulk Enable/Disable Schedules
    (view/BulkScheduleTool)
  - File Management
    (data/File)
  - Reports
  - System Monitoring
  - System Settings
    (view/DataSettings)
- **Advanced Tools**
  - Custom Variables
    (data/StaticVariable)
  - Model Report
- **Single Sign On**
  - SSO SP Settings
    (relation/HcsSsoSpREL)
  - Certificate Management
    (data/Certificate)
  - SSO SP Metadata
    (data/HcsSpMetadataDAT)
- **About**
  - Version
    (view/HcsVersionVIEW)
  - Patches
    (data/Patch)
  - Adaptations
    (data/adaptation log)
  - License
    (Condition: MACRO: macro.IsProviderDeploymentMCR)
    (view/AboutLicense)
  - License Counts
    Dashboard name: Automate-VOSS-License-Overview

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.2.8. Menu: HcsSAMenu

- **About**
  - Version

    (view/HcsVersionVIEW)

15.2.9. Menu: Insights - Admin

Menu for the Insights - Admin role

- **Hierarchy Management**

  Hierarchy Management - Manage Sites, Customers, other hierarchy elements
- **Role Based Access**

  Administrator role settings
- **App and Device Integration**

  Setup applications and devices to send and receive data
  - Microsoft Overview

    (Condition: MACRO: macro.is microsoft enabled)

    Dashboard name: Automate-UC-Integration-Microsoft-Overview

    General Microsoft tenant settings and management
  - Webex Overview

    (Condition: MACRO: macro.is cisco webex teams enabled)

    Dashboard name: Automate-UC-Integration-Webex-Overview

    General Webex tenant settings and managment
  - VOSS Arbitrators

    Dashboard name: Insights-Admin-Arbitrator-Management
  - VOSS Agents

    (data/AssuranceDemSystemStats)
- **Insights Dashboards**

  A collection of dashboards providing insights into Microsoft
- **System Configuration**

  Platform Settings
- **System Functions**

  Administration and associated support functions
  - Transaction Overview

    Dashboard name: Automate-Additional-Admin-Functions-Transaction-Overview

    A dashboard providing an overview of key transaction metrics.

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Tools

    Dashboard name: Insights-Additional-Admin-Functions-Admin-Tools

    Import, Bulk loader, auditing, logging and other admin support tools

- **About**

  Information on system software installation

  - Version

    (view/HcsVersionVIEW)
  - Patches

    (data/Patch)
  - Adaptations

    (data/adaptation log)
  - License

    (view/AboutLicense)
  - License Counts

    Dashboard name: Automate-VOSS-License-Overview

15.3. Default dashboards

15.3.1. Automate - Additional Admin Functions - Admin Tools

General tools, file access and information

Links

- **General Tools**
  - Transaction Log
  - Transactions Log Level Configuration
  - Bulk Load
  - Alerts
  - Import
  - Macro Evaluator
  - Dashboard Exports
  - Schedules
- **Files and Logs**
  - File Management
  - Certificate Management
  - User Management logs
  - Create Model Report

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Model Report Results
- **Overbuild Tools**
  - Overbuild Overview
  - Site Defaults
  - Run Overbuild
  - Run Analogue Gateway Overbuild
  - Run Dial-Plan Overbuild
  - Dial-Plan Overbuild Search Queries
  - Fix User Phone Associate Tool
  - Move user (without Services)

15.3.2. Automate - Additional Admin Functions - Data Sync

Manage data sync options for the various integrated UC apps

Counters

- Active Schedules
- Inactive Schedules

Links

- **General Data Sync Options**
  - All Pull Syncs
  - All Purge Syncs
  - Sync Scheduling
  - Model Type Lists
  - Model Instance Filters
  - Bulk Schedule Activation / Deactivation
  - Default Sync Workflows
  - Datasync Builder
- **LDAP Data Syncs**
  - Sync LDAP Users
  - Resync LDAP Users
  - LDAP User Sync
  - LDAP User Purge (HcsLdapUserPurge filter)
  - LDAP Schema Import (HcsLdapSchemaImport filter)
- **Cisco Webex Calling Data Syncs**
  - Cisco Webex Sync (SyncSpark filter)
  - Cisco Webex Purge (PurgeSpark filter)

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Microsoft Data Syncs**
  - Microsoft Apps Sync (SyncMS filter)
  - Microsoft Apps Purge (PurgeMS filter)
- **Cisco Data Syncs**
  - Cisco UC Apps Sync (HcsPull filter)
  - Cisco CUCM User Sync (HcsUserSync filter)
  - Cisco CUCM-CNF Sync (HcsCnf filter)
  - Cisco UC Apps Purge Sync (HcsPurge sync filter)
  - Cisco CUCM Phone Purge Sync (HcsPhonePurge filter)
  - Cisco CUCM Phone Sync (HcsPhoneSync filter)
  - Cisco CUCM-CNF Device Changes
  - Cisco CUCM User Purge Sync (HcsUserPurge filter)

15.3.3. Automate Analyst - Hierarchy

Hierarchy Dashboard for VOSS - Analyst Role

Counters

- Resellers
- Customers
- Intermediate Nodes
- Sites

Charts

- **Number of Admins by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** User
- **Sites by Customer (Top 10)**
  - **Description:** Number of Site for the top 10 customers
  - **Type:** chart-pie
  - **Resource:** Site
- **End Users by Customer - Top 5**
  - **Description:** Number of Site for the top 10 customers
  - **Type:** chart-column
  - **Resource:** Multivendor Subscriber View
- **Site Count Trend (Weekly)**
  - **Description:** Trend on the number of sites in the system on a weekly basis

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-line
  - **Resource:** Site Trend Metrics

15.3.4. Automate Analyst - Home

Main Dashboard for Automate - Admin Role

Counters

- Customers
- Sites
- Users
- Numbers in Use

Charts

- **Overall User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Transaction Status Trend**
  - **Description:** Shows the transaction status over time
  - **Type:** chart-line
  - **Resource:** Transactions
- **Transaction Actions - Top 10**
  - **Description:** Shows a split of the top 10 actions performed
  - **Type:** chart-pie
  - **Resource:** Transactions

15.3.5. Automate Analyst - Microsoft Overview

Overview dashboard for Automate Analyst role

Counters

- Security Groups
- O365 Groups
- Teams
- Licensed Users
- Unlicensed Users
- Teams Voice Users - no number

Charts

- **User License Status (Top 20)**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:** Summary of User assigned licenses - number of users with each set of licenses
  - **Type:** chart-pie
  - **Resource:** Microsoft O365 User
- **License Allocations by Intermediate Node**
  - **Description:** number of license allocations setup for each Intermediate node - count indicates how many different licenses are allocation
  - **Type:** chart-pie
  - **Resource:** Microsoft License Allocation

Tables

- **License Inventory Summary**
  - **Resource:** Microsoft O365 User SKU
  - **drilldown-modelType:** device/msgraph/MsolAccountSku
  - **Fields:** Customer, License Name, Owned, Used, Available, perc Available
- **License Allocation Summary**
  - **Resource:** Microsoft License Allocation
  - **drilldown-modelType:** data/MsLicenseAllocation
  - **Fields:** Hierarchy Node, License Name, Limit, Used, Available, perc Available

15.3.6. Automate Analyst - Number Management

VOSS Automate Number Inventory dashboard for Automate - Analyst Role

Counters

- Inventory: All
- Inventory - Available
- Inventory - Allocated
- Customer Numbers
- Intermediate Numbers
- Site Numbers

Charts

- **Number Inventory Usage (Used Numbers Only)**
  - **Description:** Chart showing how numbers are used
  - **Type:** chart-column
  - **Resource:** Number Inventory
- **Number Status Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Number Inventory Trend Metrics

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Internal Inventory Status Chart**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Number Inventory
- **Number Vendor Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Number Inventory Trend Metrics
- **Internal Inventory Vendor Chart**
  - **Description:** Chart showing split of numbers by vendor
  - **Type:** chart-column
  - **Resource:** Number Inventory

15.3.7. Automate Analyst - Users & Services - Cisco User Services

Cisco User overview for Automate - Analyst Role

Counters

- UCM Users
- EM Device Profiles
- Voicemail Boxes
- Single Number Reach
- Phones
- Standalone Phones

Charts

- **Cisco User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Cisco Phone Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Cisco UCM Phone Trend Metrics

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.8. Automate Analyst - Users & Services - Microsoft User Management

Microsoft User overview for Automate - Analyst Role

Counters

- Teams Users
- Teams Voice Users
- Teams Voice Users - no number
- Meeting Rooms
- Common Area Phones
- Resource Accounts
- Teams Premium
- Teams Phone Mobile
- Distribution Lists
- User Mailboxes
- Shared Mailboxes
- Meeting Room Mailboxes

Charts

- **Microsoft User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Teams User Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Multivendor Subscriber View
- **Voice Users by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.9. Automate Analyst - Users & Services - Webex Contact Centre User Services

Webex Contact Centre User Overview dashboard for Automate - Analyst Role

Counters

- Total Users
- Users with Cloud Voice
- Contact Centre Users
- Skills Profiles

Charts

- **Licensed Active CC Users**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Contact Centre User
- **Contact Center Agents per Skill Profile**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Contact Centre User
- **Users by Site**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Contact Centre User

15.3.10. Automate Analyst - Users & Services - Webex User Services

Webex User Management Dashboard

Counters

- Total Users
- Users with Cloud Voice
- Users with UCM Calling
- Workspaces
- User Phones

Charts

- **Webex User Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling User

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Webex Device Type**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling Device
- **Device Software Version**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling Device
- **Device Connection Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Device
- **Webex User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Voice Users by Site**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Multivendor Subscriber View

15.3.11. Automate Analyst - Webex Overview

Webex overview for Automate - Analyst Role

Counters

- Users with UCM Calling
- Users with Webex Calling license
- Users with Contact Centre license
- Total Webex Users

Charts

- **Top 10 License Usage Percentage**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License
- **Purchased Licenses**
  - **Description:**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-column
  - **Resource:** Webex Calling License
- **Consumed Licenses**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License

Tables

- **Webex License Inventory**
  - **Resource:** Webex Calling License
  - **drilldown-modelType:** device/spark/License
  - **Fields:** Customer, Name, Total Available, Total Used, Percentage Licenses Used

15.3.12. Automate - Call Groups - Cisco Call Groups

Cisco CUCM & CUC Call Group Settings

Counters

- Hunt Groups
- Call Pickup Groups
- Auto Attendants

Links

- **Call Group Settings**
  - View Hunt Groups
  - View Call Pickup Groups
  - Add Hunt Group
  - Add Call Pickup Group
  - Cross Site Hunt Groups
  - View Cisco Auto Attendant
  - Add Cisco Auto Attendant
  - Cisco Auto Attendant Schedule
  - Add Greeting Files

Charts

- **Pickup Groups by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Cisco UCM Call Pickup Group
- **Hunt Groups by Site (Top 10)**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Cisco UCM Hunt Pilot

15.3.13. Automate - Call Groups - Microsoft Call Groups

Microsoft Call Group Settings

Counters

- Auto Attendants
- Call Queues
- Holidays
- Resource Accounts

Links

- **Call Group Settings**
  - View Auto Attendants
  - View Call Queues
  - Add Auto Attendant
  - Add Call Queue
  - Resource Accounts
  - Manage Holidays
  - File Upload
  - View Files

Charts

- **Call Queues by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams Call Queue
- **Auto Attendants by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams Auto Attendant

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.14. Automate - Hierarchy Management

Hierarchy Management Dashboard

Counters

- Resellers
- Customers
- Intermediate Nodes
- Sites

Links

- **Hierarchy Management**
  - Reseller
  - Delete Reseller
  - Customer
  - Delete Customer
  - Intermediate Node
  - Delete Intermediate Node
  - Site
  - Delete Site
  - Site Defaults
  - Site Defaults Templates
  - Customer Build
  - Run Hierarchy Model Reports
  - Hierarchy Model Report Results
- **Hierarchy Management**
  - Intermediate Node
  - Delete Intermediate Node
  - Site
  - Delete Site
  - Site Defaults
  - Site Defaults Templates
  - Run Hierarchy Model Reports
  - Hierarchy Model Report Results
- **Hierarchy Management**
  - Site
  - Delete Site
  - Site Defaults

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Site Defaults Templates

Charts

- **Sites by Customer (Top 10)**
  - **Description:** Number of Site for the top 10 customers
  - **Type:** chart-pie
  - **Resource:** Site
- **End Users by Customer - Top 5**
  - **Description:** Number of Site for the top 10 customers
  - **Type:** chart-column
  - **Resource:** Multivendor Subscriber View
- **Sites by Intermediate Node**
  - **Description:** Number of Site by Intermediate Node
  - **Type:** chart-pie
  - **Resource:** Site
- **End Users by Intermediate Node**
  - **Description:** Number of End Users by Intermediate Node
  - **Type:** chart-column
  - **Resource:** Multivendor Subscriber View
- **End Users by Site**
  - **Description:** Number of End Users by Site
  - **Type:** chart-column
  - **Resource:** Multivendor Subscriber View
- **Site Count Trend (Weekly)**
  - **Description:** Trend on the number of sites in the system on a weekly basis
  - **Type:** chart-line
  - **Resource:** Site Trend Metrics

15.3.15. Automate - Home

Main Dashboard for Automate - Admin Role

Counters

- Customers
- Sites
- Users
- Numbers in Use

Links

- **Quick Actions**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Manage Users
  - Manage Admins
  - Number Management
  - Transaction Overview
  - Data Syncs
  - Import
  - Bulk Load

Charts

- **Overall User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Transaction Status Trend**
  - **Description:** Shows the transaction status over time
  - **Type:** chart-line
  - **Resource:** Transactions
- **Transaction Actions - Top 10**
  - **Description:** Shows a split of the top 10 actions performed
  - **Type:** chart-pie
  - **Resource:** Transactions

15.3.16. Automate - Microsoft - Exchange

Exchange management dashboard

Counters

- User Mailboxes
- Shared Mailboxes
- Room Mailboxes
- Distribution Groups

Links

- **Quick Actions**
  - Add Shared Mailbox
  - Add Room Mailbox
  - View Shared Mailboxes
  - View Room Mailboxes
  - Add Distribution Group

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - View User Mailboxes
  - View Distribution Group

Charts

- **User Mailbox Count by Region/Agency**
  - **Description:** management of exchange elements in the tenant
  - **Type:** chart-pie
  - **Resource:** Microsoft Exchange Online User Mailbox
- **User Mailbox Count by Customer**
  - **Description:** management of exchange elements in the tenant
  - **Type:** chart-pie
  - **Resource:** Microsoft Exchange Online User Mailbox
- **User Mailbox Count by Site**
  - **Description:** management of exchange elements in the tenant
  - **Type:** chart-pie
  - **Resource:** Microsoft Exchange Online User Mailbox

15.3.17. Automate - Microsoft - Home

Main Dashboard for Automate - Admin Role - Microsoft Only variant

Counters

- Entra Users
- Unlicensed Entra Users
- Teams Users
- Exchange Users
- Admins

Links

- **Quick Actions**
  - Manage Users
  - Manage Admins
  - Number Management
  - Transaction Overview
  - Data Syncs
  - Import
  - Bulk Load

Charts

- **Overall User Trend**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Transaction Status Trend**
  - **Description:** Shows the transaction status over time
  - **Type:** chart-line
  - **Resource:** Transactions
- **Transaction Actions - Top 10**
  - **Description:** Shows a split of the top 10 actions performed
  - **Type:** chart-pie
  - **Resource:** Transactions

15.3.18. Automate - Microsoft Insights

A collection of dashboards providing insights into Microsoft

Links

- **User and Device Inventory**
  - Microsoft Teams Devices
  - Microsoft Teams Active Directory User List
- **Performance - Service Management**
  - Microsoft Teams Service Health
  - Microsoft Teams User Experience Overview
- **Diagnostics**
  - Microsoft Teams Call List
  - Microsoft Teams Calls with Issues
  - Microsoft Teams Site Quality
  - Microsoft Teams Call Audio Device Detailed
  - Microsoft Teams Diagnostic Call Debug
  - Microsoft Teams Call Detail
  - Microsoft Teams PSTN Calls
  - Microsoft Teams Direct Routing Call Analysis
  - Microsoft Teams Call Review Detailed
- **Usage and Adoption**
  - Microsoft Teams Usage Analysis
  - Microsoft Teams User Review - Call Trends
  - Microsoft License Usage and User Device Stats

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Microsoft Teams Call Activity Trends
- **Digital Experience Monitoring**
  - Agent Stats
  - System Trace Details
  - System Trace Status
  - Web Service Status

Charts

- **Service Reliability**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Healthoverviews

Tables

- **Latest Service Status**
  - **Resource:** Assurance MsTeams Healthoverviews
  - **drilldown-modelType:** data/AssuranceMsTeamsHealthoverviews
  - **Fields:** Service, Status

15.3.19. Automate - Microsoft - License Management Analysis

Dashboard showing specific analysis for license managers

Counters

- Licensed Users
- Users without Licenses
- Users with E5 License

Charts

- **E5 License Allocation Per Region/Agency**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft License Allocation
- **User License Assignment**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft O365 User

Tables

- **License Allocations with low available inventory - 10perc or less**
  - **Resource:** Microsoft License Allocation

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **drilldown-modelType:** data/MsLicenseAllocation
  - **Fields:** Hierarchy Node, License Name, Limit, Used, Available, perc Available
- **Microsoft licenses with low available inventory - 10perc or lower**
  - **Resource:** Microsoft O365 User SKU
  - **drilldown-modelType:** device/msgraph/MsolAccountSku
  - **Fields:** Customer, License Name, Owned, Used, Available, perc Available

15.3.20. Automate - Microsoft - License Management

Dashboard specific to Microsoft License Management

Links

- **Microsoft License Setup**
  - Microsoft License Inventory
  - MS License Allocation
  - Email Groups
  - License Alerting setup
  - Microsoft License Name Mappings
  - Microsoft Service Plan Name Mappings
- **Microsoft License Assignment**
  - Microsoft Security Groups
  - Manage Group Membership
  - User Direct Assign License
  - Advanced User Assignment

Charts

- **Number of License Allocations by Region/Agency**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft License Allocation
- **Licensed User Count by Region/Agency**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Microsoft O365 User

Tables

- **Microsoft License Allocation**
  - **Resource:** Microsoft License Allocation
  - **drilldown-modelType:** data/MsLicenseAllocation

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Fields:** Hierarchy Node, License Name, Limit, Used, Available, perc Available
- **Microsoft License Inventory**
  - **Resource:** Microsoft O365 User SKU
  - **drilldown-modelType:** device/msgraph/MsolAccountSku
  - **Fields:** Customer, License Name, Owned, Used, Available, perc Available

15.3.21. Automate - Microsoft - Microsoft User Management

Microsoft Teams User Management

Counters

- Teams Users
- Teams Voice Users
- Teams Voice Users - no number
- Meeting Rooms
- Teams Premium
- Teams Phone Mobile
- Common Area Phones
- Resource Accounts

Links

- **Quick Actions**
  - Manage Users
  - Onboard User
  - Microsoft Quick User
  - Offboard User
  - Move User and Services
  - Microsoft User Details
  - Call Forward and Delegation
  - User Staging
  - System User Details
  - Detailed O365 Users
  - Detailed Teams Users

Charts

- **Microsoft User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Teams User Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Multivendor Subscriber View
- **Voice Users by Customer (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User
- **Teams User Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Multivendor Subscriber View
- **Voice Users by Region/Agency**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User
- **Teams User Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Multivendor Subscriber View
- **Voice Users by Site (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User

15.3.22. Automate - Microsoft - User Overview

This dashboard provides an overview of key user metrics

Counters

- Automate User Overview
- Microsoft User Services Overview
- Cisco User Services Overview
- Cisco User Services Overview

Charts

- **O365 Users Licensed by Customer**
  - **Description:** Number of users that have a license assigned in O365
  - **Type:** chart-pie

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Multivendor Subscriber View
- **Microsoft Teams Users by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User
- **Microsoft Exchange User Mailboxes by Customer**
  - **Description:** Number of User Mailboxes in Exchange
  - **Type:** chart-pie
  - **Resource:** Microsoft Exchange Online User Mailbox
- **O365 Users Licensed by Region/Agency**
  - **Description:** Number of users that have a license assigned in O365
  - **Type:** chart-pie
  - **Resource:** Multivendor Subscriber View
- **Microsoft Teams Users by Region/Agency**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User
- **Microsoft Exchange User Mailboxes by Region/Agency**
  - **Description:** Number of User Mailboxes in Exchange
  - **Type:** chart-pie
  - **Resource:** Microsoft Exchange Online User Mailbox
- **Overall User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Microsoft User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.23. Automate - Number Management

VOSS Automate Number Management

Counters

- Inventory: All
- Inventory: Available
- Inventory: Used
- Inventory: Cooling
- Inventory: Reserved

Links

- **Number Inventory Management**
  - View Number Inventory
  - Manage Number Inventory
  - Line Usage Search
  - Cooling and Reserved Number Management
  - Number Inventory Audit Tool
  - E164 Inventory
  - Add E164 Inventory
  - (N to N) DN to E164 Associations
  - (N to 1) DN to E164 Associations with Update

Charts

- **Internal Inventory Status Chart**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Number Inventory
- **Internal Inventory Vendor Chart**
  - **Description:** Chart showing split of numbers by vendor
  - **Type:** chart-column
  - **Resource:** Number Inventory
- **Number Inventory Usage (Used Numbers Only)**
  - **Description:** Chart showing how numbers are used
  - **Type:** chart-pie
  - **Resource:** Number Inventory
- **Number Status Trend**
  - **Description:**
  - **Type:** chart-line

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Number Inventory Trend Metrics
- **Number Vendor Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Number Inventory Trend Metrics

15.3.24. Automate - Role Based Access

Management of admin users and related settings

Counters

- Admins
- Roles

Links

- **Roles and Admins**
  - Admins
  - Role Management
  - Authorized Admin Hierarchy Roles
- **Role Configuration**
  - Dashboards
  - Dashboards Permission Groups
  - Menu Layouts
  - Field Display Policies
  - Themes
  - Access Profiles
  - Menu Diff Tool
  - Menu Merge Tool
- **Privacy and Login Control**
  - Credential Policy
  - Hierarchy Default Credential Policy
  - Privacy Policy Configuration
  - Login Notification Banner
  - Configure SSO IDP
  - Upload SSO IDP Metadata
- **Dashboard Configuration**
  - Color Mappings
  - Value Mappings

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Field Groupings
  - Permission Groups
  - Dashboards

Charts

- **Top 10 Active Admins (Number of Transactions)**
  - **Description:** Shows the 10 most active admins
  - **Type:** chart-pie
  - **Resource:** Transactions
- **Number of Admins by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** User

15.3.25. Automate - Security Management - Defender for Endpoint Actions

Dashboard for Defender for Endpoint actions - endpoint management

Links

- **Incident and Alert Actions**
  - View Incidents
  - View Alerts
- **Device Actions**
  - View Devices
  - View and Manage Machine Actions
  - Bulk Actions
  - Initiate Scan on Device(s)
  - Manage Isolation of Device(s)
  - Offboard Device(s)
  - Manage code execution on device(s)
  - Collect investigation from device(s)
  - Stop and Quarantine File on device(s)

Charts

- **Device Count by Exposure**
  - **Description:** Count of machines by exposure level
  - **Type:** chart-pie
  - **Resource:** Defender Devices
- **Device Count by Status**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:** Count of machine actions by type of action
  - **Type:** chart-pie
  - **Resource:** Defender Devices
- **Action Count by Type**
  - **Description:** Count of machine actions by type of action
  - **Type:** chart-pie
  - **Resource:** Defender Actions

Tables

- **Action Counts by machine - Top 10**
  - **Resource:** Defender Actions
  - **drilldown-modelType:** device/mssecurity/MachineAction
  - **Fields:** Machine DNS Name

15.3.26. Automate - Security Management - Defender for Endpoint Overview

Defender for Endpoint overview dashboard - stats and summary data

Counters

- Alerts
- Alerts
- High Severity Alerts
- Total Devices
- Unhealthy Devices
- High Risk Devices

Charts

- **Secure Score (perc) Trend - Daily**
  - **Description:** Trend of Daily Secure Score rating over time
  - **Type:** chart-line
  - **Resource:** Defender Secure Score
- **Alerts Trend - Daily**
  - **Description:** Daily Trend of alert counts by type over time
  - **Type:** chart-line
  - **Resource:** Defender Alerts
- **Alert Severity**
  - **Description:** chart showing count of alerts by severity
  - **Type:** chart-pie
  - **Resource:** Defender Alerts

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Device Platforms**
  - **Description:** Count of devices by platform
  - **Type:** chart-pie
  - **Resource:** Defender Devices
- **Device Groups**
  - **Description:** Count of devices by device group
  - **Type:** chart-pie
  - **Resource:** Defender Devices

Tables

- **Alerts**
  - **Resource:** Defender Alerts
  - **drilldown-modelType:** device/msgraphsecurity/Alert
  - **Fields:** Alert Name, Devicetags, Severity, Status, Classification, Determination, Category, Device DNS Name, User Account Name, Detection Source, Product Name, Policy Name, Policy Rule Name, Assigned To, Created, Last Updated
- **Devices**
  - **Resource:** Defender Devices
  - **drilldown-modelType:** device/mssecurity/Machine
  - **Fields:** Name, Last Seen, First Seen, OS Platform, Version, Last IP Address, Health Status, RBAC Group Name, Risk Score, Exposure Level, Machine Tags

15.3.27. Automate - Security Management - Defender for Office Actions

Dashboard for Defender for Office actions - email quarantine, safe link, safe attachment

Counters

- Quarantined Emails
- Released Emails
- Pending Requests
- Rejected Requests
- Safe Link Policies
- Policies Created
- Pending Requests
- Rejected Requests
- Safe Attachment Policies
- Policies Created
- Pending Requests
- Rejected Requests

Copyright © 2025 VisionOSS Limited. All rights reserved.

Links

- **Quarantine Email Actions**
  - View Quarantined Emails and Request Release
  - View Released Emails
  - View Release Requests
- **Safe Link Policies**
  - Manage Safe Link Policies
  - Request New Safe Link Policy
  - View Safe Link Policy Requests
  - Safe Link Policy Templates
- **Safe Attachment Policies**
  - Manage Safe Attachment Policies
  - Request New Safe Attachment Policy
  - View Safe Attachment Policy Requests
  - Safe Attachment Policy Templates

15.3.28. Automate - Security Management - Defender for Office Overview

Defender for Office overview dashboard - stats and summary data

Counters

- Quarantine Messages Counts

Charts

- **Quarantine Messagess Over Time**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Quarantine Messages
- **Quarantine Messages by Site**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Quarantine Messages
- **Quarantine Release Requestors**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Quarantine Messages
- **Quarantine Messages**
  - **Description:**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-pie
  - **Resource:** Quarantine Messages
- **Quarantine Messages Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Quarantine Messages

Tables

- **Top 10 Sender**
  - **Resource:** Quarantine Messages
  - **drilldown-modelType:** device/msexchangeonline/QuarantineMessage
  - **Fields:** Sender Address
- **Top 10 Recipient**
  - **Resource:** Quarantine Messages
  - **drilldown-modelType:** device/msexchangeonline/QuarantineMessage
  - **Fields:** Recipient Address

15.3.29. Automate Service Desk - Additional Admin Functions - Admin Tools

General tools, file access and information for the Service Desk Role

Links

- **General Tools**
  - Transaction Log
  - Bulk Load
  - Alerts
- **Overbuild Tools**
  - Overbuild Overview
  - Site Defaults
  - Run Overbuild
  - Run Analogue Gateway Overbuild
  - Run Dial-Plan Overbuild
  - Dial-Plan Overbuild Search Queries
  - Fix User Phone Associate Tool
  - Move user (without Services)

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.30. Automate Service Desk - Role Based Access

Management of admin users and related settings for Service Desk Role

Counters

- Admins

Links

- **Roles and Admins**
  - Admins

Charts

- **Top 10 Active Admins (Number of Transactions)**
  - **Description:** Shows the 10 most active admins
  - **Type:** chart-pie
  - **Resource:** Transactions
- **Number of Admins by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** User

15.3.31. Automate - System Configuration

System Configuration

Links

- **Customizations**
  - Model Filter Criteria
  - Quick Add Groups
  - Configuration Templates
  - User Profiles
  - Field Display Policies
  - Flow Through Provisioning Criteria
  - Macros
  - Manage Number Filters
  - Dropdown Filters
  - Cisco Move User Filter
  - Cisco Move User Filter Order
  - Datasync Builder Templates
  - Datasync Profiles
  - Model Instance Filter Templates

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Preferences and Defaults**
  - Global Settings
  - Site Defaults
  - MultiVendor Username Mapping Macros
  - Network Device List
  - Countries
  - Auto Line Deletion Preferences
  - Cisco Line Config Mapping
  - Cisco Phone Config Mapping
  - Cisco Device Profile Config Mapping
  - Cisco Reassign Services Profiles
  - Cisco Reassign Services Templates
- **System Monitoring**
  - Settings and Model Aggregatation
  - Database Statistics
  - Model Counts
  - VOSS Automate Cluster
  - Login Sessions
  - Worker Queue
  - Call Manager
  - Unity Connection
  - LDAP
- **License Audit Setup**
  - Email Destinations
  - File Destinations
  - Cloud Licensing Service
  - SFTP Destinations
  - File Transfer Destinations
  - Audit Settings
  - Audit Report Files
  - System User Audit
  - System User Audit Report Files
- **Email Setup**
  - SMTP (Email) Server
  - Email Templates
  - Email Groups

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Test Email Setup
- **Entitlement Management**
  - Device Types
  - Device Groups
  - Catalogs
  - Entitlement Profiles
- **Customer Build Configuration**
  - Customer and Site Build Core Workflow Steps
  - Customer Build Templates
  - Customer Build Macros
  - Customer Build Validation Rules
  - Customer Build Data Action Rules

15.3.32. Automate - UC Integration - Cisco CUC Detailed Configuration

Management of Cisco CUC settings

Links

- **CUC Servers and Nodes**
  - Unity Connection Servers
  - Unity Connection Details
  - Network Device Lists
- **Phone System Settings**
  - Phone Systems
  - Port Groups
  - Ports
- **CUC Routing**
  - Unity Class of Services
  - Routing Rules
  - Call Handlers
- **CUC General Settings**
  - Authentication Rules
  - Imported Time Zones
  - Installed Languages
  - Language Mapping
- **Cisco Unity SIP Integration**
  - Integrate Unity-CallManager

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Remove Integrate Unity-CallManager
  - Dial Plan Profile
  - Integration Log
  - Unity Tenant Add
  - Unity Tenant Delete
- **CUC User Settings and Import**
  - Unity User Templates
  - Imported Users
- **Cisco Unity Connection Localization**
  - Installed CUCM User Locales
  - Installed CUCXn Languages
  - CUC Timezone Filter
- **Cisco Voicemail Services**
  - Voicemail Service
  - Associate VM Service to Customer
  - Pilot Number
  - Associate Pilot Number to Site
- **CUCM Voicemail Settings**
  - VoiceMail Pilots
  - VoiceMail Profiles
  - Recording Profiles

15.3.33. Automate - UC Integration - Cisco CUCM Detailed Configuration

Management of Cisco CUCM call routings, various patterns and call settings

Links

- **CUCM Servers and Nodes**
  - CUCM Cluster and Servers
  - CUCM Presence Servers
  - CUCM Server Details
  - CUCM Publishers (with -p Filter)
  - Headset Enablement
  - Network Device Lists
  - User Field Mappings
- **CUCM Basic Settings**
  - UCM Server Settings

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - UCM Process Nodes
  - Call Manager Groups
  - CUCM Group Selection
  - CUCM Group Counts
  - Device Pools
  - Locations
  - Regions
  - Date Time Group
  - CUCM Schedules
- **CUCM Parameters and Options**
  - Service Parameters
  - EnterprisePhone Config
  - Device Mobility Group
  - Device Mobility Info
  - Audio Codec Pref List
- **Media and Conferencing**
  - Annunciators
  - Conference Bridges
  - Media Termination Points
  - Transcoders
  - Media Resource Groups
  - Media Resource Group List
  - Announcements
  - MeetMe
- **Phone Resources**
  - Phone Types
  - Device Defaults
  - Softkey Templates
  - Phone Button Templates
  - Common Phone Profile
  - Phone FCP Policies
  - Common Device Configuration
- **CUCM Music On Hold**
  - Manage MOH Clusters
  - MOH Servers
  - Manage Files And Upload to MOH Cluster

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Upload Multiple Files to MOH Clusters
  - Add MOH Audio Source
  - List MOH Audio Files
  - Manage MOH Audio Source
  - Fixed MOH Sources
- **UC and Phone Services**
  - IP Phone Services
  - UC Services
  - UC Service Profiles
- **Cisco FAC Management**
  - Forced Authorization Codes
  - Sync FAC Codes Cross Clusters
- **Phone-Based Registration Support**
  - PBR Set-Up
  - PBR Config
  - PBR phonereg IP Phone Service
  - AutoRegistration Phone Protocol
  - PBR UDT Templates
  - PBR ULT Templates
  - Auto Reg Phones
  - PBR Phones and PINs
  - PBR Register Phone
- **Calls Settings**
  - Client Matter Codes
  - Forced Authentication Codes
  - Call Park
  - Directed Call Park
  - Application Dial Rules
  - ILS Configuration
  - CallerFilter Access Lists
  - SRST Reference
- **GDPR and Other Settings**
  - Time Periods
  - Time Schedules
  - GDPR Advertised Patterns
  - GDPR Blocked Patterns

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Remote Clusters
- **SIP Trunks and Scripts**
  - SIP Profiles
  - SIP Trunk Security Profiles
  - SIP Trunks
  - SIP Normalization Scripts
- **Phone and Service Device Models**
  - CUCM Phones
  - CUCM EM DeviceProfiles
  - CUCM Remote Destinations
  - CUCM RD Profiles
  - CUCM RD ToD Access
  - CUCM Caller Filter List
  - CUCM DefaultDeviceProfiles
- **EMCC Settings**
  - EMCC Group
  - EMCC Route Patterns
  - EMCC Configuration Templates
  - EMCC Feature Configuration
  - EMCC Intercluster Service Profile
- **Cisco User Self Provisioning**
  - User Profiles
  - Self Provisioning Line Masks
  - Universal Device Templates
  - Universal Line Templates
- **Routing**
  - Route Group
  - Local Route Group Names
  - Route Lists
  - Route Patterns
  - Route Partitions
  - CTI Route Points
  - Route Plan
  - SIP Route Patterns
  - Hcs DP SIP Route Pattern
  - Route Filters

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **IOS Management - General**
  - IOS Devices
  - IOS Command Builder
  - IOS Commands
  - IOS Commands Consolidation
- **MGCP and SCCP Analog Gateways**
  - SCCP and MGCP Analog Gateways
  - Add Port to Analog Gateway
  - UCM SCCP Analog Endpoints
  - UCM MGCP Analog Endpoints
- **SIP Gateways**
  - SIP Local Gateways
  - SIP Gateway Port
  - Associate SIP Local Gateway
  - IOS Gateway CFTs (with GS IOSGateway filter)
  - Quick Add SIP Local Gateway
- **CUCM Network Elements**
  - WLAN Profiles
  - WLAN Profiles Groups
  - WiFi Access Point Controllers
  - WiFi Hotspots
  - Network Access Profiles
- **Translation and Transformation**
  - Translation Patterns
  - Calling Party Transformation Patterns
  - Calling Search Spaces
  - Called Party Transformation Patterns
- **Cisco CUCM LDAP Settings**
  - Run CUCM LDAP Directory Sync
  - CUCM LDAP System
  - CUCM LDAP Directory
  - CUCM LDAP Authentication
  - CUCM LDAP Custom Filters
  - CUCM Feature Groups
- **Cisco UCCX Management**
  - UCCX Server

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Agent Profiles
  - UCCX Agents
  - UCCX Agent Stats
  - UCCX Teams
  - UCCX Skills
  - UCCX Resource Groups
  - UCCX Service Queue
  - Manage Agent Skills
  - Manage Resource Group Skills
  - Manage Team Skills
- **Cisco UCCE Agent Line tagging Setup**
  - CC Servers
  - CC Service
  - Agent Lines
  - CC Users
  - CC Users Preferences
  - CC User CFTs (with GS CCUser filter)

15.3.34. Automate - UC Integration - Cisco Webex Contact Centre Configuration

Webex Contact Centre Dashboard

Counters

- Webex Contact Centre Sites
- Webex Contact Centre Teams
- Webex Users
- Webex Contact Centre Users

Links

- **Customer Experience**
  - Channels
  - Queues
  - Business Hours
  - Audio Files
  - Flows
- **Desktop Experience**
  - Multimedia Profiles
  - Outdial ANI

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Dial Plans
  - Address Books
  - Desktop Profiles
- **Advanced**
  - Holidays
  - Overrides
  - Work Type
  - Auxiliary Codes
- **User Management**
  - Sites
  - Teams
  - Skill Definitions
  - Skill Profiles
  - User Profiles
  - Webex Users
  - Onboard User (Quick Add)

Tables

- **License Summary**
  - **Resource:** Webex Calling License
  - **drilldown-modelType:** device/spark/License
  - **Fields:** License Name, Total Licenses Purchased, Licenses Used, Subscription Reference

15.3.35. Automate - UC Integration - Cisco Webex Detailed Configuration

Webex Overview Dashboard

Counters

- Webex Instances
- Webex Locations
- Webex Users

Links

- **Webex Calling Connection and Licenses**
  - Webex Application Access
  - Webex Licenses
  - Webex Location to Hierarchy Mapping
- **Webex Calling Devices**
  - Activate Webex Device

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Webex Devices
  - Workspace Device Configuration Profiles
  - Quick Add Webex Device
  - Test Workspace Device Configuration Profiles
  - Replace Webex Device
  - Rebaseline Device Schedule Configuration
  - Supported Devices (device model)
- **Webex Calling Locations and Settings**
  - Locations
  - Location Calling Details
  - Workspaces
  - Workspace Call Settings
  - Call Park Group
  - Call Park Extensions
- **Webex Calling Users and Service Settings**
  - Webex Numbers
  - Groups
  - Teams
  - Calling Profiles
  - Wholesale Customer
  - Wholesale Users
  - Bulk Update tool

Tables

- **License Summary**
  - **Resource:** Webex Calling License
  - **drilldown-modelType:** device/spark/License
  - **Fields:** License Name, Total Licenses Purchased, Licenses Used, Subscription Reference, Customer

15.3.36. Automate - UC Integration - Dialplan Tools

Setup and use dialplan orchestration tools and features in the system

Links

- **Custom Dialplan Tool - Actions**
  - Custom Dial Plans
  - Delete Custom Dialplans
  - Custom Dialplan Viewer

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Custom Dialplan Operations
  - Global Data
  - Site Data
  - Custom Dialplan Logs
- **Custom Dialplan Tool - Cisco Basic Setup Models**
  - Device Pool - Region - Location - SRST
  - Physical Locations
  - Media Resource Group
  - Media Resource Group List
  - Conference Bridge
  - Media Termination Point
  - Transcoders
- **Custom Dialplan Tool - Cisco Routing Models**
  - Partitions
  - Calling Search Space
  - CTI Route Points
  - Local Route Groups
  - Route Groups
  - Route List
  - Route Patterns
  - SIP Route Patterns
  - SIP Trunks
  - Call Park
  - Translation Patterns
  - Called Party Transformations
  - Calling Party Transformations
  - Advertised Patterns
  - Time Schedules
  - Time Periods
- **Custom Dialplan Tool - Microsoft Dialplan Models**
  - PSTN Gateway
  - PSTN Usage
  - Voice Route
  - Voice Routing Policy
  - Translation Rule
  - Tenant Dialplan

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Calling Policies
  - Call Park Policies
  - Emergency Call Routing Policies
  - Calling Line Identity
  - Enhanced Encryption Policies
  - Online Voicemail Policies
- **Cisco UCPrep Management**
  - UCPrep Profiles
  - UCPrep Profile Push
  - UCPrep Friendly Timezones
  - UCPrep App User List
  - UCPrep Configuration Templates (ucprep filter)
- **Cisco-MS Teams Hybrid Dialplan Elements deployed (MS-Teams filter)**
  - CUCM MS-Teams Route Partitions
  - CUCM MS-Teams CSSs
  - CUCM MS-Teams SIP Trunks
  - CUCM MS-Teams Translation Patterns
  - CUCM MS-Teams Route Patterns
  - CUCM MS-Teams Remote Destination Profile
  - CUCM MS-Teams Remote Destinations
  - CUCM MS-Teams RD ToD Access
  - CUCM MS-Teams Caller Filter List
  - MS-Teams Pilot Numbers
- **Cisco-MS Teams Hybrid - DPA Configuration**
  - Cisco-MS-Teams Customer Configuration
  - Cisco MS-Teams DPA CFTs
  - Cisco MS-Teams DPA Templates
  - Cisco MS-Teams DPA Configuration
  - User Profiles
  - Multi-Vendor Service Definitions
- **HCS Dial Plan Tools - For use with managed HCS Dialplans**
  - Dial Plan Schemas
  - Dial Plan Schema Groups
  - Associate Custom Dial Plan Schema Group
  - HCS Emergency and CLI Transformation Settings
  - Customer HCS Dial Plan

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - CoS-CSS Mapping for QuickAddSubscriber
  - Cisco Site DialPlans
  - Site Short Codes
  - Type 4 Directory Number Routing
  - Type 1-3 SLC TPs (ISR-PT filter)
  - Line Classes of Service

15.3.37. Automate - UC Integration - Extended UC App Configuration

Advanced UC App configuration Settings

Links

- **LDAP Server Settings**
  - LDAP Server
  - VOSS-LDAP Network Device
- **Insights**
  - Insights Assurance Arbitrators
  - Onboard Assets
  - Offboard Assets
  - Digital Experience Monitoring Agents
  - Digital Experience Monitoring Profiles
  - Arbitrator Credentials
- **LDAP Users Activities**
  - LDAP User Sync
  - LDAP Custom Role Mappings
  - Sync LDAP Users
  - LDAP Schedule
  - User Field Mappings
- **Microsoft Operator Connect for Providers**
  - Operator Connect Tenant
  - Partner Operator Consent
  - Numbers
  - Calling Profiles
  - Upload Number Range
  - Release Number Range
  - Number Order History
  - Number Release History

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Number Usage Capabilties

15.3.38. Automate - UC Integration - Microsoft Detailed Configuration

Managing Teams General Settings

Counters

- Azure Users
- Teams Users
- Exchange Users

Links

- **MS Teams Network and Emergency Routing**
  - MS-Teams Network Region
  - MS-Teams Network Site
  - MS-Teams Network Subnet
  - MS-Teams Trusted IP Address
  - MS-Teams Lis Civic Address
  - Emergency Locations (Relation)
  - Emergency Location Networks (Relation)
- **MS Teams Meetings and Messaging Policies**
  - Meeting Policy
  - Messaging Policy
  - Live Events Policy
  - App Permission Policy
  - App Setup Policy
  - Teams Policy
  - Update Policy
  - Enhanced Encryption Policy
  - Client Configuration
  - Teams Templates
- **MS Teams Voice Policies**
  - Voice Routing Policy
  - Voicemail Policy
  - Calling Policy
  - Caller ID Policy
  - Emergency Calling Policy
  - Emergency Call Routing Policy

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Call Park Policy
  - Audio Conferencing Policy
  - Voice Applications Policy
  - Shared Calling Routing Policy
  - Survivable Branch Appliance Policy
- **MS Teams Dialplan**
  - PSTN Gateways
  - MS Numbers
  - PSTN Usages
  - Translation Rules
  - Tenant Dialplan
  - Voice Route
  - Voice Routing Policy
  - Call Blocking
  - Inbound Blocked Number Patterns
  - Inbound Exempt Number Patterns
- **MS Auto Attendant Setup**
  - Auto Attendant Supported Language
  - Auto Attendant Supported Time Zone
  - MS-Teams Holidays
- **Microsoft License Management Mapping Configuration**
  - Microsoft License Name Mappings
  - Microsoft Service Plan Name Mappings

15.3.39. Automate - UC Integration - Microsoft Overview

General settings for the Microsoft Tenant

Counters

- Security Groups
- O365 Groups
- Teams
- Licensed Users
- Unlicensed Users
- Teams Voice Users - no number

Links

- **General Tenant Functions**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - Tenant Setup
  - Certificates
  - External Access
  - Tenant Domains
  - License Inventory
  - License Allocation
  - Network Device Lists
- **Group and Team Management**
  - Security Groups
  - O365 Groups
  - Mail Enabled Security Groups
  - Distribution Groups
  - Manage Group Membership
  - Teams

Charts

- **User License Status (Top 20)**
  - **Description:** Summary of User assigned licenses - number of users with each set of licenses
  - **Type:** chart-pie
  - **Resource:** Microsoft O365 User
- **License Allocations by Intermediate Node**
  - **Description:** number of license allocations setup for each Intermediate node - count indicates how many different licenses are allocation
  - **Type:** chart-pie
  - **Resource:** Microsoft License Allocation

Tables

- **License Inventory Summary**
  - **Resource:** Microsoft O365 User SKU
  - **drilldown-modelType:** device/msgraph/MsolAccountSku
  - **Fields:** Customer, License Name, Owned, Used, Available, perc Available
- **License Allocation Summary**
  - **Resource:** Microsoft License Allocation
  - **drilldown-modelType:** data/MsLicenseAllocation
  - **Fields:** Hierarchy Node, License Name, Limit, Used, Available, perc Available

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.40. Automate - UC Integration - SBC Management

SBC Integration and configuration Settings

Links

- **AudioCodes Routing Manager (ARM) Configuration**
  - AudioCodes Routing Manager Connection
  - Audiocodes Registered Users
- **Oracle Disaster Recovery Routing Configuration**
  - Define DR Call Routing Plans
  - Activate/Deactivate DR Routing Plans
- **Oracle SBC Configuration**
  - Oracle SBC Connection
  - SBC Realm Config
  - SBC Local Routing Config
  - SBC Access Control
  - SBC Codec Policy
  - SBC DTLS SRTP Profile
  - SBC ICE Profile
  - SBC Local Policy
  - SBC Media Policy
  - SBC Physical Interface
  - SBC RTCP Policy
  - SBC SIP Profile
  - SBC TCP Media Profile
  - SBC Config Management
- **Oracle ECB Configuration**
  - Oracle ECB Connection
  - ECB Realm Config
  - ECB User Number
  - ECB Access Control
  - ECB Media Policy
  - ECB Network Interface
  - ECB Physical Interface
  - ECB Config Management

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.41. Automate - UC Integration - Webex Overview

General settings for the Webex Organisation

Counters

- Users with UCM Calling
- Users with Webex Calling license
- Users with Contact Centre license
- Total Webex Users

Links

- **Webex General Organisation Functions**
  - Webex Organisation
  - Webex License Inventory
  - Wholesale Customers
  - Network Device Lists

Charts

- **Top 10 License Usage Percentage**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License
- **Purchased Licenses**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License
- **Consumed Licenses**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License

Tables

- **Webex License Inventory**
  - **Resource:** Webex Calling License
  - **drilldown-modelType:** device/spark/License
  - **Fields:** Customer, Name, Total Available, Total Used, Percentage Licenses Used

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.42. Automate - Users & Services - Cisco User Services

Manage Cisco Users & Phones services

Counters

- UCM Users
- EM Device Profiles
- Voicemail Boxes
- Single Number Reach
- Phones
- Standalone Phones

Links

- **User Quick Actions**
  - Manage Users
  - Onboard User
  - Cisco Quick User
  - Cisco User Details
  - System User Details
  - Hybrid Cisco-Microsoft Conversion
  - Consolidate Cisco and Microsoft Users
  - Move User and Services
  - Reset Passwords and PINs
  - Reassign User Services
  - Refresh User Services
  - Convert to CUCM-Local User
- **Phone Quick Actions**
  - Cisco Phones
  - Cisco Quick Add Phone
  - Move Cisco Phone
  - Replace Cisco Phone
  - Add Controlled Device to Cisco User
  - Remove Controlled Device from Cisco User
  - Cisco Hot Line Set-Up
  - Cisco Headsets Inventory
  - Login User to Phone
  - Logout User from Phone
  - Logout User from Multiple Phones

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Detailed User Service Listings**
  - Cisco Voicemail Users
  - Cisco Extension Mobility Profiles
  - Cisco Single Number Reach
  - Cisco Lines
  - Cisco Intercom Lines
- **Additional Phone Management Functions**
  - Cisco Phone Status Export
  - Reset-Restart Site Cisco Phones
  - Manage Cisco Phone xConfiguration
  - Cisco SCCP Analog Endpoints
  - Cisco MGCP Analog Endpoints
  - Add Devices to Application User
  - Add Application Users to Device
  - Cisco Headsets Templates

Charts

- **Cisco User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Cisco Phone Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Cisco UCM Phone Trend Metrics

15.3.43. Automate - Users & Services - Microsoft User Management

General settings for the MS Tenant for GlobalAdmin

Counters

- Teams Users
- Teams Voice Users
- Teams Voice Users - no number
- Meeting Rooms
- Common Area Phones
- Resource Accounts
- Teams Premium

Copyright © 2025 VisionOSS Limited. All rights reserved.

- Teams Phone Mobile
- Distribution Lists
- User Mailboxes
- Shared Mailboxes
- Meeting Room Mailboxes

Links

- **Quick Actions**
  - Manage Users
  - Onboard User
  - Microsoft Quick User
  - Offboard User
  - Move User and Services
  - Microsoft User Details
  - Call Forward and Delegation
  - User Staging
  - System User Details
  - Detailed O365 Users
  - Detailed Teams Users
- **General Exchange Functions**
  - View User Mailboxes
  - Add Shared Mailbox
  - View Shared Mailboxes
  - Add Room Mailbox
  - View Room Mailboxes
  - Add Distribution Group
  - View Distribution Groups

Charts

- **Microsoft User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Teams User Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Multivendor Subscriber View
- **Voice Users by Site (Top 10)**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User

15.3.44. Automate - Users & Services - User Details

This dashboard provides details of key User services

Tables

- **Summary of Services**
  - **Resource:** Multivendor Subscriber View
  - **drilldown-modelType:** relation/MultiVendorSubscribers
  - **Fields:** Provider, Reseller, Customer, Site, Username, First Name, Last Name, Email, License Status, Numbers, Voice, Voice Devices, Microsoft Licensed, Microsoft Collaboration Only, Microsoft Collaboration Teams, Microsoft Email Exchange, Cisco Webex Calling Behavior, Hybrid
- **Microsoft Service Details**
  - **Resource:** Multivendor Subscriber View
  - **drilldown-modelType:** relation/MultiVendorSubscribers
  - **Fields:** Provider, Reseller, Customer, Site, Username, First Name, Last Name, Email, O365 User Principal Name, Teams Account Enabled, Teams Feature Types, Line URI, Number Type, Voice Enabled, Exchange User Principal Name
- **Cisco Service Details**
  - **Resource:** Multivendor Subscriber View
  - **drilldown-modelType:** relation/MultiVendorSubscribers
  - **Fields:** Provider, Reseller, Customer, Site, Username, First Name, Last Name, Email, UCM User ID, Phone 1 Name, Phone 1 Product, Phone 1 Line, EM Profile Name, EM Profile Line, SNR Profile Name, SNR Line, Voicemail Alias, Voicemail Number, Contact Center Agent ID, Contact Center Agent Extension
- **Cisco Webex Service Details**
  - **Resource:** Multivendor Subscriber View
  - **drilldown-modelType:** relation/MultiVendorSubscribers
  - **Fields:** Provider, Reseller, Customer, Site, Username, First Name, Last Name, Email, Webex Email, Webex Work Number, Calling Behavior, Webex Licenses

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.45. Automate - Users & Services - User Overview

This dashboard provides an overview of key user metrics

Counters

- Automate User Overview
- Microsoft User Services Overview
- Cisco User Services Overview
- Cisco User Services Overview

Charts

- **Cisco Users by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Cisco UCM User
- **Microsoft Teams Users by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Microsoft Teams User
- **Webex Users by Customer**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling User
- **Overall User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Microsoft User Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Webex User Trends**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Cisco User Trend**
  - **Description:**
  - **Type:** chart-line

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Multivendor Subscriber View Trend Metrics

15.3.46. Automate - Users & Services - Webex Contact Centre User Services

Webex Contact Centre User Management Dashboard

Counters

- Skills Profiles
- Contact Centre Users
- Total Users
- Users with Cloud Voice

Links

- **Quick Actions**
  - View Users
  - Onboard User (Quick Add)

Charts

- **Users by Site**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Contact Centre User
- **Contact Center Agents per Skill Profile**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Contact Centre User
- **Licensed Active CC Users**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Contact Centre User

15.3.47. Automate - Users & Services - Webex User Services

Webex User Management Dashboard

Counters

- Total Users
- Users with Cloud Voice
- Users with UCM Calling
- Workspaces
- User Phones

Copyright © 2025 VisionOSS Limited. All rights reserved.

Links

- **User Quick Actions**
  - Manage Users
  - Onboard User
  - Webex Quick User
  - Offboard User
  - Webex User details
  - Move User and Services
  - System User Details
- **Device Quick Actions**
  - Webex Devices
  - Quick Add Webex Device
  - Replace Webex Device
  - Webex Workspaces
  - Quick Add Workspace
  - Activate Webex Device
  - Refresh Devices

Charts

- **Webex User Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling User
- **Webex Device Type**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling Device
- **Device Software Version**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling Device
- **Device Connection Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Device
- **Webex User Trend**
  - **Description:**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-line
  - **Resource:** Multivendor Subscriber View Trend Metrics
- **Voice Users by Site**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Multivendor Subscriber View

15.3.48. Automate - VOSS License Overview

Dashboard to give an overview of the VOSS License consumption and stats in the system

Counters

- Automate Platform License Usage Totals

Charts

- **Automate License Usage Totals Trend (Weekly)**
  - **Description:** Automate License usage totals trended over time
  - **Type:** chart-line
  - **Resource:** Automate License Counts Trend Metrics
- **Automate License Usage Breakdown - Totals**
  - **Description:** Breakdown of the Automate license usage by metric
  - **Type:** chart-pie
  - **Resource:** Automate License Counts

Tables

- **VOSS Automate License information only fields**
  - **Resource:** Automate License Counts
  - **drilldown-modelType:** data/LicenseAuditCounts
  - **Fields:** Provider, Customer, Users With More Than 10 Devices, Cisco/Microsoft Integrated Services (Hybrid)
- **Automate License Usage metrics - full data set**
  - **Resource:**
  - **drilldown-modelType:** N/A
- **VOSS Automate License - Microsoft User Information fields**
  - **Resource:** Automate License Counts
  - **drilldown-modelType:** data/LicenseAuditCounts
  - **Fields:** Provider, Customer, Total Graph Users, Ms Teams Voice Users, Ms Exchange Users, Meeting Rooms
- **VOSS Automate License Usage Counts**
  - **Resource:** Automate License Counts

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **drilldown-modelType:** data/LicenseAuditCounts
  - **Fields:** Provider, Customer, Total License Usage, Users, Standalone Devices, Meeting Rooms, Cisco UCCX, Webex Contact Center

15.3.49. DEM Agent Stats

Provides an at-a-glance view of agent connectivity, web performance, and system statistics to monitor and optimize digital experience.

Charts

- **Web Performance**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Web Performance
- **Agent Connectivity**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Connectivity

Tables

- **Agent Connectivity**
  - **Resource:** Assurance Dem Connectivity
  - **drilldown-modelType:** data/AssuranceDemConnectivity
  - **Fields:** Timestamp, Agent, Taskname, Host, Interface, ASN, Source, Destination, Protocol, Port, Hop, Psize, Drop, Rcv, Tos, Snt
- **Agent n of Jobs**
  - **Resource:** Assurance Dem System Stats
  - **drilldown-modelType:** data/AssuranceDemSystemStats
  - **Fields:** Agent, Web Performance Jobs, Connectivity Jobs
- **Web Performance**
  - **Resource:** Assurance Dem Web Performance
  - **drilldown-modelType:** data/AssuranceDemWebPerformance
  - **Fields:** Timestamp, Agent, Interface, Remote Ip, Url, Method, Response Code, Num Redirects, Num Connects, Speed Download, Speed Upload
- **Dem system stats**
  - **Resource:** Assurance Dem System Stats
  - **drilldown-modelType:** data/AssuranceDemSystemStats
  - **Fields:** Timestamp, Agent, Ip Address, Distribution, Kernel Version, Number Of Cpus, Cpu Usage, Average Cpu Usage, Memory Usage, Disk Usage, Agent, Distribution

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.50. DEM System Trace Details

Provides detailed metrics on system connectivity, including ASN and hop-based insights into latency, jitter, packet loss, and trace details for performance monitoring.

Charts

- **ASN Average Jitter (ms)**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Connectivity
- **ASN Average Latency (ms)**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Connectivity
- **ASN Average Loss (perc)**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Connectivity
- **Hop Average Loss (perc)**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Connectivity
- **Hop Average Jitter (msec)**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Connectivity
- **Hop Average Latency (msec)**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Connectivity

Tables

- **Hop Details**
  - **Resource:** Assurance Dem Connectivity
  - **drilldown-modelType:** data/AssuranceDemConnectivity
  - **Fields:** Hop ID, Hop IP Address, ASN, Avg Latency, Worst Latency, Best Latency, Last Latency, Avg Jitter, Last Jitter, Max Jitter, Int Jitter, Packet Loss
- **Connectivity Test Results**
  - **Resource:** Assurance Dem Connectivity

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **drilldown-modelType:** data/AssuranceDemConnectivity
  - **Fields:** Timestamp, Agent, Taskname, Destination, Protocol, Tos, Psize, Number of Hops, Latency Avg, Jitter Avg, Loss, Success

15.3.51. DEM System Trace Status

Offers a detailed view of system trace performance, highlighting top ASNs and destinations with the highest latency, jitter, and packet loss, alongside connectivity test results for comprehensive monitoring.

Charts

- **Top 10 ASN with highest average Pkt Loss**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Connectivity
- **Top 10 ASN with highest average Jitter**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Connectivity
- **Top 10 ASN with highest average latency**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Connectivity
- **Average Hop Pkt Loss Per Destination (ms)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Connectivity
- **Average Hop Jitter Per Destination (ms)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Connectivity
- **Average Hop Latency Per Destination (ms)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Connectivity
- **Average Hop Pkt Loss Per DEM Agent (perc)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Connectivity

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Average Hop Jitter Per DEM Agent (ms)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Connectivity
- **Average Hop Latency Per DEM Agent (ms)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Connectivity

Tables

- **Connectivity Test Results**
  - **Resource:** Assurance Dem Connectivity
  - **drilldown-modelType:** data/AssuranceDemConnectivity
  - **Fields:** Timestamp, Agent, Taskname, Destination, Protocol, Tos, Psize, Number of Hops, Latency Avg, Jitter Avg, Loss, Success

15.3.52. DEM Web Service Status

Provides insights into web service performance metrics such as response times, connection times, and error messages, with trends and detailed test results for enhanced monitoring and optimization.

Charts

- **Average Total Time (sec)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance
- **Average Start Transfer Time (sec)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance
- **Average Redirect Time (sec)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance
- **Average App Connect Time (sec)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance
- **Max Connect Time**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance
- **Max Name Lookup Time (sec)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance
- **URLs and Average Response Profile Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Web Performance
- **Agents and Average Response Profile Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Dem Web Performance
- **Top Error Messages (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Web Performance
- **Top Response Codes (Top 10)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Dem Web Performance
- **WEB Performance Test Case Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Dem Web Performance

Tables

- **Most Recent Web Performance Tests**
  - **Resource:** Assurance Dem Web Performance
  - **drilldown-modelType:** data/AssuranceDemWebPerformance
  - **Fields:** Timestamp, Agent, Taskname, Url, Remote Ip, Method, Http Version, Errormsg, Response Code
- **WEB Performance Test Cases Count of Processed**
  - **Resource:** Assurance Dem Web Performance
  - **drilldown-modelType:** data/AssuranceDemWebPerformance

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Fields:** Agent, Taskname

15.3.53. ENTAdminDashboard

Links

- **Configure Provider**
  - Configure Provider
- **Manage User Roles**
  - Manage and Import Custom Themes
  - Configure Menu Layouts
  - Configure Dashboards
  - Configure and Manage Roles
- **Configure SSO**
  - Certificate Management
  - Configure SP Settings
  - Export Metadata

15.3.54. HcsAdminDashboard

Links

- **Configure Provider**
  - Configure Provider
- **Manage User Roles**
  - Manage and Import Custom Themes
  - Configure Menu Layouts
  - Configure Dashboards
  - Configure and Manage Roles
- **Configure SSO**
  - Certificate Management
  - Configure SP Settings
  - Export Metadata

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.55. HcsSysadminDashboard

Dashboard for sysadmin user

Links

- **Administration Tasks**
  - Manage Themes
  - View Transactions
  - Manage License
  - Hierarchy Nodes
  - Manage Quick Add Groups
  - Manage User Profiles
  - Configure System Global Settings
  - Bulk Schedule Activation/Deactivation
  - SMTP Server
  - Web Proxies

15.3.56. Insights - Additional Admin Functions - Admin Tools

General tools, file access and information

Links

- **General Tools**
  - Transaction Log
  - Transactions Log Level Configuration
  - Bulk Load
  - Alerts
  - Import
- **Files and Logs**
  - File Management
  - Certificate Management

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.57. Insights Admin - Arbitrator Management

Insights Arbitrator Management Dashboard for Insights application

Counters

- Insights Arbitrator Servers

Links

- **Insight Arbitrator Configuration**
  - Add Arbitrator Server

15.3.58. Insights - Admin Home

Main Dashboard for Insights - Admin Role

Counters

- Customers
- Sites

Links

- **Quick Actions**
  - Manage Admins
  - Transaction Overview
  - Import

Charts

- **Transaction Status Trend**
  - **Description:** Shows the transaction status over time
  - **Type:** chart-line
  - **Resource:** Transactions
- **Transaction Actions - Top 10**
  - **Description:** Shows a split of the top 10 actions performed
  - **Type:** chart-pie
  - **Resource:** Transactions

Tables

- **Admin Users**
  - **Resource:** User
  - **drilldown-modelType:** relation/User
  - **Fields:** Display Name, Role, Located At

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.59. Insights - Diagnostics

A collection of diagnostic dashboards

Links

- **Microsoft Diagnostics**
  - Microsoft Teams Call List
  - Microsoft Teams Calls with Issues
  - Microsoft Teams Site Quality
  - Microsoft Teams Diagnostic Call Debug
  - Microsoft Teams PSTN Calls
  - Microsoft Teams Direct Routing Call Analysis
  - Microsoft Teams Call Activity Trends
- **Cisco Webex Diagnostics**
  - Insights Webex Calling
  - Insights Webex Participants
  - Insights Webex Meeting Quality

15.3.60. Insights - Digital Experience Monitoring

A collection of dashboards providing insights into synthetic testing

Links

- **Digital Experience Monitoring**
  - Agent Stats
  - System Trace Details
  - System Trace Status
  - Web Service Status

15.3.61. Insights Microsoft License & User Device Stats

Insights Microsoft License & User Device Stats

Charts

- **MS Licenses Being Utilized By Type**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Userlicenses

Tables

- **Latest Reported Status For Each Active Microsoft Teams User**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Assurance MsTeams Getteamsuseractivityuserdetail Latest
  - **drilldown-modelType:** data/AssuranceMsTeamsGetteamsuseractivityuserdetailLatest
  - **Fields:** Tenantname, User Id, User Principal Name, Report Refresh Date, Last Activity Date, Last Activity Days, Is Licensed, Assigned Products, Total Cost, Annual Cost, Tenant Display Name
- **Teams Device Details**
  - **Resource:** Assurance MsTeams Devices
  - **drilldown-modelType:** data/AssuranceMsTeamsDevices
  - **Fields:** Device Id, Display Name, Account Enabled, Operating System, Physical ID's, Device Version, Trust Type, Profile Type, Tenant
- **User Data for Licenses In Use**
  - **Resource:** Assurance MsTeams Userlicenses
  - **drilldown-modelType:** data/AssuranceMsTeamsUserlicenses
  - **Fields:** Display Name, Assigned Licenses SKUID, Assigned Licenses

15.3.62. Insights Microsoft Teams Active Directory User List

Insights Microsoft Teams Active Directory User List

Tables

- **User List**
  - **Resource:** Assurance MsTeams Users
  - **drilldown-modelType:** data/AssuranceMsTeamsUsers
  - **Fields:** Given Name, Surname, ID, User Principal Name, Mail, Job Title, Office Location

15.3.63. Insights Microsoft Teams Audio Device

Device inventory with compliance details

Charts

- **Top 10 Microphones With The Worst Capture Not Functioning Event Ratio Value**
  - **Description:** Capture Not Functioning Event Ratio: Fraction of the call that the media endpoint detected the capture device was not working properly.
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Media Render Devices (Speaker)**
  - **Description:** Top 10 Media Render Devices (Speaker)
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Media Capture Devices (Microphone)**
  - **Description:** Top 10 Media Capture Devices (Microphone)

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics

Tables

- **Detected User and Media Capture Device (Microphone) List**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** Display Name, Product Family, Platform, Microphone, Compliance, Usage
- **Detected User and Media Capture Device (Speaker) List**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** Display Name, Product Family, Platform, Speaker, Compliance, Usage
- **Top 10 Media Render Devices (Speaker)**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** Speaker, Display Name, Platform, Compliance, Usage
- **Top 10 Media Capture Devices (Microphone)**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** Microphone, Display Name, Platform, Compliance, Usage

15.3.64. Insights Microsoft Teams Call Activity Trends

Insights Microsoft Teams Call Activity Trends

Charts

- **Session Failure Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session Aggregated
- **Session Failures**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Call Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Calls Volume Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord
- **Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Microsoft Reported Teams User Activity Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord

15.3.65. Insights Microsoft Teams Call Audio Device Detailed

Insights MS Teams Audio device detailed statistics

Charts

- **Top 10 Windows-MacOS and Web Render Devices (Speaker)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Android and Room System Capture Devices (Microphone)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Media Render Devices (Speaker)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Microphones Worst Capture**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Speakers Worst Render**
  - **Description:**
  - **Type:** chart-column

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Microphones Worst Device Glitch**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Speakers Worst Device Glitch**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Media Capture Devices (Microphone)**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Windows-MacOS and Web Media Capture Devices (Microphone)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Top 10 Android and Room System Render Devices (Speaker)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics

Tables

- **Detected User and Media Capture Device (Microphone) List**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** User, Product Family, Platform, Microphone, Compliant
- **Detected User and Media Capture Device (Speaker) List**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** User, Product Family, Platform, Speaker, Compliant

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.66. Insights Microsoft Teams Call Detail

Teams Call Statistics - Call Detail and Participant Metrics

Charts

- **Media Type**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Stream

Tables

- **Call List Peer To Peer**
  - **Resource:** Assurance MsTeams Callrecord Reliability
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordReliability
  - **Fields:** Tenant Name, Call ID, Start Time, Organizer, Call Type, End Time, Session Failure Count, Audio Quality, Video Quality, VBSS Quality
- **Participant Provided Session Feedback Scores**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** callid, Session ID, Participant, Type, Feedback Rating
- **Participant List**
  - **Resource:** Assurance MsTeams Callrecord Participant
  - **drilldown-modelType:** N/A
  - **Fields:** detected participant id, Participant Name
- **Participant Metrics**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Stream
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantStream
  - **Fields:** tenantname, callid, Segment ID, Media, Participant, Agent Side, Stream Direction, Audio Degradation, Packet Loss Rate, RTT, Jitter, Audio Network Jitter
- **Session Failures**
  - **Resource:** Assurance MsTeams Callrecord Session Aggregated
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionAggregated
  - **Fields:** Session ID, Caller, Caller Type, Callee, Callee Type, Failure Stage, Failure Reason
- **Call List Conference/Meetings**
  - **Resource:** Assurance MsTeams Callrecord Reliability
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordReliability
  - **Fields:** Tenant Name, Call ID, Start Time, Organizer, Call Type, End Time, Session Failure Count, Audio Quality, Video Quality, VBSS Quality

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.67. Insights Microsoft Teams Call List Call Queues

Teams Call Queue Statistics - Call Detail and Quality Metrics

Charts

- **VLAB Q Audio Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Corp NY Sales Q Audio Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Corp LA Support Q Audio Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Corp LA Sales Q Audio Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord

Tables

- **Corp-NY-Sales Q - Call List**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** Calls, Startdatetime, Enddatetime, Detected Participant Displayname
- **Corp-LA-Support Q - Call List**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** Calls, Startdatetime, Enddatetime, Detected Participant Displayname
- **VLAB Q**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** Calls, Startdatetime, Enddatetime, Detected Participant Displayname
- **Corp-LA-Sales Q - Call List**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Fields:** Calls, Startdatetime, Enddatetime, Detected Participant Displayname
- **Microsoft Teams Call List**
  - **Resource:** Assurance MsTeams Callrecord
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecord
  - **Fields:** Callid, Organizer Displayname, Participant Array, Audio Quality, Video Quality, Vbss Quality, Quality Info, Duration

15.3.68. Insights Microsoft Teams Call List Combined

Teams Full Call List - Includes Call Quality

Charts

- **Top 10 Organizers**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Call Reliability**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Audio**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Video**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Session Failure**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Audio Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Video Trend**
  - **Description:**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability

Tables

- **Microsoft Teams Call List**
  - **Resource:** Assurance MsTeams Callrecord Reliability
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordReliability
  - **Fields:** Tenant Name, Call ID, Organizer Displayname, Start Time, Type, Media Types, Call Reliability, End Time, Audio Quality, Video Quality, VBSS Quality

15.3.69. Insights Microsoft Teams Call List

Insights Microsoft Teams Call List

Links

- **Dashboard Navigation**
  - User Experience Overview
  - Call Debug
  - Calls with Issues
  - Site Statistics
  - PSTN Calls
  - Direct Routing Analysis
  - Call Activity Trends

Charts

- **Call Modalities**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Stream Video Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord
- **Stream Video Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord
- **Call Reliability Trend**
  - **Description:**
  - **Type:** chart-line

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Assurance MsTeams Callrecord
- **Stream Audio Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord
- **Stream Audio Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord

Tables

- **Call List**
  - **Resource:** Assurance MsTeams Callrecord
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecord
  - **Fields:** Callid, Organizer Displayname, Participant List, Audio Quality, Video Quality, Vbss Quality, Quality Info
- **Select User**
  - **Resource:** Assurance MsTeams Callrecord
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecord
  - **Fields:** User Displayname

15.3.70. Insights Microsoft Teams Call List Teams Rooms

Teams Room Call Statistics - Call Detail and Quality Metrics

Charts

- **Call Reliability**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Audio**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Video**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Audio Trend**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability
- **Stream Quality Video Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability

Tables

- **MTR2 Call Count**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** Calls, Startdatetime, Enddatetime, Detected Participant Displayname
- **MTR1 Call Count**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** Calls, Startdatetime, Enddatetime, Detected Participant Displayname
- **Microsoft Teams Call List**
  - **Resource:** Assurance MsTeams Callrecord Reliability
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordReliability
  - **Fields:** Tenant Name, Call ID, Organizer Displayname, Start Time, Type, Media Types, Call Reliability, End Time, Audio Quality, Video Quality, VBSS Quality

15.3.71. Insights Microsoft Teams Call Review Detailed

Insights Call Review Call Detail Report

Charts

- **Calls Volume Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Call Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Call Quality Trend**
  - **Description:**
  - **Type:** chart-column

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Average Call Duration (Seconds)**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Call Modality vs Reported Quality**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Modality**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Session Failure Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
- **Call Type vs Reported Quality**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality

Tables

- **Top 100 Calls**
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordReliabilityModality
  - **Fields:** callid, quality merged, Start Time, Call Type, Organizer, Participants, Modality, Info

15.3.72. Insights Microsoft Teams Calls with Issues

Insights Microsoft Teams Calls with Issues

Charts

- **Top 10 Sites with Poor VBSS**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session
- **Top 10 Sites with Poor Video**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session
- **Top 10 Sites with Poor Audio**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session

Tables

- **Participants Impacted**
  - **Resource:** Assurance MsTeams Callrecord Session Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionParticipant
  - **Fields:** Participant
- **Detected Quality Metric Incidents**
  - **Resource:** Assurance MsTeams Callrecord Session Stream Incidents
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionStreamIncidents
  - **Fields:** Callid, Sessionid, Media, Streamdirection, Incident
- **Call List**
  - **Resource:** Assurance MsTeams Callrecord
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecord
  - **Fields:** Startdatetime, Organizer Displayname, Callid, Type, Enddatetime, Audio Quality, Video Quality, Vbss Quality, Quality Info

15.3.73. Insights Microsoft Teams Devices

Insights Microsoft Teams Devices

Tables

- **Teams Device OS Details**
  - **Resource:** Assurance MsTeams Devices
  - **drilldown-modelType:** data/AssuranceMsTeamsDevices
  - **Fields:** Lxt Customer Name, Display Name, Operating System, Operating System Version, Registration DateTime, Is Compliant?, Approx. Last Sign In

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.74. Insights Microsoft Teams Diagnostic Call Debug

Insights Microsoft Teams Diagnostic Call Debug

Tables

- **Failures by Subnet/Location**
  - **Resource:** Assurance MsTeams Callrecord Session
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSession
  - **Fields:** Caller Subnet, Failure Stage, Failure Reason
- **Caller Session Media Stream Details**
  - **Resource:** Assurance MsTeams Callrecord Media Stream
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordMediaStream
  - **Fields:** Callid, Media, Streamdirection, Caller Subnet, Ave Jitter, Max Jitter, Ave Audio Network Jitter, Max Audio Network Jitter, Ave Round Trip Time, Max Round Trip Time, Ave Packet Loss Rate, Max Packet Loss Rate, Ave Video Frame Rate, Ave Video Frame Loss perc, Low Frame Rate Ratio, Ave Bandwidth Estimate
- **Detected Quality Metric Incidents**
  - **Resource:** Assurance MsTeams Callrecord Session Stream Incidents
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSessionStreamIncidents
  - **Fields:** Callid, Sessionid, Media, Streamdirection, Incident
- **User, Call and Participant list**
  - **Resource:** Assurance MsTeams Callrecord
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecord
  - **Fields:** Organizer Displayname, Callid, Participant List, Participant Array, Audio Quality, Video Quality, Vbss Quality, Quality Info

15.3.75. Insights Microsoft Teams Direct Routing Call Analysis

Insights Microsoft Teams Direct Routing Call Analysis

Charts

- **Call Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
- **Top 10 Callee Number Based On Duration**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
- **Top 10 Caller Number Based On Duration**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
- **Top 10 Callee Number Based On Attempt**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
- **Top 10 Caller Number Based On Attempt**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
- **Call Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
- **Microsoft Teams Direct Call Routing Volume**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls

Tables

- **Call List**
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordDirectRoutingCalls
  - **Fields:** Invitedatetime, Calltype, User, UPN, Caller, Callee, Duration, Status, SIP Code, SIP Phrase, SBC
- **Top 100 Fully Qualified Domain Name Of The Session Border Controller**
  - **Resource:** Assurance MsTeams Callrecord Direct Routing Calls
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordDirectRoutingCalls
  - **Fields:** Session Border Controller, Call Count, Percentage Failed Call, Percentage Successful Call

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.76. Insights Microsoft Teams PSTN Calls

Insights Microsoft Teams PSTN Calls

Charts

- **Top Country Usage**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams PSTN Record IDs
- **Top 10 Caller Numbers**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams PSTN Record IDs
- **Top 10 Callee Numbers**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams PSTN Record IDs
- **Top PSTN Users**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams PSTN Record IDs

Tables

- **Call List**
  - **Resource:** Assurance MsTeams PSTN Record IDs
  - **drilldown-modelType:** data/AssuranceMsTeamsPSTNRecordIDs
  - **Fields:** Call Id, Calleenumber, Calltype, Callernumber, Userprincipalname, Calltype, Operator, Startdatetime, Enddatetime, Charge, Connectioncharge, Duration, Usagecountrycode, Calldurationsource

15.3.77. Insights Microsoft Teams Service Health

Teams Service Health as reported by Microsoft

Charts

- **Service Reliability Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Healthoverviews
- **Top 10 Active Service Events**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Issues
- **Top 10 Active Event Categories**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Issues
- **Incident Resolved Indicator**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Issues
- **Top 10 Active Feature Events**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Issues

Tables

- **Latest Cloud Service Status**
  - **Resource:** Assurance MsTeams Healthoverviews
  - **drilldown-modelType:** data/AssuranceMsTeamsHealthoverviews
  - **Fields:** Timestamp, Service, Status, service, lxt timestamp epoch
- **Microsoft Event List**
  - **Resource:** Assurance MsTeams Issues
  - **drilldown-modelType:** data/AssuranceMsTeamsIssues
  - **Fields:** Collection Time, Event ID, Title, Origin, Classification, Service, Feature Group, Feature, Start Time, End Time, Impact, Resolved, Status
- **Event Journal**
  - **Resource:** Assurance MsTeams Issues
  - **drilldown-modelType:** data/AssuranceMsTeamsIssues
  - **Fields:** Event ID, Posts, Origin

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.78. Insights Microsoft Teams Site Quality

Insights Microsoft Teams Site Quality

Charts

- **Site VBSS Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session
- **Site Video Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session
- **Site Audio Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Session
- **Site VBSS Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Session
- **Site Video Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Session
- **Site Audio Quality**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Session

Tables

- **Calls**
  - **Resource:** Assurance MsTeams Callrecord Session
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSession
  - **Fields:** Callid, Organizer Displayname, Caller Subnet, Callee Subnet, Caller Displayname, Callee Displayname, Audio Quality, Video Quality, Vbss Quality, Quality Info

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.79. Insights Microsoft Teams Usage Analysis

Microsoft Teams Usage Analysis

Charts

- **Calls Trend By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Meetings Trend By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Private Chat Messages By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Team Chat Messages By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Call Volume By Day**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Meetings Volume By Day**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Private Chat Message Volume By Day**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Team Chat Message Volume By Day**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Modality Duration Trend By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Modality Volume By Day**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Organized Meetings Volume By Day**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Organized Meetings By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Attended Meetings Volume By Day**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
- **Attended Meetings By Day**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day

Tables

- **Total Audio Modality Duration**
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
  - **drilldown-modelType:** N/A
  - **Fields:** Total Audio Duration (Sum)
- **Total Video Modality Duration**
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
  - **drilldown-modelType:** N/A
  - **Fields:** Total Video Duration (Sum)
- **Total Screen Share Modality Duration**
  - **Resource:** Assurance MsTeams Getteamsuseractivitycounts Day
  - **drilldown-modelType:** N/A

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Fields:** Total Screen Share Duration (Sum)

15.3.80. Insights Microsoft Teams User Experience Overview

Insights Microsoft Teams User Experience Overview

Charts

- **Platform Use**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
- **Reported Round Trip Time (sec)**
  - **Description:** Maximum network propagation round-trip time. Acceptable round-trip time is less than 500 msec.
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Stream
- **Reported Packet Loss Rate (perc)**
  - **Description:** Packet loss rate for the stream. Acceptable packet loss rate is less than 1perc.
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Stream
- **Reported Audio Jitter (sec)**
  - **Description:** Maximum of audio network jitter computed over each of the 20 second windows during the session. Acceptable threshold is less than 30 msec.
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Stream
- **Reported Jitter (sec)**
  - **Description:** Maximum jitter for the stream. Acceptable threshold is less than 30 msec.
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Stream
- **Audio Call Quality over Time**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord

Tables

- **User Device Details**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** User, Microphone, Speaker, Product, Platform

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Render Devices**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** Renderdevicename
- **Capture Devices**
  - **Resource:** Assurance MsTeams Callrecord Segment Participant Metrics
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordSegmentParticipantMetrics
  - **Fields:** Capturedevicename
- **User List - Choose a User to filter**
  - **Resource:** Assurance MsTeams Callrecord
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecord
  - **Fields:** Organizer Displayname

15.3.81. Insights Microsoft Teams User Review - Call Trends

Insights Call Trends

Charts

- **Microsoft Teams Calling Volume Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
- **Top 10 Most Active Participants on Microsoft Teams Calls**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
- **Top 10 Most Active Organizers on Microsoft Teams Calls**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
- **Microsoft Teams Modality Volume Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
- **Microsoft Teams Calling Duration Trend**
  - **Description:**
  - **Type:** chart-line

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
- **Microsoft Teams Modality Quality Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
- **Microsoft Teams Session Failure Trend**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant

Tables

- **Total Duration**
  - **Resource:** Assurance MsTeams Callrecord Reliability Modality Participant
  - **drilldown-modelType:** data/AssuranceMsTeamsCallrecordReliabilityModalityParticipant
  - **Fields:** Duration

15.3.82. Insights Microsoft User Usage Analysis

Insights Microsoft User Usage Analysis

Charts

- **User Activity Distribution**
  - **Description:** Shows the number of users with each activity rating. Active = current use, PT1M = last used 1 month ago, PT6M = last used 6 months ago
  - **Type:** chart-column
  - **Resource:** Assurance MsTeams Getteamsuseractivityuserdetail Latest

Tables

- **User Messaging Stats**
  - **Resource:** Assurance MsTeams Getteamsuseractivityuserdetail Latest
  - **drilldown-modelType:** data/AssuranceMsTeamsGetteamsuseractivityuserdetailLatest
  - **Fields:** User Principal Name, Private Chat, Reply, Team Chat, Urgent, Post
- **User Call Stats**
  - **Resource:** Assurance MsTeams Getteamsuseractivityuserdetail Latest
  - **drilldown-modelType:** data/AssuranceMsTeamsGetteamsuseractivityuserdetailLatest
  - **Fields:** User Principal Name, Calls, Audio Duration, Video Duration, Screen Share Duration
- **User Meeting Stats**
  - **Resource:** Assurance MsTeams Getteamsuseractivityuserdetail Latest
  - **drilldown-modelType:** data/AssuranceMsTeamsGetteamsuseractivityuserdetailLatest

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Fields:** User Principal Name, Ad Hoc Attended, Ad Hoc Organized, Meetings, Meetings Attended, Meetings Organized, Scheduled One Time Attended, Scheduled One Time Organized, Scheduled Recurring Attended, Scheduled Recurring Organized
- **Teams License utilization analysis for licensed users**
  - **Resource:** Assurance MsTeams Getteamsuseractivityuserdetail Latest
  - **drilldown-modelType:** data/AssuranceMsTeamsGetteamsuseractivityuserdetailLatest
  - **Fields:** Tenantname, User Id, User Principal Name, Report Refresh Date, Activity Rating, Last Activity Date, Last Activity Days, Assigned Products, Total Cost, Annual Cost, Is Licensed

15.3.83. Insights - Performance - Service Management

A collection of dashboards providing insights into Microsoft

Links

- **Microsoft Performance - Service Management**
  - Microsoft Teams Service Health
  - Microsoft Teams User Experience Overview

15.3.84. Insights - System Configuration

Insights Only System Configuration

Links

- **License Audit Setup**
  - Email Destinations
  - File Destinations
  - Cloud Licensing Service
  - SFTP Destinations
  - File Transfer Destinations
  - Audit Settings
  - Audit Report Files
- **Preferences and Defaults**
  - Global Settings
- **Customizations**
  - Model Filter Criteria

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.85. Insights - Usage & Adoption

A collection of dashboards providing insights into usage & adoption

Links

- **Microsoft Usage and Adoption**
  - Microsoft Teams Usage Analysis
  - Microsoft Teams User Review - Call Trends
  - Microsoft User Usage Analysis
  - Microsoft Teams Call Activity Trends

15.3.86. Insights - User & Device Inventory

A collection of dashboards providing insights into user & device inventory

Links

- **Microsoft User and Device Inventory**
  - Microsoft Teams Devices
  - Microsoft Teams Active Directory User List
  - Microsoft Teams Call Audio Device Detailed
- **Cisco Webex User and Device Inventory**
  - Insights Webex Devices
  - Insights Webex Licenses
  - Insights Webex Users
  - Insights Webex Locations and Workspaces

15.3.87. Insights Webex Calling

Insights Webex Calling

Charts

- **Call Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex CDR Feeds
- **Top Called**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex CDR Feeds
- **Top Calling**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex CDR Feeds
- **Top Inbound Trunks**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex CDR Feeds
- **Top Outbound Trunks**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex CDR Feeds
- **Call Releasing Party**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Assurance Webex CDR Feeds

Tables

- **User Drill down**
  - **Resource:** Assurance Webex CDR Feeds
  - **drilldown-modelType:** data/AssuranceWebexCdrFeeds
  - **Fields:** User
- **Calls**
  - **Resource:** Assurance Webex CDR Feeds
  - **drilldown-modelType:** data/AssuranceWebexCdrFeeds
  - **Fields:** Call Id, Start Time, Location, User, User Type, Calling Number, Client Type, Model, Call Type, Device Mac, Called Number, Called Line Id, Answered, Releasing Party, Redirecting Number, Redirect Reason, Original Reason, Inbound Trunk, Outbound Trunk, Duration

15.3.88. Insights Webex Devices

Insights Webex Devices

Charts

- **Number of Workspaces at each Location**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling Place
- **User Devices**
  - **Description:**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Type:** chart-line
  - **Resource:** Webex Calling Device Trend Metrics
- **Workspace Devices**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Webex Calling Device Trend Metrics
- **Webex Device Errors**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Device
- **Number of devices at each Location**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling Device
- **Webex Devices Trend**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Webex Calling Device Trend Metrics
- **Webex Devices Software Versions**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Device
- **Webex Devices Connection Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Device
- **Webex Devices By Type**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Device

Tables

- **Device Detailed Location**
  - **Resource:** Webex Calling Device
  - **drilldown-modelType:** relation/WebexDevice
  - **Fields:** Device Name, MAC Address, Device IP Address, Device Type, Workspace Name, Person Email, Customer, Site, Connection Status, Error Codes

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.89. Insights Webex Licenses

Insights Webex Licenses

Charts

- **Top 10 License Usage Percentage**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License
- **Webex Purchased Licenses**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License
- **Webex Consumed Licenses**
  - **Description:**
  - **Type:** chart-column
  - **Resource:** Webex Calling License

Tables

- **Webex Licenses**
  - **Resource:** Webex Calling License
  - **drilldown-modelType:** device/spark/License
  - **Fields:** Customer Name, License Name, Subscription ID, Purchased Licenses, Consumed Licenses, Percentage Licenses Used

15.3.90. Insights Webex Locations and Workspaces

Insights Webex Locations and Workspaces

Counters

- Number Of Workspaces
- Number of Locations

Charts

- **Workspace Capacity**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Place
- **Workspace Device Type**
  - **Description:**
  - **Type:** chart-pie

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Resource:** Webex Calling Place
- **Workspace Types**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling Place

Tables

- **Webex Locations**
  - **Resource:** Webex Calling Location
  - **drilldown-modelType:** relation/WebexLocation
  - **Fields:** Customer, Name, Timezone, Notes
- **Webex Workspaces**
  - **Resource:** Webex Calling Place
  - **drilldown-modelType:** relation/WebexTeamsPlace
  - **Fields:** Customer, Displayname, Type, Supporteddevices, Health

15.3.91. Insights Webex Meetings Quality

Insights Webex Meetings Quality

Charts

- **Webex Meeting Qualities QoS - Screen Share Out**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex Meeting Qualities QoS - Screen Share In**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex Meeting Qualities QoS - Video Out**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex Meeting Qualities QoS - Video In**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Audio Out - Packet Loss**

Copyright © 2025 VisionOSS Limited. All rights reserved.

  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Audio In - Packet Loss**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Audio Out - Latency**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Audio In - Latency**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex AudioOut - Jitter**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex Audio In - Jitter**
  - **Description:**
  - **Type:** chart-line
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex Meeting Qualities QoS - Audio in MOS**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Qualities QoS
- **Webex Meeting Qualities QoS - Audio out MOS**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Qualities QoS

Copyright © 2025 VisionOSS Limited. All rights reserved.

15.3.92. Insights Webex Participant

Insights Webex Participant

Charts

- **Top Hosts**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Assurance Webex Meeting Participants

Tables

- **User Meeting devices**
  - **Resource:** Assurance Webex Meeting Qualities
  - **drilldown-modelType:** data/AssuranceWebexMeetingQualities
  - **Fields:** Cameraname, Speakername, Microphonename, Clienttype, Clientversion, Hardwaretype, Networktype, Ostype, Osversion
- **WEBEX Meetings quality**
  - **Resource:** Assurance Webex Meeting Qualities
  - **drilldown-modelType:** data/AssuranceWebexMeetingQualities
  - **Fields:** Meetinginstanceid, Webexusername, Webexuseremail, Participantid, Ostype, Osversion
- **WEBEX Meetings quality**
  - **Resource:** Assurance Webex Meeting Participants
  - **drilldown-modelType:** data/AssuranceWebexMeetingParticipants
  - **Fields:** Id, Host, Displayname, Email, State

15.3.93. Insights Webex Users

Insights Webex Users

Counters

- Total Webex Users
- Users with Webex Calling
- Users with UCM Calling
- User Phones
- Users with Contact Centre License

Charts

- **User Status**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling User

Copyright © 2025 VisionOSS Limited. All rights reserved.

- **Login Enabled**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling User
- **Invite Pending**
  - **Description:**
  - **Type:** chart-pie
  - **Resource:** Webex Calling User

Tables

- **Webex Users**
  - **Resource:** Webex Calling User
  - **drilldown-modelType:** relation/SparkUser
  - **Fields:** Customer Name, Site, Date User was Created, Display Name, Email, First Name, Last Name, Nick Name, Login Enabled, Invite Status, Status, Calling Pro, Contact Center

15.3.94. selfservice_dashboard

Links

- **My Details**
  - My Details
  - My Transactions
- **My Phones**
  - Product
- **My Lines**
  - Pattern

Copyright © 2025 VisionOSS Limited. All rights reserved.

16. Appendix: Glossary

16.1. Glossary

1ESS
Number One Electronic Switching System

1FR
Flat rate service

2 5G
Enhanced 2G mobile telephone

2G
Second generation mobile telephone

3G
Third generation mobile telephone

4WTS
Four-wire termination set

A number
Calling number. The number of the party initiating a call. See also B number.

AC
Agile Commit

Access Profile
Customizable component in Automate.

Accessibility
For software systems, refers to guidelines issued by the World Wide Web Consortium (W3C) to remove barriers, via code and design, that prevent or make it difficult for people with disabilities to use online sites and tools.

ACD
Automatic Call Distribution - Director

ACTS
Advanced Coin Telephone Service

AD
Active Directory

ADSL
Asymmetric Digital Subscriber Line

Agent
Insights agents, lightweight synthetic testing bots connected to the Arbitrator for monitoring UC apps and other business apps.

AMA
Automatic Message Accounting

Analytics
An Insights solution. Insights Analytics delivers powerful log analytics with no data collection caps or scale limitations. Insights Analytics comprises Dashboard, Arbitrator, and optionally, Windows Forwarder

ANI
Automatic Number Identification

API
Application Programming Interface

Arbitrator
Insights Arbitrator is a log analytics platform that allows multiple data sources and log formats to be consumed, extracted, analyzed, and correlated, for complete event, alarm and systems monitoring.

Associated
Associated phone. An associated phone is linked to a user. The phone's linked user is then associated with the phone's number.

Assurance
An Insights solution. Insights Assurance provides business performance intelligence, allowing monitoring of UC apps with log analytics and customizable alerts, and comprises the the Dashboard and Arbitrator applications, with optional integrations for Automate, Avaya, and Windows Forwarder.

Auto Attendant
An automated (auto) attendant system that transfers telephone calls to the extension of a user or department without the intervention of a receptionist or operator. This is achieved via a system of voice menus that the person initiating the call interacts with via their telephone keypad or via voice commands. In some auto attendant systems, there are message-only information menus and voice menus that are used so that an organization can provide business information such as hours, directions to their premises, information about job opportunities, and answer other frequently-asked questions. After the message has played, the caller can be forwarded to the operator or they can return to the main menu.

Automate
The Automate system, a business and vendor agnostic solution focused on digital office management and unified communication (UC), able to integrate with any external application that includes APIs.

AXL
Administration XML (AXL) interface supporting multiple AXL schema versions, which provide an abstraction layer between AXL Applications and the Unified CM database. Also, Cisco AVVID XML (AXL) server, a component of Cisco CallManager. The AXL server enables the Cisco EGW to identify and monitor individual end-user lines required for DPNSS supplementary services such as call back and extension status.

B number
Called number. The number of the party receiving a call. See also A number.

BAP
Business Admin Portal

BAT
The file name extension for a batch file (.bat). Also, a phone template (BAT phone template), or the

Copyright © 2025 VisionOSS Limited. All rights reserved.

recommended device name prefix in Automate when provisioning phones with a fake MAC address

BC
Business Commit

BKEY
Business key

BOK
Unblocking

BU
Business Unit

Camelot
SIP call load generator used to make SIP calls. Used to create load for UCM and UCxn.

CC
Country code

CCCE
Cisco Contact Center Express. Contact center solution, also known as Cisco Unified Contact Center Express (UCCX), designed for mid-market enterprise branch or corporate departments requiring a sophisticated customer interaction management solution for up to 300 agents.

CCIS
Common Channel Interoffice Signaling

CCM
Cisco CallManager. Call process software, also known as Cisco Unified Communications Manager, or UCM.

CDET
Cisco Defect and Enhancement Tracking system for HCS.

CDR
Call Data Records. Also, Call Detail Record

CEL
Cisco Enterprise Linux Cisco Testbeds

CEPB
Communications Enabled Business Processes

CEPM
Cisco Enterprise Policy Manager, used for managing entitlement.

CER
Cisco Emergency Responder. Used for filling out information to route emergency calls.

CF
Call forward

CFD
Customer Found Defect

CFT
Configuration Template

CIA
Change Impact Analysis

CID
Caller ID

Copyright © 2025 VisionOSS Limited. All rights reserved.

CIPC
Cisco IP Communicator, a soft client (which looks like a phone) on PC for voice

Cisco Emergency Responder
Also known as CER, a server that ensures that the Cisco Unified Communications Manager (Unified CM) sends emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes.

Cisco SRST
Cisco Secure Survivable Remote Site Telephony, a disaster mitigation technology.

Cisco Unified Presence
Also known as CUP, a standards-based platform that collects information from multiple sources about user availability and communications capabilities to provide rich presence status and facilitate presence-enabled communications with Cisco Unified Communications and other critical business applications.

Cisco36xx
A Cisco 36xx Series Router

CLI
Command-line interface. Also short for Caller ID (Caller Line Identification).

CLID
Caller ID / Caller Line ID

CLIP
Calling Line Identification Presentation

CLIR
Calling Line Identification Restriction

Cluster ID (CID)
An ID assigned to each Cisco Unified Communications Manager PBX cluster in the system. This is configurable when adding the cluster and can be viewed on the cluster details page.

Contact Center
A hardware and software solution that involves the intelligent routing of all contacts, call treatment, and general contact management over a multichannel IP infrastructure. Contact Centers often contain functionality to enable automatic call distribution functionality that interfaces with an organization's unified communications solution.

CoS
Short for Class of service. The term refers to a Calling Search Space (CSS) that is specifically used to define call routing and feature processing for a line or a phone.

COSI
Cisco Open Source Initiative

COSMOS
Wire records

CPID
Call processing identifier (unique system-wide). First part of the FINT. The CPID and RID need to be unique within a provider. This is assigned to hardware as required (e.g. PBX, PGW, Voicemail, etc). The CPID is generally configurable when adding the hardware and is displayed when viewing the settings.

CR
Change Request

Copyright © 2025 VisionOSS Limited. All rights reserved.

CRUD
Short for Create Read Update Delete

CSF
Client Service Framework

CSM
Cisco Security Manager

CSP
Communications Service Provider

CSS
Calling search space

CSV
Short for Comma-separated Values

CT
Call type

CTI
Computer telephony integration, also called computer-telephone integration or CTI, is technology that allows interactions on a telephone and a computer to be integrated or co-ordinated. As contact channels have expanded from voice to include email, web, and fax, the definition of CTI has expanded to include the integration of all customer contact channels (voice, email, web, fax, etc.) with computer systems.

CUAE
Cisco Unified Application Environment, an application development environment for developers.

CUBE
Cisco Unified Border Element. Cisco IOS Session Border Controller (SBC) that interconnects independent voice over IP (VoIP) and video over IP enterprise networks for data voice and video transport. CUBE is an integrated Cisco IOS Software application that runs on the Cisco 2900/3900 and 2800/3800 Series Integrated Services Routers (ISRs), the Cisco AS5350XM/AS5400XM universal gateways and the ASR 1002/1004/1006 routers.

CUC
Short for Cisco Unity Connection

CUC (CUCXM)
Cisco Unity Connection. Voice mail system

CUCCE
Cisco Unified Contact Center Enterprise. Call center management.

CUCCX
Cisco Unified Contact Center Express

CUCDM
Cisco Unified Communications Domain Manager.

CUCI
Cisco Unified Communications Integration. See also CUCIMOC.

CUCIMOC
Cisco Unified Communications Integration for Microsoft Office Communicator. Requires Microsoft OCS & Office Comm AD; Cisco UCM provides call control click to dial phone status.

CUCM Local
UCM local user, a user managed directly within Cisco UCM. Their authentication and user information

Copyright © 2025 VisionOSS Limited. All rights reserved.

are stored locally in UCM. In Automate these users display as “CUCM Local”, and on UCM these users display as “Enabled Local User”. Users can be converted from CUCM-LDAP to CUCM local users. This conversion is typically required when a user has been deleted from the LDAP server, and the UCM has synced with the LDAP server, setting the user to “Inactive”. Converting the user to a UCM local user prevents the user from being automatically deleted during the Garbage Collection process on the UCM.

CUCM-LDAP User
A UCM-LDAP user in the Automate system refers to a user whose information is synced from an LDAP directory to the Cisco Unified Communications Manager (UCM).

CUCMBE
Cisco Unified Communications Manager Business Edition. VOIP PBX.

CUCX
Cisco Unified Contact Center Express. See also CCX or UCCX.

CUE
Cisco Unity Express. Linux based, runs on ISR blade; voice mail

CUEA
Cisco Unified Expert Advisor. Routes call to agents based on expertise

CUIS
Cisco Unified Intelligence Suite

CUMA
Cisco Unified Mobility Advantage. Mobile Client

Cisco Communications Manager Appliance. In a Network server and communicates to Smart Phone Client CUMC and SIP to UCM

CUMC
Cisco Unified Mobile Communicator. Client in a smart phone for connection to CUMA - SIP to UCM

CUMP
Cisco Unified Meeting Place (similar to WebEx).

CUnM
Cisco netManager Unified Communications. Part of the UC management suite.

CUOM
Cisco Unified Operations Manager. Part of the UC management suite.

CUP
Cisco Unified Presence. Presence Server.

CUPC
Cisco Unified Personal Communicator. UC PC soft client.

CUPM
Provisioning Manager. Part of the UC management suite.

CUPS
Short for Cisco Unified Presence Server. Provides Presence Status.

CUSM
Cisco Unified Service Monitor. A service monitor.

CUSSM
Cisco Unified Service Statistics Monitor. Service statistics.

Copyright © 2025 VisionOSS Limited. All rights reserved.

CUVA
Cisco Unified Video Advantage. Screen video with phone PC app

CUVC
Cisco Unified Video Conferencing. Video conferencing server bridge

CVP
Cisco Voice Portal. Call center scripts.

Dashboards
Insights Dashboard server ships with standard, read-only templates called VOSS Reference Dashboards. Insights dashboards are configured to display data that provides statistics for the system. Customers can use the reference dashboards as shipped, or clone and edit the dashboards to create custom dashboards. Insights Dashboards are based on search definitions that extract data from one or more fields. These may be predefined search definitions that ship with the default dashboards, or definitions that you set up to create custom views of the data to meet the needs of your organization.

Dashboards are also available in Automate.

DDCO
Direct Dial Central Office (Opposite of DID)

DDD
Direct Distance Dialing

DDI
Direct Dial Inward (same as DID).

DECT
Digital Enhanced Cordless Telecommunications

DEM
Digital Experience Monitoring

Device Model
Device model of the Automate database includes a copy of the structure and data from each of the UC apps that Automate integrates with (for example, UCM, Microsoft Teams, LDAP, Microsoft Graph, CUCX, Webex Teams). Each device model resides in a subsection dedicated to the UC app source it belongs to. The data in the device model is always considered a copy only, whereas the source UC app is the data master. Data models are owned and managed by Automate. See also, “Views”, “Relation Models”, “MongoDB”.

DHCP
Dynamic Host Configuration Protocol. Used to perform basic configuration of computer systems, usually at boot time. May be used to set network parameters such as IP address, subnet mask and host name.

Dial plan
A dial plan establishes the expected number and pattern of digits for a telephone number, including country codes, access codes, area codes, extension numbers and all combinations of digits dialed. Dial plans must comply with the telephone networks to which they connect.

Dialplan
Defines the number construction rules

DID
Direct Inward Dialing (US term for DDI).

Digital Experience Monitoring
Also known as DEM, Digital Experience Monitoring is deployed to do front door testing to test connectivity to web-based systems, such as Microsoft Teams. DEM is deployed in the Arbitrator to display data

Copyright © 2025 VisionOSS Limited. All rights reserved.

in the Dashboard when alerts and alarms are raised for DEM collected metrics that are out of permitted thresholds. For Insights, DEM can deliver metrics such as overall round trip times to the application, the amount of hops taken, best and worst latency, the connection path (shown hop-by-hop).

Directory Number Routing
DNR, or Directory Number Routing, allows an administrator to make their DN inventory inter- and intra-site routable by adding the necessary translation patterns on Cisco Unified Communications Manager (UCM) when deploying a non-SLC-based dial plan. Normally, for the SLC-based dial plans, because each site requires a unique SLC, these translation patterns can automatically be deployed. This is not the case for non-SLC (flat) dial plans. In this case, DNR instances can be created when DN inventory is added to make these internally routable.

DMS
Digital Multiplex System

DN
Short for Directory Number. This number can be assigned to a user and can be dialed. A DN may be composed of an extension prefix and/or a site location code and/or extension, but the DN is the final form of the internal dialable number. The DN is not the E.164 number, although they may coincide.

DN Inventory
Short for Directory Number Inventory. A list of directory numbers (DNs) configured in Automate that can then be used in a line configuration. The DN inventory resides only in Automate and is not pushed to Cisco Unified Communications Manager (UCM). DNs may also be used as feature pilot numbers (for example, Hunt Pilot or Call Pickup patterns). When used as a service number, the DN is marked as unavailable and it cannot be used in a line configuration. DN inventory is configured at the Site or Customer hierarchy level. However, to configure DN inventory at a customer hierarchy, the customer dial plan must be configured not to use site location codes ("flat dial plan").

DNIS
Dialed Number Identification System

DP
Short for Dial plan

DPCODE
Dial Peer Code

DPNSS
Digital Private Network Signaling System.

Drop account
The Insights Dropbox (drop) account is used for install and upgrade. The username is "drop". By default, the password is not set and can be set up via the CLI Administration menu (Change Dropbox Password).

DSL
Digital Subscriber Line

DTMF
Dual-tone multi-frequency. A method for instructing a telephone switching system of the telephone number to be dialed. This is done by sending pairs of tones down the line.

E.164 Associations
E.164 Associations allow the customer's DNs to be reachable from the PSTN network (DDI routing). The Administrator creates an E.164 (PSTN)-to-DN (internal extensions) association to provide the DDI mapping.

E.164 Inventory
A list of E.164 (E164) numbers configured at a site hierarchy. This list only resides in Automate and is

Copyright © 2025 VisionOSS Limited. All rights reserved.

not pushed to Cisco Unified Communications Manager (CUCM, or CallManager).

E.164 Number
The globally routable phone number that includes country code and country-specific format. This number is used for offnet Public Switched Telephone Network (PSTN) calls. E164 numbers must always be unique and the local PTT should ensure that the same number ranges are not given out twice.

E164
Also E.164. ITU-T recommendation defining PSTN numbering plan E164.

ECE
Early Customer Engagement

EDRs
Event Data Records

EISUP
Extended ISDN User Part

ELIN
Emergency Location Identification Number

EMCC
Short for Extension Mobility Cross Connect

EOL
End of line. Variable used by the system to determine the end of line in each model.

ER
Emergency Release. The term used to describe an ES by VOSS.

Events
Configurable tool in Automate. A condition or trigger that drives a certain behavior, activity, workflow, or steps within a workflow in Automate. Available only to the VOSS team.

EXT
Extension and external prefix

EXTN
Extension Final part of the FINT

FAC
Short for Forced Authentication Code

FDM
Frequency-division multiplexing

FDP
Field Display Policy. GUI rules that define how fields display and behave.

FINT (fint)
Full Internal Number, CPID + RID + SLC + EXTN = Cisco Unified CM DN. This is the full internal number the system knows the lines as. The construct of this is defined in the number construction rules. When a location is added, the full fint inventory is created for the location.

FNN
The full national number (PSTN number). The E164 telephone number without area code

Garbage Collection
An internal, scheduled service on Cisco Unified Communications Manager (UCM) that removes, for example, inactive users. In Automate, converting a user from CUCM-LDAP to CUCM Local is typically required when the user is deleted from the LDAP server, the UCM has synced with the LDAP server,

Copyright © 2025 VisionOSS Limited. All rights reserved.

and the user is set to “Inactive”. In this scenario, the user is deleted when the Garbage Collection process runs on the UCM. Converting the user to a UCM Local user prevents the user from being automatically deleted.

GDPR
Short for General Data Protection Regulation

Generic Driver
The Automate core element, a tool that can learn the structure and detail of external APIs to create the models reflecting the UC app integrated with Automate as device models, and enables Automate to reflect the external system structure and offer feature parity. The creation of the device models automatically creates a Automate API for each model. These APIs are used by the Automate interface and bulk loaders and can also be used for external integration.

GK
Gatekeeper

Glassfish
Open Source Application Server

GPRS
General Packet Radio Service

GSM
Global system for mobile communications

GUI
Graphical user interface

GUI Rules
Configurable tool in Automate governing the behavior of the Automate interface, such as the display of drop-down lists, or the dependency between fields (for example, where the value selected in one field defines whether another field displays). Available only to the VOSS team.

GW
Gateway

H - M-UCS
Hosted - Managed-Unified Communications Solution

H 323
ITU - T umbrella recommendation defining audio-visual protocols on a packet network H323 Protocol.

HCS
Short for Hosted Collaboration Solution.

HN
Hierarchy Node

HOST
Hand Over System Test

Hosted UCS - HUCS
This setting does not apply to Cisco HCS.Short form of Hosted Unified Communications Services. An abbreviation of M - HUCS.

HSI
H323 Signaling Interface

HUCS
This setting does not apply to Cisco HCS.Short form of Hosted Unified Communications Services - HUCS is a comprehensive, converged IP communications system of data, voice, video, and mobility

Copyright © 2025 VisionOSS Limited. All rights reserved.

applications, enabling more effective and secure personal communications that directly affect both sales and profitability.

Hunting
Hunt Group
Hunting, or a hunt group, is a telephony concept that refers to the concept of distributing phone calls from a single telephone number to several phone lines. A number of different hunt methods exist that can be configured depending on the organizations needs and requirements. The most common hunting methods include multi-line hunting, linear hunting, circular hunting and most-idle hunting.

ICPID
Call processing identifier, IPPBX-based

IDDD
International Direct Distance Dialing

Idle URL
An Idle URL can be seen as a form of advanced screensaver. When a phone has been not received user input for a configurable amount of time (URL Idle Time Parameter), the system will perform a HTTP GET for the URL in the URL Idle field and will then display the contents of the URL on the phones screen. This content can be anything from an organizations logo to more advanced data such as a weather forecast or company updates.

IDP
Identity Provider

ILEC
Incumbent Local Exchange Carrier

IM
Instant messaging

IMACS
IMACs stands for Installs, Moves, Adds and Changes. It covers the administration for: Installing new Customers, Locations, Users and Phones; moving Users and Phones; Adding Users and Phones and changing the Features and Services used for Users and Phones.

IMAP
IMAP load generator: Used to generate IMAP traffic for UCxn.

IMP
Interface Messaging Processor

INI
Internal Number Inventory

Inventory
When a phone is initially entered into the system, it is added as an inventory item in the Service Providers warehouse. The Device Name and type are the only things known about this Phone. Over time, the phone will be allocated initially to a Reseller, who in turn will allocate it to a Customer. It is still an inventory item. It does not become a provisioned phone until it has been allocated to a Location.

IOS
Internetwork Operating System is an operating system from Cisco that is the primary control program used on Cisco Routers and devices. IOS is widely used and is robust system software that supports the common functions of all products under Cisco's CiscoFusion architecture.

IP
Internet Protocol

Copyright © 2025 VisionOSS Limited. All rights reserved.

IP Addressing
IP Addressing should be unique, however, where two Customers have chosen the same private IP address ranges for their locations, NAT will be required to ensure that IP addresses within the system are unique.

IPCBU
IP Communications with a key focus on UCM and IP phones.

IPT
Internet Protocol Telephony (IP Telephony)

ISC
The Cisco IP Solution Center (ISC). A security management solution from Cisco.

ISD
International Subscriber Dialing

ISDN
Integrated Services Digital Network

ISP
Inter-site prefix

ISUP
ISDN user part

ITU-T
International Telecommunications Union - Developer of global info-communications standards

IVR
Interactive voice response

JSON
A language independent, lightweight data interchange format that was initially introduced for Javascript. JSON is commonly used for APIs and data storage, and is the standard format for presenting data from the Automate database. Depending on their access rights, high level Automate admins have the abilility to view the data on every page in Automate in JSON format. Some Automate pages provide a JSON Edit option via the Automate toolbar. The JSON Editor displays all the attributes of the model and their order in the model, and allows the admin to update field values via the editor instead of the GUI.

LDAP
Lightweight Directory Access Protocol

LEPN
Location Emergency Published Number

Line / Line Relation
In the context of the Shared Lines Across Sites feature, the line or line relation is the line configured via the Lines page, which is pushed to Cisco Unified Communications Manager (UCM). A line is also pushed to UCM when it is referenced in a phone, extension mobility profile, or single number reach profile, and doesn't already exists on the Cisco UCM. On Cisco UCM, a line corresponds with the items under menu Call Routing > Directory Number. It is also called a "line relation" because this is the technical term for the construct within Automate.

Line Appearance
A line appearance is the assignment of a line to a phone. One line can have many line appearances. If a line has more than one line appearance, it is considered a shared line.

Location Name
The Location name must be unique within a Customer. A naming convention is recommended,

Copyright © 2025 VisionOSS Limited. All rights reserved.

where a suffix is added to the location name that contains a reference to the Customer, for example, nsydney_cisco, Location names can be re-used within different Customers.

Logged on
Only a phone that has Extension Mobility Support can be logged onto by a user using a User Mobility profile. Once logged-on, the phone adopts the profile of the Mobile User and drops their registered number and profile.

LRID
Routing identifier, location-based

M - HUCS
Managed Hosted Unified Communications Service

MAC
Message Authentication Code

MAC Address
A Media Access Control address (MAC address), is a unique identifier assigned to network devices by their manufacturers. They are used for identification and in the Media Access Control protocol sub layer. MAC addresses are unique by their very nature.

MACD
Short for Move, Add, Change, Delete. MACD operations on services in enterprise communications.

Macro Functions
Predefined utilities performing calculations, used for configuring macros.

Macros
Customizable components in Automate.

MDF
Main Distribution Frame

Menu
Customizable component in Automate.

MF
Multi-frequency

MGCP
Media Gateway Control Protocol

MML
Man-machine language

MOH
Music on Hold

MongoDB
The main database used by Automate, MongoDB is a hierarchical database, organized in several sections, each with their own use. The structure of data held is referred to as models.

Movius
Movius is a leader in carrier-grade media servers, application servers and real-time multimedia applications for IP and TDM networks.

MT
Multi-tenant

MVS
Multi vendor user

Copyright © 2025 VisionOSS Limited. All rights reserved.

MWI
Message waiting indicator

NANP
North American Numbering Plan - a dial plan based on 3-digit area codes and 7-digit telephone numbers used by 24 countries in North America and the Caribbean.

NAT
Network Address Translation - A standard that enables a local area network (LAN) to use one set of IP addresses for internal network traffic and a second set of addresses for external traffic.

NDL
Network Device List

NDLR
Network Device List Reference

NetFlow
An Insights solution, comprising DS9 and Dashboard applications. Insights NetFlow provides the architecture to allow visualization and analysis of network traffic flow data.

Netwise
A Netwise CMG Telephony Server

Network Observability
An Insights feature, configured in Arbitrator via probe scripts that collect data from the customer's network devices, and which data is displayed for analysis purposes via two standard, read-only Network Observability dashboards for the Analytics solution, in the Dashboard system.

NGN
Next Generation Network

NOA
Nature Of Address

NSITE
Solution Testing primarily used for verifying HCS as a solution and scale testing.

NTP
Network Time Protocol. Used to synchronize computer system clocks to a high degree of accuracy.

OCS
Online Charging System, a system allowing Communication Service Providers to charge their customers, in real time, based on service usage.

OSS
Operations Support Systems

Overbuild
Overbuild is a Automate feature that allows you to integrate with a customer's xisting UC infrastructure.

PABX
Private Automated Branch Exchange, often shortened to PBX.

PAI
P-Asserted-Identity

PAT
Port Address Translation. A form of network address translation whereby each IP Address on the LAN is translated to the same IP address but each with a different port.

PBT
Phone Button Template

Copyright © 2025 VisionOSS Limited. All rights reserved.

PBX
Private branch exchange. Digital or analog telephone switchboard located on the user premises and used to connect private and public telephone networks

PCC
Padded Country Code

PGW
Packet Gateway. IP to TDM / PSTN networks

PGW Cisco Transit switch
The Cisco PGW (Protocol Gateway) is a multi-protocol, carrier-grade soft-switch designed to support media gateway control functions and interworking in next-generation networks (NGNs).

Phone MAC Address
See the MAC Address glossary entry for a full explanation of a MAC address. By their very nature, all Phone MAC addresses in the system are unique.

Pilot Number
A pilot number is an address or location within a PBX or IP-PBX and is generally defined as a blank extension number or an extension that does not have a person or telephone associated with it. Without a defined pilot number, the PBX or IP-PBX cannot locate where the incoming call was received. Pilot Numbers are used in the system for a number of services such as Hunt Groups and Voicemail services.

PIN
Personal Identity Number

PLAR
Private Line Automatic Ringdown

PMBX
Private Manual Branch Exchange

PNOC
Cisco Proactive Network Operations Center

PostgreSQL
The relational database used by Insights and which holds a managed copy of some of the data from MongoDB. Data in PostgreSQL is organized in tables and is referred to as resources. Charts and other analysis options in Automate dashboards draw their data from this database.

POTS
Plain Old Telephone Service

PRD
Product Requirements Definition

PRI
Primary Rate Interface. ISDN interface to primary rate access

Provisioned
Once a phone has been moved into a Location and into a specific subnet, the system allocates an IP address to the phones MAC address. If that phone is physically connected to the correct VLAN in the Location, then it will be automatically provisioned with the allocated IP address.

Provisioning Workflows
The mechanism managing processes and tasks in the order specific to the provisioning needs and business requirements in Automate.

PSB
Product Security Baseline

Copyright © 2025 VisionOSS Limited. All rights reserved.

PST
Product Specification Tool

PSTN
Public Switched Telephone Network

PT
Partition

PTT
Push to Talk

Public Holiday
Public holidays are often referred to as Bank Holidays, National holidays, Federal Holidays and Vacations. Public Holidays are days that have been declared by a national, or sometimes local, authority to be non-working days. Public holidays are usually declared as an official observance of a religious, national, or culturally significant event. The impact on business is that businesses may be closed for business on days that would traditionally be trading days, for example Monday to Friday. Public holidays on days that are traditionally days of rest, tend to have a lesser impact on business.

PWF
Provisioning Workflow

QAG
Quick Add Group

QAS
Quick Add User

QoS
Quality of Service

QS
Quick User

QSIG
Q Signaling (ISDN-based protocol for signaling between PBXs)

RBAC
Role Based Access Control

RCMAC
Recent Change Memory Administration Center

RD
Short for Remote Destination

RDP
Remote Destination Protocol

Registered
Only a provisioned phone can be registered. The registering process provides the phone with a telephone number and a configuration file. Only a registered phone can operate as a normal phone and can make and receive calls.

Relation
Relation model, a logical arrangement of multiple models in Automate, usually combining two or more device and data models. The anchoring model for the relation to which all other models in this relation are linked is called the “left hand model”. The left hand model controls the model summary information, that is, it is the source of the data shown in the lists. Most lists in Automate showing rich data are relation models.

Copyright © 2025 VisionOSS Limited. All rights reserved.

REN
Ringer Equivalency Number

RL
Short for Route List

ROI
Return on Investment

Role
Configurable component in Automate.

Routing ID (RID)
This is configurable as to whether it is a customer level or location level ID. Although it is configurable, if anything other than Location is selected you will likely have problems. This ID is selected for a location and is unique for the CPID In the case of a location, the RID could be an available rid for the CPID of the IPPBX of the location.

RTMT
UC application monitoring tool for viewing performance counters and alerts/alarms.

SAS
Solution Architecture Specification

SBC
Session Border Controller.

SBR
Scale Based Regression. Performance related

SCCP
Skinny Client Control Protocol

SCTP
Stream Controlled Transmission Protocol.

SDD
Short for Site Defaults Doc

SDL
Software Development Lifecycle

SDP
Service Delivery Platform

Service Activation
The technical process of creating, delivering, and managing a service to or for a customer. It generally involves the configuration of multiple products (for example dial-tone, voice mail, conferencing, corporate directories and XML applications) for the one service.

Session Border Controller
Also known as SBC, Session Border Controller devices are deployed at the network edge and at carrier interconnects (between users and other service providers). SBCs help secure and manage traffic in and out of enterprise carrier networks, as well as facilitating communications between incompatible signaling messages and media flows (sessions) from end devices or application servers.

SF
Single Frequency supervision tone (2600)

SIP
Session Initiation Protocol (SIP). A signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet.

Copyright © 2025 VisionOSS Limited. All rights reserved.

SIPp
Used to generate SIP traffic for CUP.

Site Code
A location level code assigned for each location in the system. This is required if you wanted more than a single location in the system (as the fint needs to be unique). The site code inventory is managed per customer in the system. The length of the site code is always allowed to be variable with a defined maximum length. Overlapping site codes are not allowed within a customer - if a site code of 1 was defined, then a site code of 12 would not be allowed.

Site defaults
Site defaults allow you to provide default values that apply at site level for configuration required when onboarding customers and users.

SLC
Site location code (unique within a customer). Penultimate part of the FINT.

SLC-based Dial Plan
A site location code (SLC)-based dial plan is one that uses unique, site-specific dialable location codes that are embedded in the DN along with the extension. For example, the default Type 1 through Type 3 Cisco dial plans are SLC-based. Only the Type 4 dial plan is not SLC-based. Type 4 dial plan is commonly referred to as a “flat” dial plan because DNs are the actual extensions. In the context of the Shared Lines Across Sites feature, this distinction between types of dial plans is important because to support the Shared Line Across Sites, where devices at different sites can share a line that supports intra/intersite dialing from every site, an SLC would not allow a line to span multiple sites (because multiple sites can’t have the same SLC). The Shared Line Across Sites feature requires the customer to deploy a non-SLC based dial plan.

SM
Session Manager.

SME
Cisco Session Manager Edition, a transit switch used to aggregate multiple unified communications systems, referred to as leaf systems.

SMS
Short Message Service. Also known as text messages.

SMTP
Simple Mail Transfer Protocol. Internet protocol providing e-mail services

SNMP
Simple Network Management Protocol. Network management protocol used in TCP/IP networks

SNR
Single Number Reach

SOAP
Simple Object Access Protocol

SP
Service Provider

SP Lock
Unlocking

SRND
Solution Reference Network Design

SRST
Survivable Remote Site Telephony. Limited call functionality when losing WAN connection

Copyright © 2025 VisionOSS Limited. All rights reserved.

SS7
Signaling System 7

SSO
Short for Single Sign-on

STD
Subscriber Trunk Dialing

SVC
Service

T-CXR
T carrier

TAC
Techincal Assistance Center

TAPI
Telephony Application Programming Interface

TCO
Total Cost of Ownership

Technician Server
A server that is not managed by the system, but rather directly by a technician.

The system
A term used in the documentation to refer to the application and its related hardware and software components.

Themes
Customizable component in Automate.

TLS
Transport Layer Security

TOD
Time of Day

TOI
Transfer of Information

TSPS
Traffic Service Position System

TXE
Telephone Exchange Electronic

TZ
Timezone

UAX
Unit Automatic Exchange

UC
Short for Unified Communications. Product suite.

UC SDP
Unified Communications Service Delivery Platform

UCaaS
Unified Communication as a Services, for hosted and managed IP Telephony, offers a proven end-to-

Copyright © 2025 VisionOSS Limited. All rights reserved.

end integrated reference architecture for Unified Communications and IP telephony services, specifically targeting large, Enterprise and Service Provider deployments.

UCBU
UCNX (Voice Mail) CUP (Presence) Mobile Clients Soft Clients Servers for these

UCCE
Unified Contact Center Enterprise. ACD Automatic call distribution

UCCX
Cisco Unified Contact Center Express. See also CUCX or CCX.

UCM
Short for Cisco Unified Communications Manager, Cisco's collaboration infrastructure for voice and video calling, messaging, and mobility. Also known as Cisco UCM.

UCNX
Unity Connection. Linux server-based unified messaging application.

UCS
Unified Computing System. Cisco servers to replace HP.

Unified Mobility
Cisco Unified Mobility

Unified Presence
Cisco Unified Presence

Unity
Cisco Unity is a powerful Unified Communications solution that provides advanced, convergence-based communication services such as voice and unified messaging on a platform that offers the utmost in reliability, scalability, and performance.

UnmanagedPBX
Un-managed PBXs are often used as parent components for a location.

URI
Uniform Resource Identifier

User Name
A unique name for a user across all customers. While Last Name and First name can be the same, User Name must be unique across all Customers. Hence, we recommend adding a domain suffix to user names, such as cmay_cisco_ns, where the suffix is an abbreviation for Cisco North Sydney location. Alternatively, the user name can be the same as the user phone number (DDI). This ensures that the user name is always unique.

View
A framework model in Automate without any actual data, used to collect information and initiate processes. For example, when opening a link in the Automate GUI that opens a page and not a list, this is a view model.

VM
Voicemail

VMware
VMware and its client software, used to manage virtual machines and UCS blade configuration. Also used to monitor performance statistics at the hardware level.

VOIP
Voice over Internet Protocol

Copyright © 2025 VisionOSS Limited. All rights reserved.

VPAT
Voluntary Product Accessibility Template, a template to assess the accessibility compliance of a site.

VQManager
Tool used to monitor jitter in the network. Jitter monitoring is important to UCxn.

WAP
Wireless Access Point / Wireless Application Protocol

WATS
Wide Area Telephone Service

WCS
Wireless Control System

WebEx
A Cisco application for meetings, messaging, and events.

WLA
Cisco Wireless Location Application

WLC
Cisco Wireless LAN Controller

WTAI
Wireless Telephony Applications Interface

XML
Extensible Markup Language

Copyright © 2025 VisionOSS Limited. All rights reserved.

Index

Symbols

1ESS, **1715**
1FR, **1715**
2 5G, **1715**
2G, **1715**
3G, **1715**
4WTS, **1715**

A

A number, **1715**
AC, **1715**
Access Profile, **1715**
Accessibility, **1715**
ACD, **1715**
ACTS, **1715**
AD, **1715**
ADSL, **1715**
Agent, **1716**
AMA, **1716**
Analytics, **1716**
ANI, **1716**
API, **1716**
app
    app install list, 526
    app install pbr, 526
Arbitrator, **1716**
Associated, **1716**
Assurance, **1716**
Auto Attendant, **1716**
Automate, **1716**
AXL, **1716**

B

B number, **1716**
BAP, **1716**
BAT, **1716**
BC, **1717**
BKEY, **1717**
BOK, **1717**
BU, **1717**

C

Call Park Management, 716
Camelot, **1717**
CC, **1717**
CCCE, **1717**
CCIS, **1717**
CCM, **1717**
CDET, **1717**
CDR, **1717**
CEL, **1717**
CEPB, **1717**
CEPM, **1717**
CER, **1717**
CF, **1717**
CFD, **1717**
CFT, **1717**
CIA, **1717**
CID, **1717**
CIPC, **1718**
Cisco Emergency Responder, **1718**
Cisco SRST, **1718**
Cisco Unified Presence, **1718**
Cisco Webex (*Feature*), 412, 623
Cisco36xx, **1718**
CLI, **1718**
CLID, **1718**
CLIP, **1718**
CLIR, **1718**
Cluster ID (*CID*), **1718**
Contact Center, **1718**
CoS, **1718**
COSI, **1718**
COSMOS, **1718**
CPID, **1718**
CR, **1718**
CRUD, **1719**
CSF, **1719**
CSM, **1719**
CSP, **1719**
CSS, **1719**
CSV, **1719**
CT, **1719**
CTI, **1719**
CUAE, **1719**
CUBE, **1719**
CUC, **1719**
CUC (*CUCXM*), **1719**

CUCCE, 1719
CUCCX, 1719
CUCDM, 1719
CUCI, 1719
CUCIMOC, 1719
CUCM Local, 1719
CUCM-LDAP User, 1720
CUCMBE, 1720
CUCX, 1720
CUE, 1720
CUEA, 1720
CUIS, 1720
CUMA, 1720
CUMC, 1720
CUMP, 1720
CUnM, 1720
CUOM, 1720
CUP, 1720
CUPC, 1720
CUPM, 1720
CUPS, 1720
CUSM, 1720
CUSSM, 1720
CUVA, 1721
CUVC, 1721
CVP, 1721

D

Dashboards, 1721
DDCO, 1721
DDD, 1721
DDI, 1721
DECT, 1721
DEM, 1721
Device Model, 1721
DHCP, 1721
Dial plan, 1721
Dialplan, 1721
DID, 1721
Digital Experience Monitoring, 1721
Directory Number Routing, 1722
DMS, 1722
DN, 1722
DN Inventory, 1722
DNIS, 1722
DP, 1722
DPCODE, 1722
DPNSS, 1722
Drop account, 1722
DSL, 1722
DTMF, 1722

E

E.164 Associations, 1722
E.164 Inventory, 1722
E.164 Number, 1723
E164, 1723
ECE, 1723
EDRs, 1723
EISUP, 1723
ELIN, 1723
EMCC, 1723
EOL, 1723
ER, 1723
Events, 1723
EXT, 1723
EXTN, 1723

F

FAC, 1723
FDM, 1723
FDP, 1723
Feature
    Feature Cisco Webex, 412
    Feature Cisco Webex Contact Center, 623
    Feature Forced Authorization Codes (*FAC*), 714
    Feature Move User, 1166
    Feature Number Management, 1023
    Feature Pexip Conferencing Overview, 1203
    Feature Phone Registration Activation Code, 510
    Feature Softkey Templates, 477
    Feature User Management, 158
    Phone Based Registration, 483
    Phone Services, 490
FINT (*fint*), 1723
Flowchart
    Audit Number Inventory, 1043
    Cisco Webex Workflow, 415
    Configure VOSS Automate for Microsoft Services, 339
    E164 Inventory Management (*Provider*), 1066
    End to end Customer and Site Dial Plans, 103
    End to end Customer Level Configuration, 99
    End to end Customer Services, 104
    End to end Data Sync, 103
    End to end Hierarchies and Customer Configuration, 98
    End to end manage devices, 101
    End to end Manage Devices (*Cisco & MSFT*), 102
    End to end Manage Users, 107
    End to end Number Management, 104
    End to end User Import, 106

Copyright © 2025 VisionOSS Limited. All rights reserved.

End-to-End Customer Process with Multi-vendor, 96
Flow Through Provisioning Workflow, 1401
Hybrid Cisco-Microsoft User Provisioning, 1276
Install Phone Based Registration, 526
Microsoft Configuration, 350
Microsoft Exchange Overview, 1131
Microsoft Overview, 329
Microsoft Quick Start, 107
Microsoft User Move Configuration, 353
Microsoft Users, 1124
Microsoft-Cisco Hybrid Overview, 1274
Number Cooling, 1036
Phone Based Registration Configuration Per Customer, 492
Phone Based Registration Overview, 483
Register a Phone, 486
Set up Phone Based Registration, 529
Setting up Entitlement, 1475
Sync with Flow Through for Cisco Webex, 184
VOSS Automate Authentication and Authorization for Microsoft, 335
FNN, **1723**
Forced Authorization Codes (FAC) (*Feature*), 714

G

Garbage Collection, **1723**
GDPR, **1724**
Generic Driver, **1724**
GK, **1724**
Glassfish, **1724**
GPRS, **1724**
GSM, **1724**
GUI, **1724**
GUI Rules, **1724**
GW, **1724**

H

H 323, **1724**
H - M-UCS, **1724**
HCS, **1724**
HN, **1724**
HOST, **1724**
Hosted UCS - HUCS, **1724**
HSI, **1724**
HUCS, **1724**
Hunt Group, **1725**
Hunting, **1725**

I

ICPID, **1725**
IDDD, **1725**
Idle URL, **1725**
IDP, **1725**
ILEC, **1725**
IM, **1725**
IMACS, **1725**
IMAP, **1725**
IMP, **1725**
INI, **1725**
Inventory, **1725**
IOS, **1725**
IP, **1725**
IP Addressing, **1726**
IPCBU, **1726**
IPT, **1726**
ISC, **1726**
ISD, **1726**
ISDN, **1726**
ISP, **1726**
ISUP, **1726**
ITU-T, **1726**
IVR, **1726**

J

JSON, **1726**

L

LDAP, **1726**
LEPN, **1726**
Line / Line Relation, **1726**
Line Appearance, **1726**
Location Name, **1726**
Logged on, **1727**
LRID, **1727**

M

M - HUCS, **1727**
MAC, **1727**
MAC Address, **1727**
MACD, **1727**
Macro Functions, **1727**
Macros, **1727**
MDF, **1727**
Menu, **1727**
MF, **1727**
MGCP, **1727**
MML, **1727**
MOH, **1727**
MongoDB, **1727**
Move User (*Feature*), 1166
Movius, **1727**
MT, **1727**
MVS, **1727**
MWI, **1728**

Copyright © 2025 VisionOSS Limited. All rights reserved.

N

NANP, **1728**
NAT, **1728**
NDL, **1728**
NDLR, **1728**
NetFlow, **1728**
Netwise, **1728**
Network Observability, **1728**
NGN, **1728**
NOA, **1728**
NSITE, **1728**
NTP, **1728**
Number Management (*Feature*), 1023

O

OCS, **1728**
OSS, **1728**
Overbuild, **1728**

P

PABX, **1728**
PAI, **1728**
PAT, **1728**
PBT, **1728**
PBX, **1729**
PCC, **1729**
Pexip Conferencing Overview (*Feature*), 1203
PGW, **1729**
PGW Cisco Transit switch, **1729**
Phone MAC Address, **1729**
Phone Registration Activation Code (*Feature*), 510
Phone Services (*Feature*), 490
Pilot Number, **1729**
PIN, **1729**
PLAR, **1729**
PMBX, **1729**
PNOC, **1729**
PostgreSQL, **1729**
POTS, **1729**
PRD, **1729**
PRI, **1729**
Provisioned, **1729**
Provisioning Workflows, **1729**
PSB, **1729**
PST, **1730**
PSTN, **1730**
PT, **1730**
PTT, **1730**
Public Holiday, **1730**
PWF, **1730**

Q

QAG, **1730**
QAS, **1730**
QoS, **1730**
QS, **1730**
QSIG, **1730**
Quick Add User (*Feature*), 1147
    Feature Number Management, 1030
    Feature Specify the Primary Line per User, 1293
Quick User (*Feature*)
    Feature Configuration, 1149
    Feature Creating Quick Add Groups, 1385
    Feature Delete a Quick Add Group, 1392
    Feature Quick Add Group Default Model, 1392
    Feature Shared Line Across Sites, 1248

R

RBAC, **1730**
RCMAC, **1730**
RD, **1730**
RDP, **1730**
Registered, **1730**
Relation, **1730**
REN, **1731**
RL, **1731**
ROI, **1731**
Role, **1731**
Routing ID (*RID*), **1731**
RTMT, **1731**

S

SAS, **1731**
SBC, **1731**
SBR, **1731**
SCCP, **1731**
SCTP, **1731**
SDD, **1731**
SDL, **1731**
SDP, **1731**
Service Activation, **1731**
Session Border Controller, **1731**
SF, **1731**
SIP, **1731**
SIPp, **1732**
Site Code, **1732**
Site defaults, **1732**
SLC, **1732**
SLC-based Dial Plan, **1732**
SM, **1732**
SME, **1732**
SMS, **1732**
SMTP, **1732**
SNMP, **1732**
SNR, **1732**

Copyright © 2025 VisionOSS Limited. All rights reserved.

SOAP, 1732
Softkey Templates (*Feature*), 477
SP, 1732
SP Lock, 1732
SRND, 1732
SRST, 1732
SS7, 1733
SSO, 1733
STD, 1733
SVC, 1733

T

T-CXR, 1733
TAC, 1733
TAPI, 1733
TCO, 1733
Technician Server, 1733
The system, 1733
Themes, 1733
TLS, 1733
TOD, 1733
TOI, 1733
TSPS, 1733
TXE, 1733
TZ, 1733

U

UAX, 1733
UC, 1733
UC SDP, 1733
UCaaS, 1733
UCBU, 1734
UCCE, 1734
UCCX, 1734
UCM, 1734
UCNX, 1734
UCS, 1734
Unified Mobility, 1734
Unified Presence, 1734
Unity, 1734
UnmanagedPBX, 1734
URI, 1734
User Management (*Feature*), 158
User Name, 1734

V

View, 1734
VM, 1734
VMware, 1734
VOIP, 1734
VPAT, 1735
VQManager, 1735

W

WAP, 1735
WATS, 1735
WCS, 1735
WebEx, 1735
WLA, 1735
WLC, 1735
WTAI, 1735

X

XML, 1735

Copyright © 2025 VisionOSS Limited. All rights reserved.