



VOSS Automate Enterprise Core Feature Guide

Release 21.3

Sep 15, 2022

Legal Information

Please take careful note of the following legal notices:

- Copyright © 2022 VisionOSS Limited.
All rights reserved.
- VOSS, VisionOSS and VOSS Automate are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

1	What's New	1
1.1	Enterprise Core Feature Guide: Release 21.3	1
1.2	Enterprise Core Feature Guide: Release 21.3-PB1	3
1.3	Enterprise Core Feature Guide: Release 21.3-PB2	5
1.4	Enterprise Core Feature Guide: Release 21.3-PB3	6
2	Conventions Used in this Guide	7
3	Introduction	8
3.1	Compatibility Matrix	8
3.2	Overview	20
3.3	Getting Started	25
4	Hierarchy Management	62
4.1	Introduction to Hierarchies	62
4.2	Navigating the Hierarchy	66
4.3	View the Hierarchy	68
4.4	Create a Provider	68
4.5	Create a Reseller	71
4.6	Create Intermediate Node	72
4.7	Delete a Hierarchy	73
4.8	Delete Issues and Purges	74
4.9	Localization Language	75
5	Customer Management	76
5.1	Manage Customers	76
5.2	Network Device Lists (NDLs)	78
5.3	CUCM Group Selection	80
5.4	CUCM Group Counts	82
5.5	Countries	83
5.6	Extension Mobility Cross Cluster (EMCC)	84
6	Site Management	90
6.1	Create a Site	90
6.2	Site Defaults Doc Templates	92
6.3	Site Defaults	92
7	Apps Management	103
7.1	VOSS Insights	103
7.2	SMTP Server	114
7.3	VOSS Phone Server Management	114
8	Cisco Apps Management	118

8.1	CUCM (Cisco Unified Communications Manager)	118
8.2	CUCM Music On Hold (MOH)	213
8.3	CUCM FAC Management	220
8.4	CUC (Cisco Unity Connection)	224
8.5	CER (Cisco Emergency Responder)	228
8.6	UCCX (Cisco Contact Center Express)	231
8.7	Webex	232
8.8	Prime Collab (Cisco PCA)	233
8.9	IOS	239
8.10	UC Prep Management	270
9	Microsoft Apps Management	292
9.1	Introduction to Microsoft UC Integration	292
9.2	Microsoft Authentication and Authorization Setup	294
9.3	Create Microsoft Teams Service Account on Azure	301
9.4	VOSS Automate App Registration in Azure	302
9.5	PowerShell Proxy Setup	315
9.6	Configure Microsoft Tenant Connection Parameters	322
10	LDAP Management	329
10.1	LDAP Integration	329
10.2	LDAP Server	335
10.3	LDAP User Sync	340
10.4	LDAP Schedule	343
10.5	Set up LDAP for Authentication Only	344
10.6	View and Update LDAP Authentication Users	346
10.7	LDAP Custom Role Mappings	346
10.8	Re-provision Synced LDAP Users	348
10.9	CUCM LDAP Directory Sync	348
11	Entitlement	350
11.1	Introduction to Entitlement	350
11.2	Entitlement Enforcement	353
11.3	Add a Device Type	355
11.4	Create Device Group	356
11.5	Create an Entitlement Catalog	356
11.6	Create an Entitlement Profile	357
12	User Management	360
12.1	Users	360
12.2	Provisioning	373
12.3	Authentication	376
12.4	Sync and Purge	384
12.5	Manage Filters	395
12.6	Move Users	396
12.7	Admins	407
12.8	Session Timeouts	408
12.9	User Accounts and Passwords	409
12.10	Access Profiles	413
12.11	Self Service	417
13	Role Management	420
13.1	Roles	420
13.2	Themes	433
13.3	Menu Layouts and Landing Pages	455

13.4	Credential Policy	483
13.5	Privacy Policy	487
14	Flow Through Provisioning Configuration	490
14.1	Flow Through Provisioning	490
15	Customizations	497
15.1	Introduction to Customizations	497
15.2	Global Settings	497
15.3	Subscriber Profiles	507
15.4	Model Filter Criteria	510
15.5	Field Display Policies	512
15.6	Configuration Templates	517
15.7	Business Admin Portal Profiles	520
15.8	Configuration Mapping for Phones, DeviceProfiles, and Lines	525
15.9	Dropdown Filters	531
15.10	Line Delete Preferences	534
15.11	Email	535
16	Cisco Dial Plan Management	540
16.1	Introduction to Dial Plan Management	540
16.2	Dialplan Management Menu	541
16.3	Dial Plan Maintenance	543
16.4	Multi-Cluster Dial Plan Maintenance	544
16.5	Dial Plan Input Data and Macros	544
16.6	Dial Plan Models	550
16.7	Dial Plan Model Bulk Loader	586
16.8	Dial Plan Log	586
16.9	Dial Plan Use Checklist	587
17	Microsoft Teams Dial Plan Management	589
17.1	Introduction to Microsoft Teams Dialplan Management	589
17.2	Configure Microsoft Tenant Dialplan	589
18	Microsoft Teams Policies	591
18.1	Introduction to Microsoft Teams Policies	591
19	Number Management	593
19.1	Number Inventory	593
19.2	Number Inventory Overview	594
19.3	View the Number Inventory	597
19.4	Number Status and Usage	599
19.5	Number Range Management	602
19.6	Number Cooling	604
19.7	Number Reservation	606
19.8	Audit Number Inventory	608
20	Unity SIP Integration	611
20.1	Overview	611
20.2	Administration GUI Menus	612
21	Teams Emergency Management	618
21.1	Teams Emergency Locations	618
21.2	Teams Emergency Location Networks	619

22 Subscriber Management	620
22.1 Cisco Subscriber Management	620
22.2 Microsoft Subscriber Management	702
22.3 Multi Vendor Subscribers	726
22.4 Hybrid Cisco-Microsoft Subscribers	733
22.5 Quick Add Subscriber	739
22.6 Line Reports	748
22.7 Customization Reports	750
22.8 Conferencing	752
22.9 Webex App Users	754
22.10 Reassign Services	766
23 Services	775
23.1 Webex App	775
23.2 Auto Attendant (Call Handler)	777
23.3 Cisco Unity Connection (CUC) Localization	792
24 Overbuild	794
24.1 Overbuild Introduction	794
24.2 Moving Model Instances	797
24.3 Overbuild Site Defaults	798
24.4 Run Overbuild	799
24.5 Overbuild Tool	805
24.6 User Phone Association	805
24.7 Overbuild Analog Gateway	806
24.8 Device Models	806
25 Administration Tools	809
25.1 Import	809
25.2 Bulk Administration	810
25.3 Alerts	823
25.4 Transactions	826
25.5 Northbound Notifications	843
25.6 Schedules	847
25.7 System Settings	849
26 Single Sign On (SSO)	851
26.1 Single Sign On (SSO) Overview	851
26.2 SSO Certificate Management	852
26.3 Configure Single Sign-On for VOSS Automate	853
26.4 Configure the System as a SSO Service Provider	859
26.5 Renew Single Sign-On Certificate for VOSS Automate	860
26.6 SAML Elements in Assertions	860
27 Data Sync	862
27.1 Introduction to Data Sync	862
27.2 Default Cache Control Policy	865
27.3 Data Sync Types	866
27.4 Full Sync	869
27.5 Enable a Scheduled Data Sync	869
27.6 Manually Run the Default Data Sync	870
27.7 Controlling a Data Sync with a Model Type List	870
27.8 Create a Targeted Model Type List	871
27.9 Model Instance Filter	872
27.10 Model Instance Filter Examples	876

27.11 View List of Device Models	878
27.12 Create a Custom Data Sync	879
27.13 Unified CM Change Notification Feature Alerts	880
27.14 Change Notification Sync	881
28 Self Service Administration	889
28.1 Introduction to Self Service Administration	889
28.2 Self Service Feature Display Policy	889
28.3 Self Service Feature Display Policy Field Reference	890
28.4 End User Access and Authentication	894
28.5 Themes and Branding	894
28.6 Self-Service Login Banner	894
28.7 Personal Phones (Remote Destinations)	895
28.8 Dual Mode Phones - Mobile ID	895
28.9 Voicemail for Self-Service	895
28.10 Links Page	895
29 Self Provisioning	896
29.1 Introduction to Self-Provisioning	896
29.2 Bottom-Up User Management	896
29.3 Top-Down User Management	897
29.4 CUCM Configuration for Self-Provisioning	897
29.5 Site Configuration for Self-Provisioning	898
29.6 Generate a User's Primary Line	898
29.7 Specify the Primary Line per Subscriber	899
29.8 Add a Self-Provisioning Universal Device Template	899
29.9 Add a Self-Provisioning Universal Line Template	901
29.10 Add a Self-Provisioning User Profile	901
29.11 Set a Default User Profile for a Site	902
29.12 Add Self-Provisioning Line Mask	902
30 Advanced Tools for System Administrators	904
30.1 Custom Variables	904
30.2 Model Report	905
31 Appendix: Business Admin Portal Configuration	906
31.1 Introduction to Business Admin Portal Configuration	906
31.2 Custom Icon Names Reference	907
32 Appendix: Optional Features	908
32.1 Dial Plan Management	908
32.2 Unity SIP Integration	913
32.3 Phone Based Registration	915
32.4 Phone Services	939
Index	946

1. What's New

1.1. Enterprise Core Feature Guide: Release 21.3

- EKB-10424: Add ability to include the Description in the Phone dropdown for Quick Add Subscriber: [Global Settings](#)
- EKB-10424: Add ability to include the Description in the Phone dropdown for Quick Add Subscriber: [Replace Phone](#)
- EKB-10424: Add ability to include the Description in the Phone dropdown for Quick Add Subscriber: [Quick Add Subscriber for CUCM Users](#)
- EKB-10448: Use certificate thumbprint auth for MS Graph driver app registration: [VOSS Automate App Registration in Azure](#)
- EKB-10448: Use certificate thumbprint auth for MS Graph driver app registration: [Configure Microsoft Tenant Connection Parameters](#)
- EKB-11022: Add Generic Flow Through Provisioning hooks to LDAP/CUCM syncs: [Site Defaults](#)
- EKB-11022: Add Generic Flow Through Provisioning hooks to LDAP/CUCM syncs: [Flow Through Provisioning](#)
- EKB-11022: Add Generic Flow Through Provisioning hooks to LDAP/CUCM syncs: [Global Settings](#)
- EKB-11056: Add support to execute an LDAP Directory Sync on Unified CM: [CUCM LDAP Directory Sync](#)
- EKB-11321: Add Countries entry to Provider Admin Menu: [Countries](#)
- EKB-11807: Delete Subscriber should provide option to leave hard phone instead of delete - similar to line behavior: [Global Settings](#)
- EKB-11807: Delete Subscriber should provide option to leave hard phone instead of delete - similar to line behavior: [View and Manage Subscribers](#)
- EKB-11866: Add new data/AuthorizedAdminHierarchy model (without allowed hierarchies): [Introduction to Self-service](#)
- EKB-11892: Add Tenant Dial Plan field to MS Quick Add Subscriber: [Site Defaults](#)
- EKB-11892: Add Tenant Dial Plan field to MS Quick Add Subscriber: [Configure Microsoft Tenant Dialplan](#)
- EKB-11892: Add Tenant Dial Plan field to MS Quick Add Subscriber: [Quick Subscriber for Microsoft Users](#)
- EKB-12012: Add Summary Header GUI rule for Lines on CTI Route Point page: [CTI Route Points](#)

- EKB-12151: Add Summary Header GUI rule for Unified Messaging Account on Voicemail page: [Voicemail](#)
- EKB-12240: Support for Unified CM IM & Presence server in Insights asset onboarding automation: [Introduction to VOSS Insights Monitoring](#)
- EKB-12240: Support for Unified CM IM & Presence server in Insights asset onboarding automation: [Onboard Assets](#)
- EKB-12240: Support for Unified CM IM & Presence server in Insights asset onboarding automation: [Add a CUCM Server](#)
- EKB-3999: Site summary page should show External ID and full address information: [Create a Site](#)
- EKB-4773: Disable “Failed Login Limiting per Source” in the “Default” Credential Policy for Provider deployments: [Customized Credential Policy](#)
- EKB-8094: Improve Menu Layout and Landing Page management pages: [Menu Layouts](#)
- EKB-8094: Improve Menu Layout and Landing Page management pages: [Landing Pages](#)
- VOSS-1068: CRUD Support for Outstanding MS Teams Policies: [Introduction to Microsoft Teams Policies](#)
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12791: Include a MS_Only_Role with associated Menu, Landing Page and BAP Profile) . See: [User Roles](#)
Documentation changes for Microsoft functionality, following update to PowerShell.
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12791: Include a MS_Only_Role with associated Menu, Landing Page and BAP Profile) . See: [Business Admin Portal Profiles](#)
Documentation changes for Microsoft functionality, following update to PowerShell.
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12733: Updated Policies across the system) . See: [Introduction to Microsoft Teams Policies](#)
Documentation changes for Microsoft functionality, following update to PowerShell.
- VOSS-886: Number Inventory Alerting (EKB-11084: Create Global Settings for INI Alerting Feature) . See: [Global Settings](#)
Added details on alerting and reporting of the number inventory.
- VOSS-886: Number Inventory Alerting (EKB-11087: Create Macros/EMAIL HTTP Template for INI Alerting Feature) . See: [Email](#)
Added details on alerting and reporting of the number inventory.
- VOSS-886: Number Inventory Alerting: [Alert Types and Alert Field Reference](#)
- VOSS-891: Productize Microsoft Hybrid Solution: [Configure Microsoft Tenant Connection Parameters](#)
- VOSS-891: Productize Microsoft Hybrid Solution: [Add an Admin User](#)
- VOSS-891: Productize Microsoft Hybrid Solution: [Global Settings](#)
- VOSS-891: Productize Microsoft Hybrid Solution: [Subscriber Profiles](#)
- VOSS-891: Productize Microsoft Hybrid Solution (EKB-12360: Multi-Vendor Subscriber: List/Form View - Enhancements) . See: [Multi Vendor Subscribers](#)
Added details on settings, user management where Cisco / Microsoft Hybrid is enabled.
- VOSS-891: Productize Microsoft Hybrid Solution: [Overview: Microsoft - Cisco Hybrid](#)

- VOSS-891: Productize Microsoft Hybrid Solution: [Hybrid Cisco-Microsoft Management](#)
- VOSS-891: Productize Microsoft Hybrid Solution: [Hybrid Service Definitions](#)
- VOSS-911: End Users with Admin Access: [Add an Admin User](#)
- VOSS-911: End Users with Admin Access: [Role-based Access](#)
- VOSS-911: End Users with Admin Access: [Authorized Admin Hierarchy](#)
- VOSS-911: End Users with Admin Access: [Configure Single Sign-On for VOSS Automate](#)
- VOSS-950: Number Inventory Updates for Hybrid support: [Number Status and Usage](#)
- VOSS-962: Provisioning Improvements on Webex App (EKB-11138: Allow QAS provisioning of WebexTeams Calling Behaviour for Site level SparkUser) . See: [Site Defaults](#)
Overall improvements to the provisioning functionality for Webex App
- VOSS-962: Provisioning Improvements on Webex App (EKB-11113: Add validation to check for Primary Line when enabling Webex Teams Calling) . See: [Webex App](#)
Overall improvements to the provisioning functionality for Webex App

1.2. Enterprise Core Feature Guide: Release 21.3-PB1

- EKB-12278: Add “Use next available line” to Quick Add Subscriber: [Quick Add Subscriber for CUCM Users](#)
- EKB-12295: Add “Use next available line” to MS Quick Add Subscriber: [Quick Subscriber for Microsoft Users](#)
- EKB-12708: Make entitlement profile empty in the data/SubscriberProfile instances for Hybrid: [Hybrid Service Definitions](#)
- EKB-12793: Move Subscriber - Extension Mobility Only not Updating/Moving Line: [Move Subscriber](#)
- EKB-12904: Protocol cant be changed when adding a Phone from relation/SubscriberPhone: [Site Defaults](#)
- EKB-12904: Protocol cant be changed when adding a Phone from relation/SubscriberPhone: [View and Manage Subscribers](#)
- EKB-12904: Protocol cant be changed when adding a Phone from relation/SubscriberPhone: [Phones](#)
- VOSS-1062: Microsoft Dynamic Emergency Calling (EKB-12878: Create templates for emergency device models) . See: [Teams Emergency Locations](#)
Documentation added for MS Teams Emergency Calling
- VOSS-1062: Microsoft Dynamic Emergency Calling (EKB-12878: Create templates for emergency device models) . See: [Teams Emergency Location Networks](#)
Documentation added for MS Teams Emergency Calling
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12869: MS Quick Subscriber GUI Rule for line_uri and automatic_line) . See: [Site Defaults](#)
Documentation changes for Microsoft functionality, following update to PowerShell.
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12954: Do not allow staging of user when Manage License flag is false) . See: [Site Defaults](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0): [PowerShell Proxy Setup](#)
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12791: Include a MS_Only_Role with associated Menu, Landing Page and BAP Profile) . See: [Add and Edit Roles](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12742: Number Inventory updates required) . See: [Global Settings](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0): [Subscriber Profiles](#)
- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12732: Add Subscriber from Profile Changes needed for PS4.x) . See: [Subscriber Profiles](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12742: Number Inventory updates required) . See: [View the Number Inventory](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12743: Number Inventory Audit changes) . See: [Number Status and Usage](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12742: Number Inventory updates required) . See: [Number Range Management](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12743: Number Inventory Audit changes) . See: [Audit Number Inventory](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12730: MS Quick Subscriber Template Changes to support PS4.x) . See: [Microsoft Subscribers](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12890: Need to have an Unstage action on Staged users when we're provisioning their MS licensing and subsequent Teams accounts) . See: [Microsoft Licenses](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12954: Do not allow staging of user when Manage License flag is false) . See: [Microsoft Licenses](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12847: Add a "New Users Only" sync for the Microsoft 365, Teams and MExchange Data Syncs) . See: [VOSS Automate Configuration and Sync](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12791: Include a MS_Only_Role with associated Menu, Landing Page and BAP Profile) . See: [VOSS Automate Configuration and Sync](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12763: Function next_available_line needs to cater for staged numbers) . See: [Quick Subscriber for Microsoft Users](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12730: MS Quick Subscriber Template Changes to support PS4.x) . See: [Quick Subscriber for Microsoft Users](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12869: MS Quick Subscriber GUI Rule for line_uri and automatic_line) . See: [Quick Subscriber for Microsoft Users](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12890: Need to have an Unstage action on Staged users when we're provisioning their MS licensing and subsequent Teams accounts) . See: [Quick Subscriber for Microsoft Users](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12954: Do not allow staging of user when Manage License flag is false) . See: [Quick Subscriber for Microsoft Users](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

- VOSS-1072: Update MS Teams Powershell Module Version (4.3.0) (EKB-12730: MS Quick Subscriber Template Changes to support PS4.x) . See: [Microsoft Exchange](#)

Documentation changes for Microsoft functionality, following update to PowerShell.

1.3. Enterprise Core Feature Guide: Release 21.3-PB2

- EKB-11638: Adhoc filter not cleared on logout: [Working with Lists](#)
- EKB-11638: Adhoc filter not cleared on logout: [Filtering Transactions](#)
- EKB-12324: Theme image filenames don't work if # character included in the filename: [Manage Themes \(Legacy Admin Portal\)](#)
- EKB-12677: Update "Existing Services" GUI rule to hide disabled services: [Create a Subscriber with Existing User](#)
- EKB-12677: Update "Existing Services" GUI rule to hide disabled services: [Quick Add Subscriber for CUCM Users](#)
- EKB-13056: In MS Tenant instance view, having Test Connection and Sync All next to each other makes it too easy to unintentionally initiate a Sync All: [Configure Microsoft Tenant Connection Parameters](#)
- EKB-13265: Voicemail accounts are not getting deleted when deleting LDAP users: [LDAP User Sync](#)
- EKB-13265: Voicemail accounts are not getting deleted when deleting LDAP users: [Global Settings](#)
- EKB-13265: Voicemail accounts are not getting deleted when deleting LDAP users: [View and Manage Subscribers](#)
- EKB-2620: Add "What would you like to do" Search box on Dashboard: [Introduction to the Admin Portal User Interface](#)
- EKB-2620: Add "What would you like to do" Search box on Dashboard: [Search in VOSS Automate](#)

1.4. Enterprise Core Feature Guide: Release 21.3-PB3

- EKB-10977: Add support for VG420 Analog Gateway: [Set up an Analog Gateway](#)
- EKB-11607: Add custom strings/boolean fields for GS Add Gateway Port: [Add Port to Analog Gateway](#)
- EKB-12307: Add a feature to exclude model types from CallManager change collector service: [VOSS Automate Change Notification Functionality](#)
- EKB-12768: Number inventory should persist extra fields and not drop them when making numbers available: [Number Range Management](#)
- EKB-12805: Line (device/cucm/Line) reset has no effect: [Reset-Restart Site Phones](#)
- EKB-12810: Expand Summary Attributes for Data Sync: [Introduction to Data Sync](#)
- EKB-12811: Expand Summary Attributes for Schedule: [Create or Update a Schedule](#)
- EKB-13017: Site Defaults Doc updated with the latest Microsoft policies: [Site Defaults](#)
- EKB-13640: Allow a DN to be shared by phone and Unity Connection call handler pilot: [Auto-Attendant Call Handler](#)
- EKB-13640: Allow a DN to be shared by phone and Unity Connection call handler pilot: [Add, Update, or Delete a Call Handler \(Auto Attendant\)](#)
- EKB-13696: Add MultiVendor MvsEnhancedProvider and MvsEnhancedCustomer role sets and BAP profiles to VOSS Automate: [User Roles](#)
- EKB-9720: New GUI drop-down lists improvements: [Search in VOSS Automate](#)

2. Conventions Used in this Guide

VOSS Automate offers two versions of its main user interface:

- Legacy Admin GUI
- Admin Portal

Where the user interface differs for workflow tasks in the system, the documentation refers either to legacy (for the classic Admin GUI), or Admin Portal (for the new GUI).

Note: This does not apply to the Self-Service interface or to the Business Admin Portal.

Formatting Conventions

The table describes formatting conventions in the VOSS Automate documentation:

Item	Description
GUI buttons and labels	These are displayed in bold text.
Menu Paths	Menu paths are also shown in bold text, e.g. Customer Management > EMCC > EMCC Group , where '>' is the delimiter between the menu levels. Important Note: The menu paths provided in this guide are the default menu paths shipped with the product. A reseller (or higher) administrator can modify these paths.
Asterisk '*' after field name, e.g. Userid *	Indicates that the field is mandatory.

3. Introduction

3.1. Compatibility Matrix

3.1.1. Supported Browsers

For this release, testing was performed using the following browser versions.

Note that older or newer versions of each browser may also be compatible.

OS Browser	Chrome	Edge	Firefox	Safari
Windows 10 64 bit	100	46	102	N/A
Ubuntu 21.04	103	N/A	98.0.2	N/A
Mac OS 12.01	103	N/A	94	15.1

3.1.2. VMware Support

For this release, testing was performed using vSphere:

- VMware vCenter Server Appliance version 7.0.0.10600
- VMware ESXi:
 - 6.7.0, 13006603
 - 6.7.0, 10302608
 - 6.5.0, 14320405
 - 6.5.0, 8294253
- Client version 7.0.0.10600

VMware version >=5.1 is supported.

VMware feature	Tested this release
HA	No
vMotion	No

3.1.3. Automate Application Compatibility Matrix

Note:

- On Cisco UC app versions we list the significant versions, including any service updates (SUs) supported under that. For exact versions tested, see the release notes for the given release. Specific notes are added if there are issues with specific Cisco UC apps versions and VOSS Automate versions.
- On the Cisco UC apps, any new provisioning settings for new features added in a SU will not be visible in VOSS Automate unless specific work was done to support them, since AXL API changes are not done in SU releases by Cisco. VOSS release notes will indicate any SU specific features that have been explicitly supported.
- If you need a version supported that is not indicated above as supported or planned, contact your VOSS team for further options and if support could be added.

VOSS Automate 21.3

Release 21.3-PB3

For release 21.3-PB3 testing was performed using the following application versions.

Note that older versions of each app may also be compatible.

Vendor	Apps	VOSS Automate 21.3-PB3	Notes, application specific caveats
Cisco	Cisco UCM	10.5.2.18900-15, 11.5.1.22900-28, 12.5.1.14900-63, 14.0.1.11900-132, 14.0.1.12900-161	14SU2 is latest validated version
Cisco	Cisco Unity Connection	10.5.2.18900-15, 11.5.1.22900-28, 12.5.1.14900-45, 14.0.1.11900-128, 14.0.1.12900-69	14SU2 is latest validated version
Cisco	HCM-F	11.5.4.11900-3, 11.5.5.10000-2, 12.5.1.10000-5, 12.6.1.10000-2	12.6.1 is latest validated version
Cisco	UCCX	12.5.1.11001-348 (SU1-ES03)	12.5.1.11001-348 (SU1-ES03) is latest validated version

Release 21.3-PB2

For release 21.3-PB2 testing was performed using the following application versions.

Note that older versions of each app may also be compatible.

Vendor	Apps	VOSS Automate 21.3-PB2	Notes, application specific caveats
Cisco	Cisco UCM	10.5.2.18900-15, 11.5.1.22900-28, 12.5.1.14900-63, 14.0.1.11900-132	14SU1 is latest validated version
Cisco	Cisco Unity Connection	10.5.2.18900-15, 11.5.1.22900-28, 12.5.1.14900-45, 14.0.1.11900-128	14SU1 is latest validated version
Cisco	HCM-F	11.5.4.11900-3, 11.5.5.10000-2, 12.5.1.10000-5, 12.6.1.10000-2	12.6.1 is latest validated version
Cisco	UCCX	12.5.1.11001-348 (SU1-ES03)	12.5.1.11001-348 (SU1-ES03) is latest validated version

Release 21.3-PB1

For release 21.3-PB1 testing was performed using the following application versions.

Note that older versions of each app may also be compatible.

Vendor	Apps	VOSS Automate 21.3-PB1	Notes, application specific caveats
Cisco	Cisco UCM	10.5.2.17900-13, 11.5.1.22900-28, 12.5.1.14900-63, 14.0.1.11900-132	14SU1 is latest validated version
Cisco	Cisco Unity Connection	10.5.2.17900-13, 11.5.1.22900-28, 12.5.1.14900-45, 14.0.1.11900-128	14SU1 is latest validated version
Cisco	HCM-F	11.5.4.11900-3, 11.5.5.10000-2, 12.5.1.10000-5, 12.6.1.10000-2	12.6.1 is latest validated version
Cisco	UCCX	12.5.1.11001-348 (SU1-ES03)	12.5.1.11001-348 (SU1-ES03) is latest validated version

Release 21.3

For release 21.3 testing was performed using the following application versions.

Note that older versions of each app may also be compatible.

Vendor	Apps	VOSS Automate 21.3	Notes, application specific caveats
VOSS	NBI	3.2.0	
VOSS	VOSS Insights Dashboard	SP64, SP65, SP66, 22.1	SP65 required for User and Number Inventory analytics
VOSS	VOSS Insights Arbitrator	SP23, SP24, SP25, 22.1	
VOSS	VOSS Insights DS9	SP8/5.0 SP1	Existing users: SP8, new users; 5.0 SP1
VOSS	VOSS Insights Raptor	SP12, 22.1	
VOSS	VOSS Phone Server	1.0.0	Base release version
Cisco	Cisco UCM	10.0, 10.5, 11.5, 12.5, 14.0	14SU1 is latest validated version
Cisco	Cisco Unity Connection	10.0, 10.5, 11.5, 12.5, 14.0	14SU1 is latest validated version
Cisco	HCM-F	10.5, 11.5, 12.5, 12.6	12.6.1 is latest validated version
Cisco	UCCX	12.5.1	12.5.1.11001-348 (SU1-ES03) is latest validated version
Cisco	Webex Meetings	Cloud based - so latest	
Cisco	Webex Teams	Cloud based - so latest	
Cisco	Cisco Contact Center	11.x, 12.x	
OpenLDAP Microsoft	Directory	OpenLDAP Active Directory	
OpenAM Shibboleth ADFS PingIdentity	SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	Only Security Assertion Markup Language (SAML) 2.0 is supported.
Microsoft	Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
ServiceNow	ServiceNow	Cloud-based - so latest	
Pexip	Pexip Infinity Conferencing Platform	24.1	Build 55723.0.0 Build date 2020-08-20T15:07:05Z

VOSS Automate 21.2

Vendor	Apps	VOSS Automate 21.2	Notes, application specific caveats
VOSS	NBI	3.2.0	
VOSS	VOSS Insights Dashboard	SP64, SP65, SP66	SP65 required for User and Number Inventory analytics
VOSS	VOSS Insights Arbitrator	SP23, SP24, SP25	
VOSS	VOSS Insights DS9	SP8/5.0 SP1	Existing users: SP8, new users; 5.0 SP1
VOSS	VOSS Insights Raptor	SP12	
VOSS	VOSS Phone Server	1.0.0	Base release version
Cisco	Cisco UCM	10.0, 10.5, 11.5, 12.5, 14.0	14SU1 is latest validated version
Cisco	Cisco Unity Connection	10.0, 10.5, 11.5, 12.5, 14.0	14SU1 is latest validated version
Cisco	HCM-F	10.5, 11.5, 12.5, 12.6	12.6.1 is latest validated version
Cisco	UCCX	11.6.2	11.6.2.10000-38 is latest validated version
Cisco	Webex Meetings	Cloud based - so latest	
Cisco	Webex Teams	Cloud based - so latest	
OpenLDAP Microsoft	Directory	OpenLDAP Active Directory	
OpenAM Shibboleth ADFS PingIdentity	SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	Only Security Assertion Markup Language (SAML) 2.0 is supported.
Microsoft	Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
Cisco	Cisco Contact Center	11.x, 12.x	
ServiceNow	ServiceNow	Cloud-based - so latest	
Pexip	Pexip Infinity Conferencing Platform	24.1	Build 55723.0.0 Build date 2020-08-20T15:07:05Z

VOSS-4-UC 21.1

Vendor	Apps	VOSS-4-UC 21.1	Notes, application specific caveats
VOSS	NBI	3.2.0	
VOSS	VOSS Analytics Dashboard	SP64, SP65	SP65 required for User and Number Inventory Analytics
VOSS	VOSS Assurance Arbitrator	SP23, SP24	
VOSS	VOSS Phone Server	1.0.0	Base release version
Cisco	Cisco UCM	10.0, 10.5, 11.5, 12.5, 14.0	14.0 is latest validated version
Cisco	Cisco Unity Connection	10.0, 10.5, 11.5, 12.5, 14.0	14.0 is latest validated version
Cisco	HCM-F	10.5, 11.5, 12.5, 12.6	12.6.1 is latest validated version
Cisco	UCCX	11.6.2	11.6.2.10000-38 is latest validated version
Cisco	Webex Meetings	Cloud based - so latest	
Cisco	Webex Teams	Cloud based - so latest	
OpenLDAP Microsoft	Directory	OpenLDAP Active Directory	
OpenAM Shibboleth ADFS PingIdentity	SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	Only Security Assertion Markup Language (SAML) 2.0 is supported.
Microsoft	Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
Cisco	Cisco Contact Center	11.x, 12.x	
ServiceNow	ServiceNow	Cloud-based - so latest	
Pexip	Pexip Infinity Conferencing Platform	24.1	Build 55723.0.0 Build date 2020-08-20T15:07:05Z

VOSS Automate Adaptations Support

The following Adaptations have been updated to be compatible with VOSS Automate 21.2.

Note:

- If these Adaptations are in use on 19.x, they must be reinstalled after upgrading to 21.2.
- If these Adaptations were already installed on 21.1, they do not have to be reinstalled after upgrading to 21.2.

VOSS Automate Adaptation	Minimum Version	Notes, application specific caveats
GS Cross Site Hunt Group	V1.9_21.1	
GS LinkedSites	V1.27_21.1	
GS Change Line	V0.1_21.1	
GS Group Voicemail	V1.12_21.1	
GS Device OOS	V0.7_21.1	
GS Number Inventory	V0.11_21.1	

VOSS-4-UC 20.1.1

Apps	VOSS-4-UC 20.1.1	Notes, application specific caveats
Cisco UCM	10.0, 10.5, 11.5, 12.5	12.5(1)SU3 is latest validated version
Cisco Unity Connection	10.0, 10.5, 11.5, 12.5	12.5(1)SU2 is latest validated version
HCM-F	10.0, 10.5, 11.5, 12.5, 12.6	12.6.1 is latest validated version
Webex Meetings	Cloud based - so latest	
Webex Teams	Cloud based - so latest	
Directory	OpenLDAP, Active Directory	
SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	
Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
Cisco Contact Center	11.x, 12.x	
ServiceNow	Cloud-based - so latest	

VOSS-4-UC 19.3.4

Apps	VOSS-4-UC 19.3.4	Notes, application specific caveats
Cisco UCM	10.5, 11.5, 12.5	12.5.1su3 is latest validated version
Cisco Unity Connection	10.5, 11.5, 12.5	12.5.1su2 is latest validated version
HCM-F	10.5, 11.5, 12.5, 12.6	12.6.1 is latest validated version
Webex Meetings	Cloud based - so latest	
Webex Teams	Cloud based - so latest	
Directory	OpenLDAP, Active Directory	
SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	
Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
Cisco Contact Center	11.6	
ServiceNow	Cloud-based - so latest	

- For the 19.3.4 PB1 - PB5 Releases, testing was performed using the following Cisco UC apps versions.

UC App	Versions
CUCM	11.5.1 SU9 (11.5.1.21900-40), 12.5.1 SU4 (12.5.1.14900-63)
CUCX	11.5.1 SU9 (11.5.1.21900-40), 12.5.1 SU4 (12.5.1.14900-45)
HCMF	11.5.5 (11.5.5.10000-2), 12.5.1 SU3 (12.5.1.13900-4), 12.6.1 (12.6.1.10000-2, use 12.5 API)

VOSS-4-UC 19.3.3

Apps	VOSS-4-UC 19.3.3	Notes, application specific caveats
Cisco UCM	10.0, 10.5, 11.5, 12.5	12.5.1su1 is latest validated version
Cisco Unity Connection	10.0, 10.5, 11.5, 12.5	12.5.1su1 is latest validated version
HCM-F	10.0, 10.5, 11.5, 12.5	12.5.1 is latest validated version
Webex Meetings	Cloud based - so latest	
Webex Teams	Cloud based - so latest	
Directory	OpenLDAP, Active Directory	
SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	
Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
Cisco Contact Center	11.6	
ServiceNow	Cloud-based - so latest	

VOSS-4-UC 19.3.2

Apps	VOSS-4-UC 19.3.2	Notes, application specific caveats
Cisco UCM	10.0, 10.5, 11.5, 12.5	12.5.1su1 is latest validated version
Cisco Unity Connection	10.0, 10.5, 11.5, 12.5	12.5.1su1 is latest validated version
HCM-F	10.0, 10.5, 11.5, 12.5	12.5.1 is latest validated version
Webex Meetings	Cloud based - so latest	
Webex Teams	Cloud based - so latest	
Directory	OpenLDAP, Active Directory	
SSO	VOSS Tested - OpenAM, Shibboleth Partner integrated - ADFS, PingIdentity	
Microsoft	Skype for Business on-prem, cloud, Microsoft Teams, Office365	
Cisco Contact Center	11.6	
ServiceNow	Cloud-based - so latest	

3.1.4. Insights Application Compatibility Matrix

Insights 22.1

Vendor	Apps	VOSS Insights Dashboard Version 22.1 / Arbitrator Version 22.1	Notes, application specific caveats
VOSS	Automate	21.3	
Cisco	Cisco UCM	10.0, 10.5, 11.5, 12.5, 14	
Cisco	Cisco Unity Connection	10.0, 10.5, 11.5, 12.5, 14	
Cisco	Cisco Contact Center Express (UCCX)	11.5, 12.5, 14	
Cisco	Cisco Contact Center Enterprise (UCCE)	10.5, 11.5, 12.5, 14	
Cisco	Webex Meetings	Cloud based (so, latest)	
Cisco	Webex Teams	Cloud based (so, latest)	
Microsoft	Microsoft (Cloud)	Microsoft Teams, Microsoft 365 Suite	
Microsoft	Microsoft (On Premise)	Skype for Business	
Polycom		Phones and Video devices attached to supported versions of Cisco UCM	
ZOOM		Zoom meetings & events, Zoom phone system, Zoom chat	
Avaya	Avaya UC Enterprise Core	Aura v7 and v8 Avaya App Integration - 7.x or 8.x <ul style="list-style-type: none"> • SMGR - Aura System Manager • OfficeLinx (ESNA) • CM - Communications • Equinox Mgt Server 	Monitoring / Alerting, Call quality analysis, License reporting, messaging / voice system status and use, session details, trunk status, DSP resource utilization, ESS & Gateway status
Avaya	Avaya Contact Center		
Avaya	Avaya Media Gateway	G430, G450	Combination of SNMP and queries

continues on next page

Table 1 – continued from previous page

Vendor	Apps	VOSS Insights Dashboard Version 22.1 / Arbitrator Version 22.1	Notes, application specific caveats
Avaya	Avaya PBX	Versions 5.x, 6.x	Combination of SNMP and queries. Policy module available for pre version 7 releases
Avaya	Avaya - Definity	G3r Versions 4, 6, 7, 9	Limited by Definity capability to send monitoring data to external systems. Most older systems are only able to be monitored by Avaya themselves. Review of your specific version is needed to determine the level of alerting and reporting.
Avaya	Avaya - Nortel Meridian	Option 11C	Alerting Only
CISCO DETAILS		<i>Supported versions are those compatible with the Cisco versions listed above unless otherwise stated.</i>	
	IM and Presence Server		
	Emergency responder		
	Cisco Jabber Devices		Device monitoring & reporting comes from UCM, not directly from the device.
	Cisco Phones		Phone monitoring & reporting comes from UCM (for example: CDR, CMR, RIS), not directly from the phone.
	Cisco Video Devices		Video Device monitoring & reporting comes from UCM and TMS, and in many cases can be collected directly from the device.
	Media Server		
	Media Resources		
	CMS (Cisco Meeting server)	11.5, 12.5, 14	

continues on next page

Table 1 – continued from previous page

Vendor	Apps	VOSS Insights Dashboard Version 22.1 / Arbitrator Version 22.1	Notes, application specific caveats
	TMS (Telepresence Mgmt)		
	TMS-XE (TMS extension for Microsoft)		
	Cisco MCU (Telepresence multiple control units)		
	VCS (Video Conferencing)		
	Cisco Webex Teams (including Control Hub)		
	CCA (Webex Audio Monitoring)		
	Expressway C & E		
	Cisco CUBE (Border Element)		
	Finesse		
	CVP (Voice Portal)		
	VXML Server		
	CME (CallManager Express)		
	CUIC (Intelligence)		
	Cisco ICM Intelligent Contact Mgmt)		
	CTIOS (Computer Telephony Integrated Object Server)		
RECORDING APPLICATIONS			
	Nice (Recording)		
	Nuance (Recording)		
	Verint (Recording)		
SBC	Sonus SBC		
SBC	Sonus SBC		
SBC	Audiocodes SBC		Includes RTCP if licensed
SBC	Oracle SBC & EBC	SBC: SCZ8.4.0 + ECB: PCZ3.3.0 +	Alerting only
VOSS			

continues on next page

Table 1 – continued from previous page

Vendor	Apps	VOSS Insights Dashboard Version 22.1 / Arbitrator Version 22.1	Notes, application specific caveats
VOSS	VOSS Automate	Version 19 or later	
NETFLOW	Netflow	Versions 5, 9, 10, IP-FIX, AWS Flow Logs, Azure NSG Logs, SD WAN Flow	Separate license for VOSS Insights Netflow

3.2. Overview

3.2.1. Welcome to VOSS Automate

VOSS 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 VOSS Automate, including provisioning steps and interactions between VOSS Automate and the UC applications of vendors that VOSS Automate supports, such as Cisco HCS. This guide also describes user and subscriber management, including LDAP-related move and push operations.

3.2.2. Unicode Limitations

For VOSS Automate, Unicode characters are supported only in the following fields:

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

3.2.3. Accessibility

VOSS Automate complies with guidelines issued by the World Wide Web Consortium (W3C) to implement functional improvements to the Admin Portal. We have tested extensively to ensure that our content is accessible to all users, and meets the Level A and Level AA Success Criteria as described in WCAG 2.1.

The table describes features to assist people with disabilities, including people who may not be able to use a mouse, or who have visual impairments:

Title display in the browser	When choosing a menu option in the Admin Portal, the selected menu option title is also displayed in the browser tab. This helps users know where they are and also helps them move between pages open in their browser.
Images have alternative text	Images on buttons that perform a function have additional alternative text, which is used by people who cannot see the image. This alternative text is displayed when the mouse pointer hovers over an image. People who are blind and use screen readers can hear the alternative text read out; and people who have turned off images to speed download or save bandwidth can see the alternative text.
Headings given a meaningful hierarchy to ease navigation	Web pages often have sections of information separated by visual headings. Each page typically has at least one heading. When there is more than one heading on a page, the headings have a hierarchy, which makes it easier for the user to navigate to a particular heading and to navigate between headings.
Contrast ratio can be changed	While some people need high contrast, for others, including people with some types of reading disabilities such as dyslexia, bright colors (high luminance) are not readable. They need low luminance. 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	<p>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.</p> <p>In a browser that supports keyboard navigation with the Tab key (for example, Firefox, IE, Chrome, and Safari):</p> <ol style="list-style-type: none"> 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.

3.2.4. Log In to the Admin Portal

The Admin Portal uses the same base address (URL) as the Legacy Admin Portal. The base address is then suffixed with `portal/#/admin`, for example: `https://{hostname}/portal/#/admin`.

Your username and password are the same.

Standard Users

To log in as a standard user:

1. Go to:
 - Legacy Admin GUI: `https://{hostname}/login`
 - Admin Portal: `https://{hostname}/admin/sso/{Login URI}/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.

LDAP Users

To log in as an LDAP user:

1. Go to URL: `https://{hostname}/login`
2. Log in, using either `{user ID}[@hierarchy]` or your email address.
 - The user ID (`{user ID}`) corresponds to the login attribute name specified in the LDAP network connection, 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.
 - `@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.

SSO Users

To log in as SSO user:

1. Go to URL:
 - Legacy Admin GUI: `https://{host name}/sso/{SSO login URI}/login`
 - Admin Portal: `https://{host name}/admin/sso/{Login URI}/login`
2. Log in using the relevant SSO identity provider credentials.

Related Topics

- Create a Landing Page in the Core Feature Guide
- SSO Users and Login in the Core Feature Guide
- LDAP Users and Login in the Core Feature Guide

3.2.5. Multi Vendor Support

VOSS Automate supports provisioning and management of all unified communications (UC) applications, across multiple UC vendors, including Cisco, Microsoft, and Avaya.

VOSS Automate supports single vendor and multi vendor installations.

Vendor	Solution
Cisco	Provides for customized UC app management via the following capabilities: <ul style="list-style-type: none"> • 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
Microsoft	See Introduction to Microsoft UC Integration Provides a single, integrated, synchronized interface for managing the existing Microsoft Teams collaboration service, through the web portal, bulk-loading, or the REST API. <ul style="list-style-type: none"> • 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.
Avaya	Manage Avaya enterprise voice, extended into Microsoft Teams.

Related Topics

- Multi Vendor Subscribers in the Core Feature Guide
- Microsoft Overview in the Core Feature Guide

3.3. Getting Started

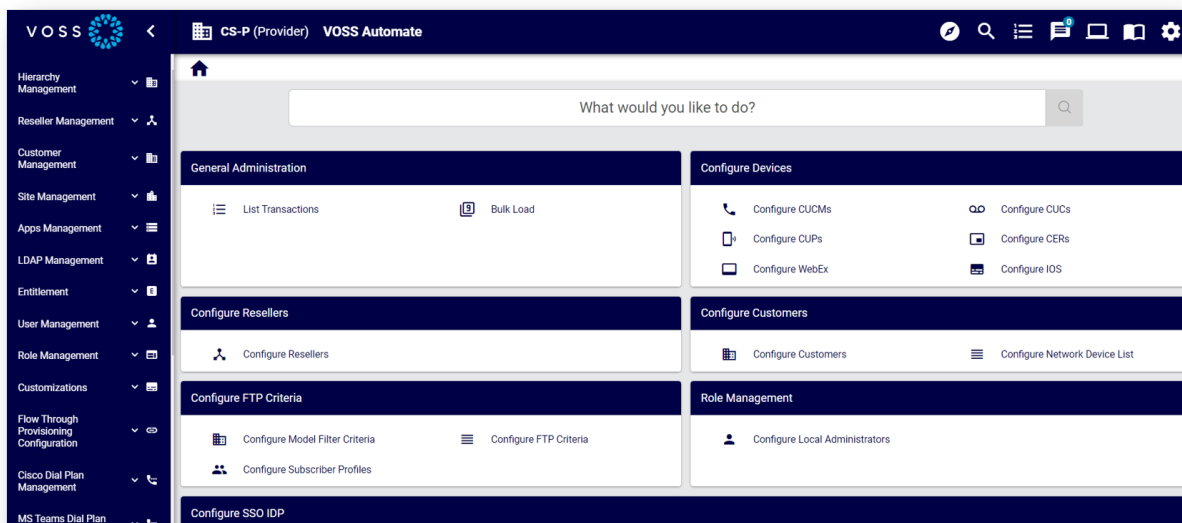
3.3.1. Introduction to the Admin Portal User Interface

This topic describes the user interface for the VOSS Automate Admin Portal.

Note: VOSS Automate v21.2 ships with a new logo and an updated look and feel, including additional options for customized themes. Additionally, VOSS-4-UC is now VOSS Automate. As at v21.2, you may still see some references to VOSS-4-UC. These will be replaced in future versions.

Related Topics

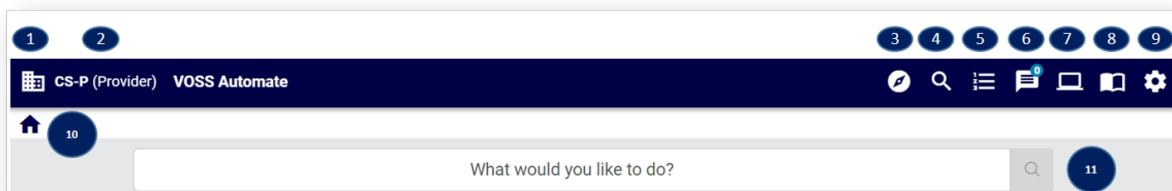
- Introduction to Themes in the Core Feature Guide
- Theme Customization topics in the Advanced Configuration Guide



The Admin Portal Menu Bar

The table describes the information and controls available on the Admin Portal menu bar:

Admin Portal:



1. Hierarchy tree view	A hierarchy tree view and pop-up displays a tree or list of available nodes. See Navigating the Hierarchy
2. 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 Navigating the Hierarchy .
3. Search (Compass icon)	What would you like to do? Launches a free text search field where you can search on actions, such as <i>Modify subscriber</i> . Performs the same search as the Search field in the header on the Home page.
4. Search (Magnifier icon)	Launches a Quick search / Global search dialog, where you can choose either Quick Search (search predefined options), or select Global Search to specify search queries and perform an advanced search.
5. Transactions list	Opens the transactions list, where you can view a list of recent transactions and drill-down to view transaction details.
6. Notifications indicator	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. System mode	Allows you to switch between the Admin Portal and Business Admin Portal.
8. Help button	Opens the system Help file in a new browser tab.
9. User profile (Cog icon)	The logged in user's username and role, with a drop-down menu for logging out or changing the password. Logout and password change is not available for SSO users. For details about logging out from an identity provider (IdP) initiated session, see the relevant user documentation for the relevant IdP.
10. Landing page	A customizable landing page and a Home navigation button to return to the Home page. See "Create a Landing Page" for details. <ul style="list-style-type: none"> • 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.
Copyright © 2021 Vooss Solutions Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@vooss-solutions.com	A search field to perform a fuzzy, free text, actions search, for example, <i>Modify Voicemail</i> or <i>Create subscriber</i> .

Forms and Lists

The Admin Portal displays information in forms and lists.

- Detail forms: 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.

Slide out notifications

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.

Accessibility

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 menu bar 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 landing page menu items. Press <Tab> to move the focus to the first landing page link.
- **Skip to navigation** - on the main user interface, move the focus to the menu bar. The first menu item receives focus.

Sessions and Authentication

Since VOSS 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.

Button Bar

For certain models, such as Roles or Credential Policy, the list view or detail view of the Admin Portal shows a button bar with a number of controls. The buttons displayed depend on the Access Profile of the user.

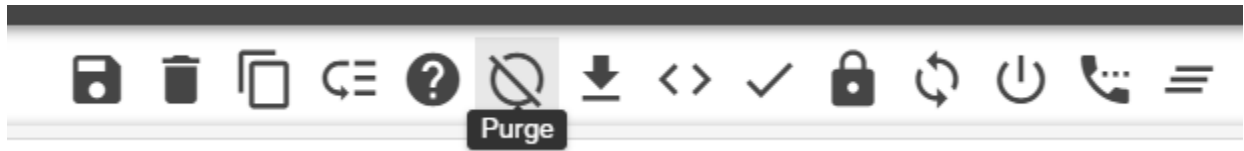
Button	Description
Add	When viewing a list, the button opens an Add form to create a new item.
Save	On the Add form, the button is used to save a newly created item. On the detail view, the button is used to save changes made to the specific item.
Delete	From a list, remove an entry or the selected entries.
Cancel	Used to cancel triggered events such as transactions, bulk loads, and so on.
Back	On the detail view, the button returns to the original list page position. The browser's back button also carries out this task.
Help	Open the on-line help page for the current model.
Move	For selected model instances, move them from the current hierarchy to another hierarchy. By default only device models have a Move button. This button is available on list and instance Admin Portal screens. When moving device models, checks are built in to disallow moving a device model instance to a hierarchy node with a different device. For Data Models, Move is allowed by editing the Data Model's definition in the Operations section.

The **Action** menu provides actions applicable to the specific view.

List View Action	Description
Bulk Load File	Only used in Administration Tools > Bulk Load , 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.

List View Action	Description
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: <ul style="list-style-type: none"> • 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.
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.
Move	For selected model instances, move them from the current hierarchy to another hierarchy. By default only device models have a Move button, which is available on list and instance Admin Portal screens. When moving device models, checks are built in to disallow moving a device model instance to a hierarchy node with a different device. For Data Models, Move is allowed by editing the Data Model's definition in the Operations section.
Clone	Make a copy of the current item. An option is available to rename the copied item.
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.
Export	Export a specific item with all its attributes.
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.
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.

On the Admin Portal GUI, buttons and icons to carry out actions - according to the form contents, e.g. Phone.



- Save
- Delete
- Clone
- Move
- Help
- Purge
- Export
- JSON Editor
- Apply
- Lock
- Reset
- Restart
- Vendor Config
- Wipe

On-line Help

Press the **Help** button on both the Main Menu button bar as well as the Button bar to open a new browser tab to show on-line help for your system. The new browser tab shows the following menu options:

1. General Help: General help information for the application.
2. Model Detail Help: Model (Item) specific help, for example data/GeneralHelp. This content may vary according to the Field Display Policy that is applied to the item.
3. Model API Help: the API reference for the item.

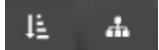

When the **Help** button (?) is pressed on the Main Menu button bar, only the three menu options are shown. When the **Help** button is pressed on the Button bar, context sensitive help specific to the associated form is also shown.

If a Field on the context sensitive help for an item is marked with an asterisk next to the field name, it is mandatory and must be filled out in order for the subsequent transaction to be successful.

A user's view of the available on-line help depends on hierarchy level, role-based access, and field display policies.






Main Page Controls



The following controls are available on the Admin Portal.

Icon	Description
	These icons are used to access the hierarchy.
	This icon is used to return to the main application page.

Form Controls

The following controls are available from a form.

Icon	Description
	Open another instance of the current form field or open a pop-up screen to add an item.
	Delete the current instance of a field from a form or open a pop-up screen to confirm.
	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.
	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 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.

Icon	Description
	On multi-tabbed forms, navigate to the previous or next tab.
	A warning icon, 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.

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.

About

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

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 with HCMF
 - Provider Decoupled
 - 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:** VOSS 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>)
```

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

3.3.2. Manage Items

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.
- 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.

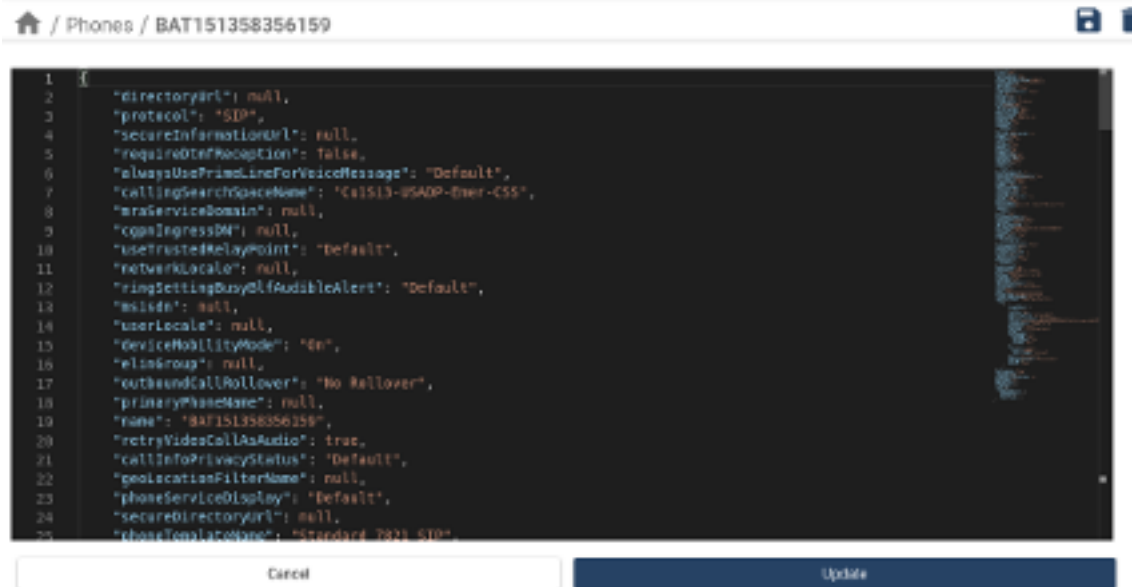
Edit in the JSON Editor

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.
- 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

VOSS Automate allows you to 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:

- 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, e.g. Subscribers, 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, Reskill Agents (Contact Center) and Upload Multiple Files to MOH Clusters.

Transfer boxes allow you to select only certain items to process in a specific transaction. For example, you may want to perform an audit on numbers from selected sites only.

A maximum of 200 items can be displayed in the **Available** transfer box. In cases where there are more than 200 available items, VOSS recommends that you use the bulk load functionality and populate a bulk load template with the required entries. You can then load this into VOSS Automate using the Bulk Load administration tool. Refer to [Bulk Load Template Export](#) and associated topics for more information.

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).
-

3.3.3. Working with Lists

Overview

Summary views of resources and services are shown in lists in the VOSS 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.

<input type="checkbox"/>	User Name	First Name	Last Name	Email Address	Role	Entitlement Profile
<input type="checkbox"/>	Filter	Filter	Filter	Filter	Filter	Filter
<input type="checkbox"/>	Aaron.Farnes	Aaron	Farnes	aaron.farnes@geologic.net	GLGC-MadridSelfService	["GeoLogic-Premium-EP", "hcs.CS-P.Geol
<input type="checkbox"/>	abdul.bernat	Abdul	Bernat	abdul.bernat@kittycat.net	CAT-BristolSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	Abel.Timoteo	Abel	Timoteo	abel.timoteo@geologic.net	GLGC-LyonSelfService	["GeoLogic-Standard-EP", "hcs.CS-P.Geol
<input type="checkbox"/>	abraham.ruark	Abraham	Ruark	abraham.ruark@kittycat.net	CAT-ReadingSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	adah.blas	Adah	Blas	adah.blas@catnip.com	CAT-AliceSpringsSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	adam.stlawrence	Adam	Stlawrence	adam.stlawrence@kittycat.net	CAT-BrisbaneSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	addie.strack	Addie	Strack	addie.strack@catnip.com	CAT-ElwoodSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	adria.hammers	Adria	Hammers	adria.hammers@kittycat.net	CAT-WollongongSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	Adriene.Lanza	Adriene	Lanza	adriene.lanza@geologic.net	GLGC-GlasgowSelfService	["GeoLogic-Premium-EP", "hcs.CS-P.Geol
<input type="checkbox"/>	afon.mcnamara	Afon	Mcnamara	afon.mcnamara@kittycat.net	CAT-BronxSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	ahmed.callicot	Ahmed	Callicot	ahmed.callicot@kittycat.net	CAT-EdinburghSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	albert.behrens	Albert	Behrens	albert.behrens@kittycat.net	CAT-BrisbaneSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	aleen.brewton	Aleen	Brewton	aleen.brewton@catnip.com	CAT-BronxSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	alejandro.wallace	Alejandro	Wallace	alejandro.wallace@catnip.com	CAT-EdinburghSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	alessandra.almeida	Alessandra	Almeida	alessandra.almeida@kittycat.net	CAT-BristolSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	alfonso.malooof	Alfonso	Malooof	alfonso.malooof@catnip.com	CAT-BronxSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	alfonzo.rook	Alfonzo	Rook	alfonzo.rook@kittycat.net	CAT-BrisbaneSelfService	["Catnip-Standard-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	alfred.papineau	Alfred	Papineau	alfred.papineau@catnip.com	CAT-ReadingSelfService	["Catnip-Premium-EP", "hcs.CS-P-CS-NB.C
<input type="checkbox"/>	Ali.Tison	Ali	Tison	ali.tison@geologic.net	GLGC-BristolSelfService	["GeoLogic-Premium-EP", "hcs.CS-P.Geol

Refresh Lists

List views refresh by default . . .

- When a transaction (related to items you're viewing on the list) completes.
- When clicking again on the menu option for the list. For example, when looking at a list of phones (default menus: **Cisco Subscriber Management > Phones**), clicking the **Phones** menu in the left navigation refreshes the 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.

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:

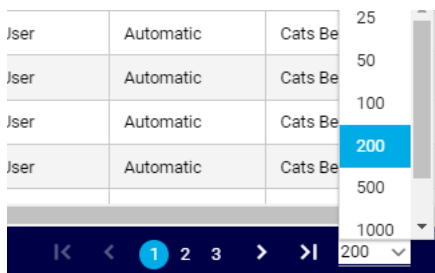
- Cells with no value move to the top or bottom of the list, depending on the sort order (ascending or descending).

- Upper case letters 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.

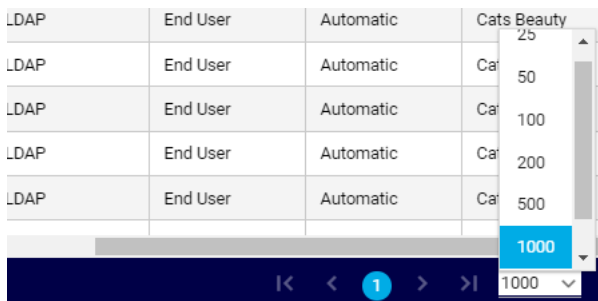
Navigate Lists

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

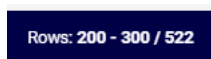
- To navigate across a multiple page list, click the right/left arrow to scroll to the next/previous page, or click a page number.



- 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

The list filter functionality you'll see in VOSS Automate depends on whether you're using the classic Admin GUI or the Admin Portal (introduced at v21.2).

Note: This topic describes filtering on resource and service summary lists. For details around filtering transactions, sub-transactions, and log lists, see [Filtering 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 landing page. The filter is retained for the list only when opening the list from a menu (any menu where that list is available).

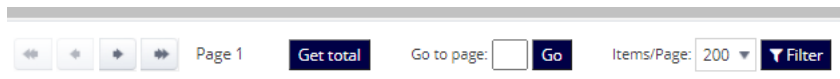
The same applies for lists that you launch from a landing page, when you create and apply a filter to the list you opened from the landing page. In this case, the filter is only retained on the list when you open that list from a landing page (any landing page where that list is available)

Filtering Lists in the Classic Admin GUI

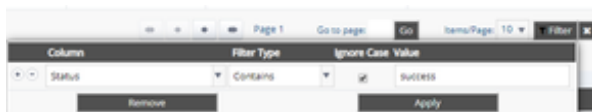
The legacy Admin GUI provides a filter dialog for specifying one or more search criteria to apply to the list.

To filter lists in the legacy Admin GUI:

1. Log into the VOSS Automate Admin GUI.
2. Open a list view for a resource or service. For example, (default menus) **User Management > Users**.
3. Open the **Filter** dialog. Two options are available:
 - Click the **Filter** button located at the bottom of the list (adjacent to the **Items/Page** drop-down).



- Mouseover any column header to display the **Filter** icon, then click on the icon to open the **Filter** dialog. In this case, the first filter defaults to the column name, but you can specify any filter you choose (one or more), and the filter applies to all data in the list.
4. To specify filter criteria, choose a column, a filter operator, and a value.



Available filter operators:

- Contains (default)
- Does Not Contain
- Starts With
- Ends With

- Equals
 - Not Equal
5. Clear the **Ignore Case** checkbox to create a case-insensitive search. This checkbox is selected by default.

Note: To filter for empty rows in a specific column, you can choose any filter type, select **Ignore Case**, and type *None* in the **Value** field of the **Filter** dialog. This works for all list views except Subscriber.

5. Specify additional filters, if required. To remove any of the filters, click **Remove**.

Note: The combination of filters you set up creates a single filter; that is, all filter rows are applied (in a logical AND) when you run the filter.

5. Click **Apply** to run the filter.
6. View the filtered list.

Note:

- While a filter is applied, clicking on a column header to sort data is only supported for the **Starts With** operator.
 - The **Located At** column only filters on the name of the hierarchy (for example, the site name), and not on the hierarchy type itself (for example, site, or customer).
 - You can perform additional actions on a filtered list, for example, to select a number of items in a filtered list to move or delete the items.
-

Filter Operators and Column Value Types

- You can use all filter operators on string value columns.
- You can use all filter operators on Boolean value columns, provided values are “True”, “true”, “False” or “false”.
- For number value columns, you can also use *Equals* and *Not Equal* filter operators.
- When filtering on decimals in number value columns:
 - To filter floating point values in number value columns, specify at least one decimal digit, for example, 2.0.
 - Filtering can be applied to values with decimal values up to 7 decimals. For example:

Consider a list of values, and the following filter: Not Equal to 2.00000001

2.20000001
2.00000001
2.000000001

In this case, the filter displays only one value (2.20000001), because the filter value exceeds 7 decimals.

Filters and Model Lists

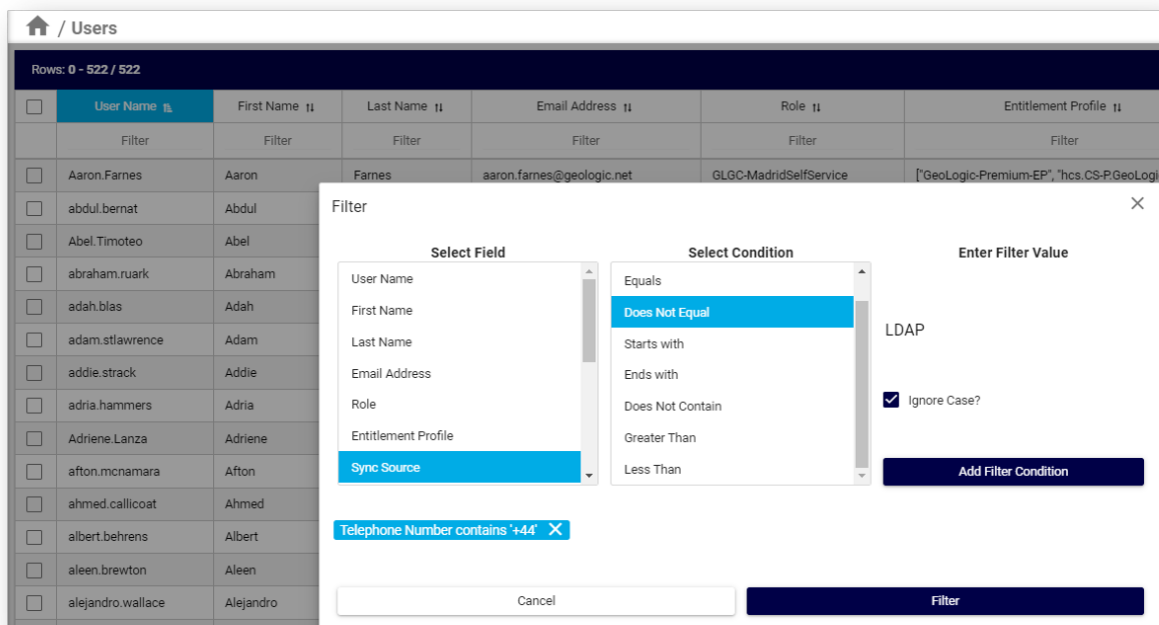
If access is available to specific models, such as configuration templates and macros, filters apply to *all* the instances in the hierarchy, since the listing of instances in these models is not restricted to a user's hierarchy.

Standard list view filters on model types are removed and replaced by any configurable filters on landing page links or menu items for the corresponding model type when these are used. See [Fixed and Configurable Filters in Menus and Landing Pages](#).

Filtering lists in the Admin Portal

The Admin Portal (introduced at v21.2), provides two options to filter a list view:

- Advanced filter, via a **Filter** dialog.
- Quick filter, via **Filter** fields below the column header row.



To filter lists in the Admin Portal:

1. Log into the Admin Portal.
2. Open a list view for a resource or service. For example, (default menus) **User Management > Users**.
3. Add filters. Two options are available:
 - Option 1: Advanced filter

Click the toolbar Filter icon () to launch the **Filter** dialog. 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**.

- Repeat this step for all the filters you want to apply to the list.
- Click **Filter**
- Option 2: Quick filter

Click in the **Filter** field below a column header, and add filter criteria. You can add criteria to one or more columns. The filter applies once you tab out of the field.

Column sort options may be disabled by the filters.

4. View filter results in the list view.

The applied filter criteria displays at the top of the list.

To clear any filter, click the red X icon at the relevant **Filter** field, or click the red X icon in the first column to clear all filters. Alternatively, click on the **Filter** text link (or on the toolbar Filter icon) to open the **Filter**, where you can remove one or more filters.

The banner above the header row displays:

- The number of result rows matching the filter.
- The applied filter, as a clickable text link. Clicking on the filter opens the **Filter** dialog, where you can add, modify, or remove filters.
- Filter values, which display in the **Filter** fields beneath the relevant column headers.

The screenshot shows a table of users with a filter banner at the top. The filter banner reads: "Filter: User Name contains 'j' and First Name contains 'm' and Sync Source contains 'c' and Sync Type contains 'l' and User Type contains 'e'". The table has columns for User Name, First Name, Last Name, Email Address, Role, Entitlement Profile, Sync Source, Sync Type, and User Type. The first row is filtered out, indicated by a red 'X' in the first column. The remaining rows show users like marloj, jamie.turner, hyman.julien, Jimmy.Leong, Jimmie.Bolyard, and jamar.gouge.

<input type="checkbox"/>	User Name	First Name	Last Name	Email Address	Role	Entitlement Profile	Sync Source	Sync Type	User Type
<input checked="" type="checkbox"/>	j	m	Filter	Filter	Filter	Filter	c	l	e
<input type="checkbox"/>	marloj	Marlo	Jooste	marloj@kittycat.net	CatnipSelfService	['Catnip-NoService-EP', 'hcs-CS-P-CS-NB.Catnip']	CUCM	CUCM-Local	End User
<input type="checkbox"/>	jamie.turner	Jamie	Turner	jamie.turner@voss-solutions.com	CS-PSelfService	['Catnip-Premium-EP', 'hcs-CS-P-CS-NB.Catnip']	CUCM	CUCM-Local	End User
<input type="checkbox"/>	hyman.julien	Hyman	Julien	hyman.julien@kittycat.net	CAT-WollongongSelfService	['Catnip-Standard-EP', 'hcs-CS-P-CS-NB.Catnip']	CUCM	CUCM-Local	End User
<input type="checkbox"/>	Jimmy.Leong	Jimmy	Leong	jimmy.leong@geologic.net	GLGC-BristolSelfService	['GeoLogic-Premium-EP', 'hcs-CS-P-GeoLogic']	CUCM	CUCM-Local	End User
<input type="checkbox"/>	Jimmie.Bolyard	Jimmie	Bolyard	jimmie.bolyard@geologic.net	GLGC-LyonSelfService	['GeoLogic-Premium-EP', 'hcs-CS-P-GeoLogic']	CUCM	CUCM-Local	End User
<input type="checkbox"/>	jamar.gouge	Jamar	Gouge	jamar.gouge@sickly.com	SKL-TolucaSelfService	['Sickly-Foundation-EP', 'hcs-CS-P-Sickly']	CUCM	CUCM-LDAP	End User

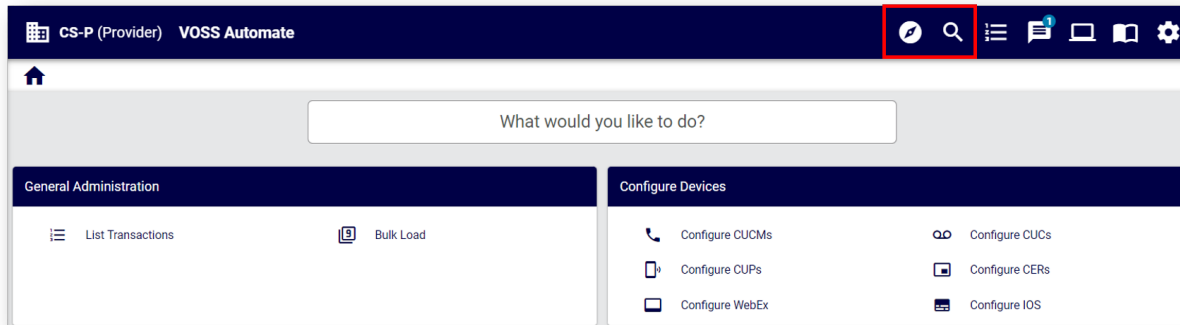
3.3.4. Search in VOSS Automate

Overview

Search Methods

There are two ways to run a search in the VOSS Admin Portal:

- *What would you like to do?* (action/navigation search)
Click the **Compass** icon, or type search criteria in the text field (from the Home page)
- Quick / Global search (*Advanced Search (Quick/Global)*)
Click the **Search** icon (magnifier) to launch the Search dialog.



Note: VOSS Automate 21.3 Patch Bundle 2 ships with an early field trial of its enhanced Search feature. This feature has been tested internally, has shown to have no impact on general system performance, and works for most use cases, as described on this page. Minor aspects of the functionality may not work as expected, for example, enhancements to search phrase use is reserved for future development.

Best Practices for Meaningful Search Results

Search results are based on the menus and landing pages allowed and configured for your role. For this reason, administrators should align naming conventions and the setup of items for user navigation with terms that are familiar to users. For example:

- Adjust the names of menus, landing pages, tasks, and quick actions if these prove to be unintuitive.
- Configure relevant landing pages for quick actions, based on user roles.
- Use the *What would you like to do?* search to quickly find actions that aren't available on landing pages.

What would you like to do?

Search using the Compass icon or search field (What would you like to do?) is a quick way to navigate to a menu item or a landing page link.

Click the toolbar **Compass** icon to run a search on 'actions' based on a search phrase or a single word, such as *add line*, *update subscriber*, or *phones*, to navigate quickly to a relevant form, view, or list.

Note: Verbs in the search phrase return results when matching the same word in a menu or landing page, based on your access profile.

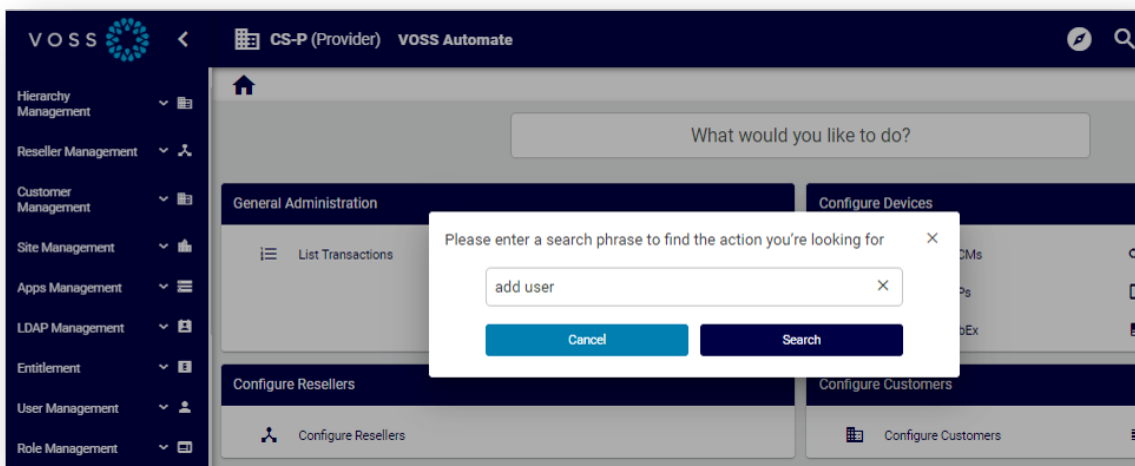
You can also run this search directly from the Home page, where you can click in the Search field, fill out a search phrase or word, and press **Enter**.



The Compass search is a case-insensitive, fuzzy, free text search, with results based on the menu layout and landing page links for your access profile. All relevant items are returned. For example, including *add* in your search phrase also generates results for *create* and *add*.

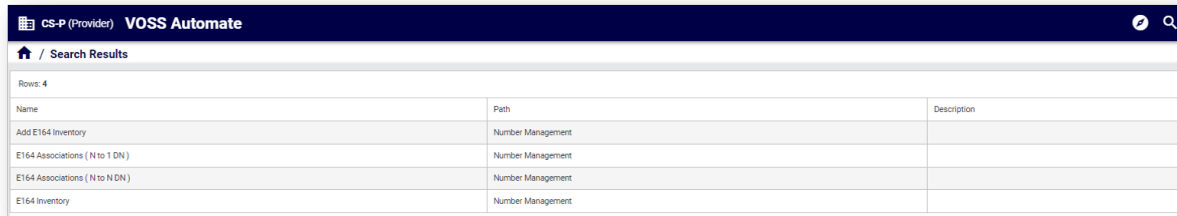
Important: At the time of writing (for 21.3-PB2):

- Plural keywords may not return all relevant results. If you don't see the results you expect, change the keyword to singular, for example, *phone* instead of *phones*, or *add subscriber*, instead of *add subscribers*.
- Using generic terms, such as *subscriber* or *phone*, returns all items relating to this keyword.
- Avoid search phrases that include *a* or *an*. For example, use *add user* instead of *add a user*.
- Search phrases that refer to a device, such as CUCM, returns all items (including device models) that have the device name in the label or description. Additionally, the phrase *add device* returns a list of results where the label starts with *device*, where the access profile allows the add operation, and (in this case), labels, descriptions, or models containing the full string, *add device*.
- For best results (depending on the permissions you have on the model types), use the following verbs in search phrases:
 - create, add
 - update, edit, modify, change
 - delete, remove



Search criteria supports abbreviations, model type keywords (such as view, relation, model), and matches for the first character of words in a string. For example, *QAS* returns *QAS - MS Teams*, as well as *Quick Add SIP Gateway*.

Note: Including numerical digits in the search criteria only returns menus with digits in the menu name. For example, search criteria including the digits *1*, *6*, or *4* returns menus with these digits in their name, such as *E164 Inventory* (by default, a sub-menu in the **Number Management** menu).



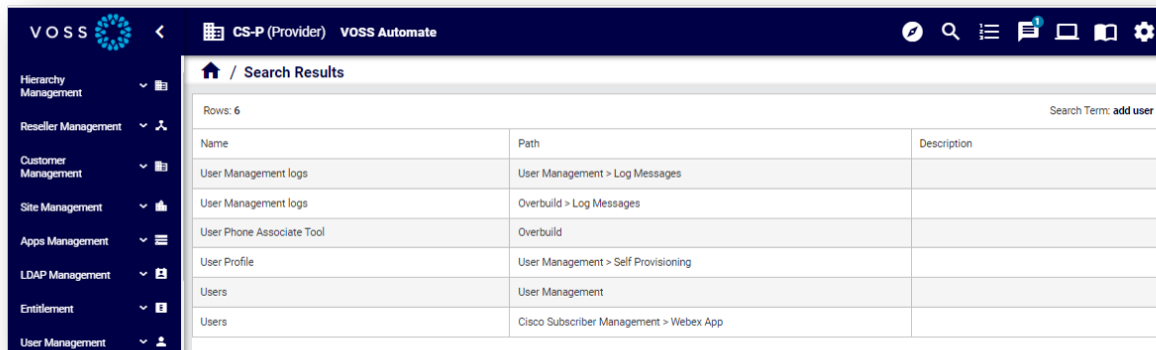
CS-P (Provider) VOSS Automate

Search Results

Rows: 4

Name	Path	Description
Add E164 Inventory	Number Management	
E164 Associations (N to 1 DN)	Number Management	
E164 Associations (N to N DN)	Number Management	
E164 Inventory	Number Management	

Search results display in a table, including the path.



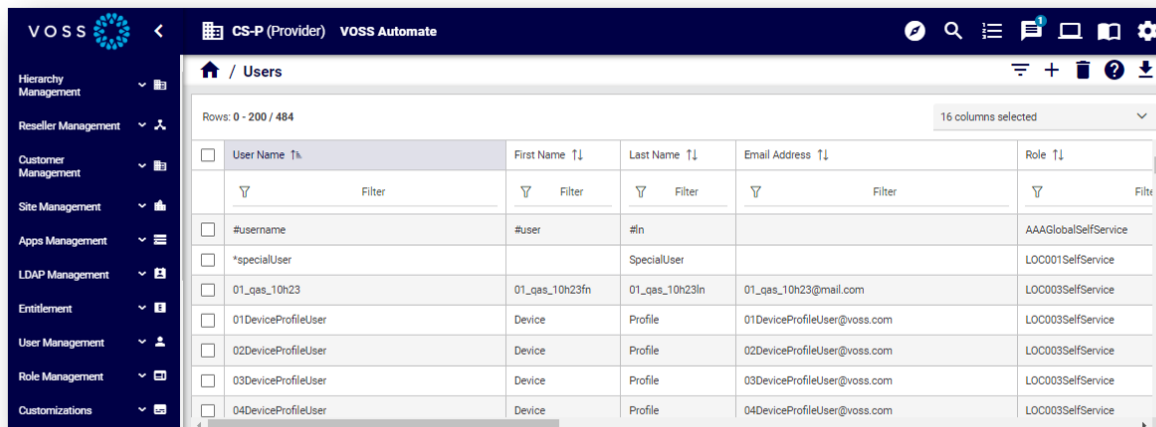
VOSS CS-P (Provider) VOSS Automate

Search Results

Rows: 6 Search Term: add user

Name	Path	Description
User Management logs	User Management > Log Messages	
User Management logs	Overbuild > Log Messages	
User Phone Associate Tool	Overbuild	
User Profile	User Management > Self Provisioning	
Users	User Management	
Users	Cisco Subscriber Management > Webex App	

Click on a search result to open it in the system.



VOSS CS-P (Provider) VOSS Automate

Users

Rows: 0 - 200 / 484 16 columns selected

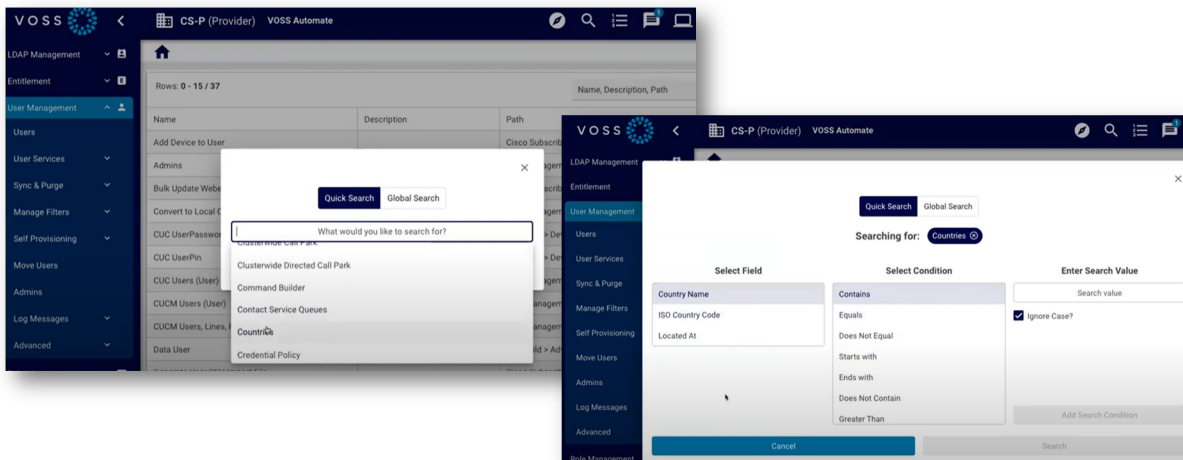
<input type="checkbox"/>	User Name $\uparrow\downarrow$	First Name $\uparrow\downarrow$	Last Name $\uparrow\downarrow$	Email Address $\uparrow\downarrow$	Role $\uparrow\downarrow$
	$\uparrow\downarrow$ Filter	$\uparrow\downarrow$ Filter	$\uparrow\downarrow$ Filter	$\uparrow\downarrow$ Filter	$\uparrow\downarrow$ Filter
<input type="checkbox"/>	#username	#user	#fn		AAAGlobalSelfService
<input type="checkbox"/>	*specialUser		SpecialUser		LOC001SelfService
<input type="checkbox"/>	01_qas_10h23	01_qas_10h23fn	01_qas_10h23ln	01_qas_10h23@mail.com	LOC003SelfService
<input type="checkbox"/>	01DeviceProfileUser	Device	Profile	01DeviceProfileUser@voss.com	LOC003SelfService
<input type="checkbox"/>	02DeviceProfileUser	Device	Profile	02DeviceProfileUser@voss.com	LOC003SelfService
<input type="checkbox"/>	03DeviceProfileUser	Device	Profile	03DeviceProfileUser@voss.com	LOC003SelfService
<input type="checkbox"/>	04DeviceProfileUser	Device	Profile	04DeviceProfileUser@voss.com	LOC003SelfService

Advanced Search (Quick/Global)

Click the toolbar **Search** icon (magnifier) to launch an advanced search filter where you can perform a quick search of list views exposed by the menu layout, or a global search, in which you can specify the model to search on.

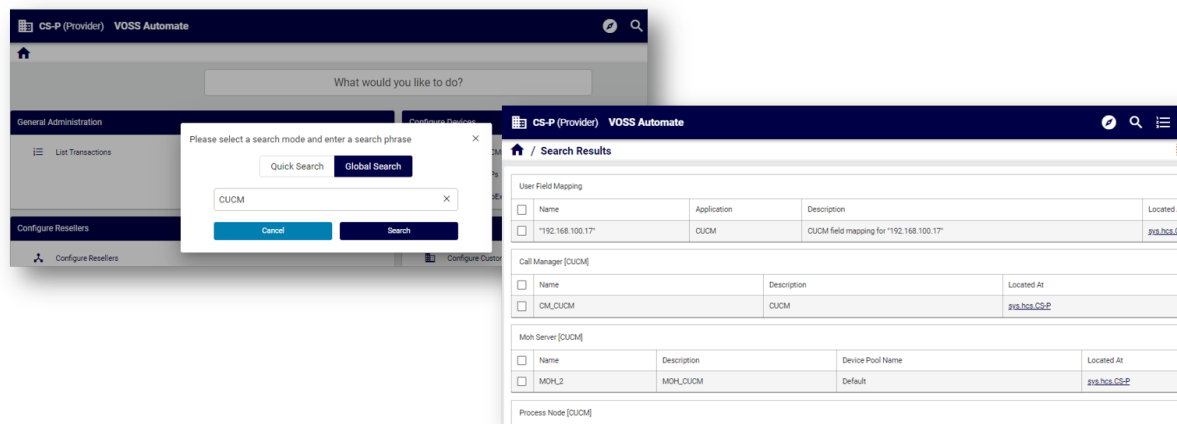
Quick Search

Quick search allows you to select an entity from a drop-down of list views based on menu layouts for your access profile. Once you choose an entity, you can filter results to specify a search value, to choose the relevant field (related to the model) and search condition (for example, an operator such as *Contains*, *Equals*, or *Starts with*), and define whether to perform a case-sensitive search.

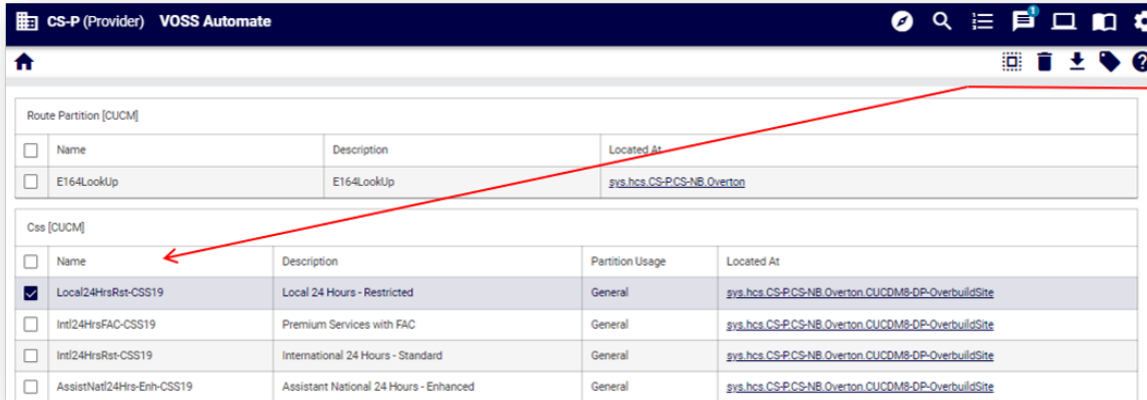


Global Search

Global search allows you to fill out search criteria (a search term or query), and run an advanced search that queries the API for the relevant model and search criteria.



For the global search results, 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.



Search results are permissions-based for your access profile, with caveats on number of items, relations, and device models.

- Search results are returned for your current hierarchy and below.
- Click on a search result to open it and view its details.
- Search results for a simple string search matches the start of 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 Global Search Queries

Global Search Syntax

You can construct search queries to search for specific items, based on VOSS Automate search syntax filters.

Search queries can contain:

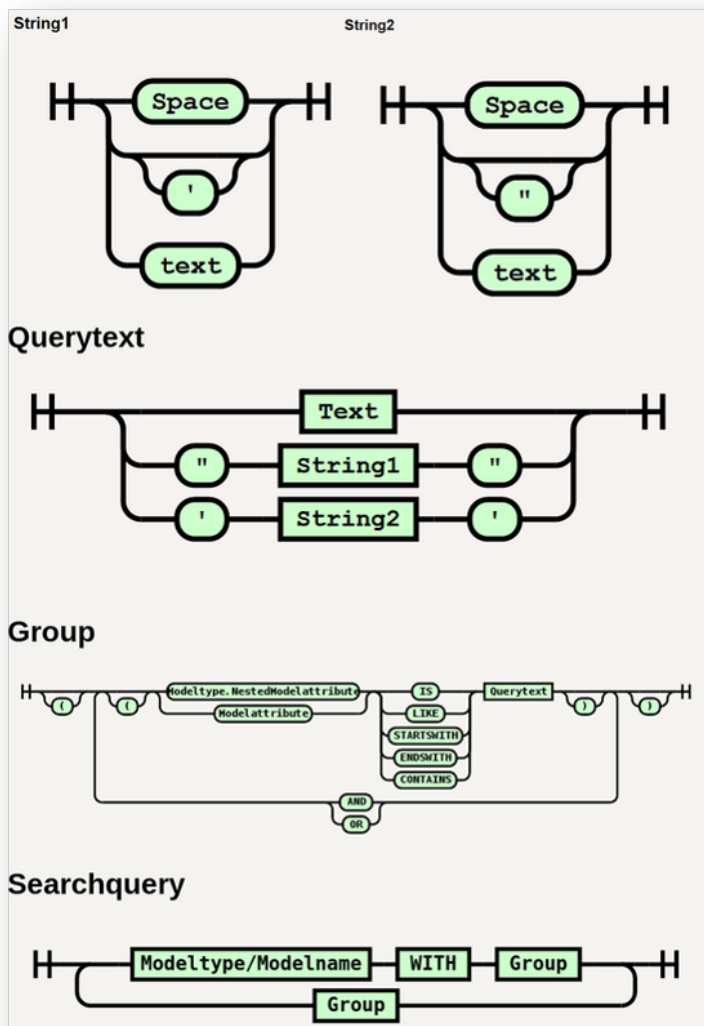
- Model type and model name references
- Model attribute and nested model attribute references
- Key words
- Brackets, for grouping
- Query string, using valid query string characters, as follows:

- 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`).



Global 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	<p>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.</p> <pre>((data/Countries WITH country_name LIKE Kingdom) AND (data/Countries WITH country_name LIKE Unite))</pre>
IS	<p>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.</p> <pre>country_name IS Spain data/Countries WITH country_name IS Spain</pre> <p>Another example with a model tag as reference:</p> <pre>tag IS "featurea"</pre>
CONTAINS	<p>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'.</p> <pre>data/Countries WITH country_name CONTAINS Sw</pre>

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'. <code>data/Countries WITH country_name LIKE swe</code>
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. <code>((data/Countries WITH country_name LIKE Kingdom) AND (data/Countries WITH country_name LIKE Unite))</code>
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'. <code>((data/Countries WITH country_name LIKE Kingdom) OR (data/Countries WITH country_name LIKE Unite))</code>

Global 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))
```

Global Search String Format

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

Multi-word and quotes Enclose in quotes. Single- and double quotes are supported. Example: '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.

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.

Search in Drop-Down Lists

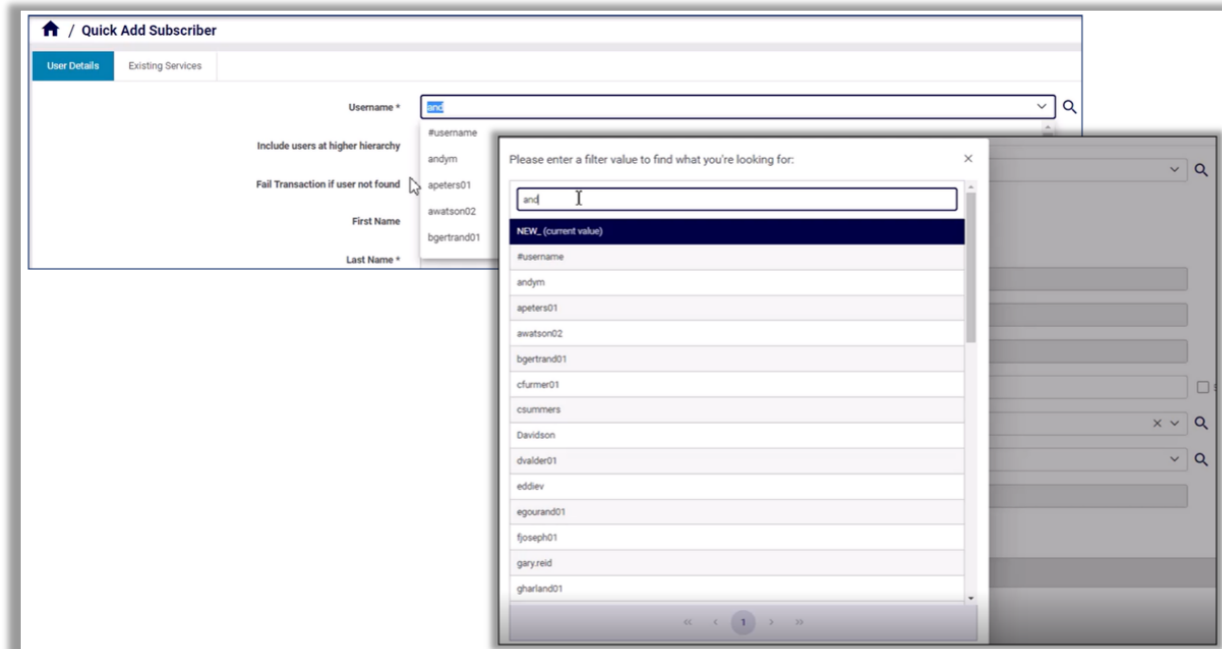
On forms where you select values from pre-populated, editable drop-down lists, VOSS Automate allows you to run a case-insensitive search to filter results.

Run a 'Contains' search

You can start typing in a drop-down field to run a **contains** search on the *first 1000* results.

Run a 'Starts with' search

If you don't find the result you're looking for, click the magnifier icon adjacent to the drop-down to perform a **starts with** search on *all results*.



3.3.5. 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
- device/cuc/Greeting
 - GreetingType
 - CallHandlerObjectId
- device/cuc/HtmlDevice
 - DeviceName
 - DisplayName
 - SubscriberObjectId
 - ObjectId
 - SmtAddress
 - 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
 - SmtAddress
- 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
 - 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
 - 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
 - associatedDevices.device
 - lineAppearanceAssociationForPresencesdepartment
 - lastName
 - primaryDevice
 - primaryExtension
 - phoneProfiles
 - status

3.3.6. 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
 - 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
 - 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
- 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
 - ownerId
 - 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
 - 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

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.

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.

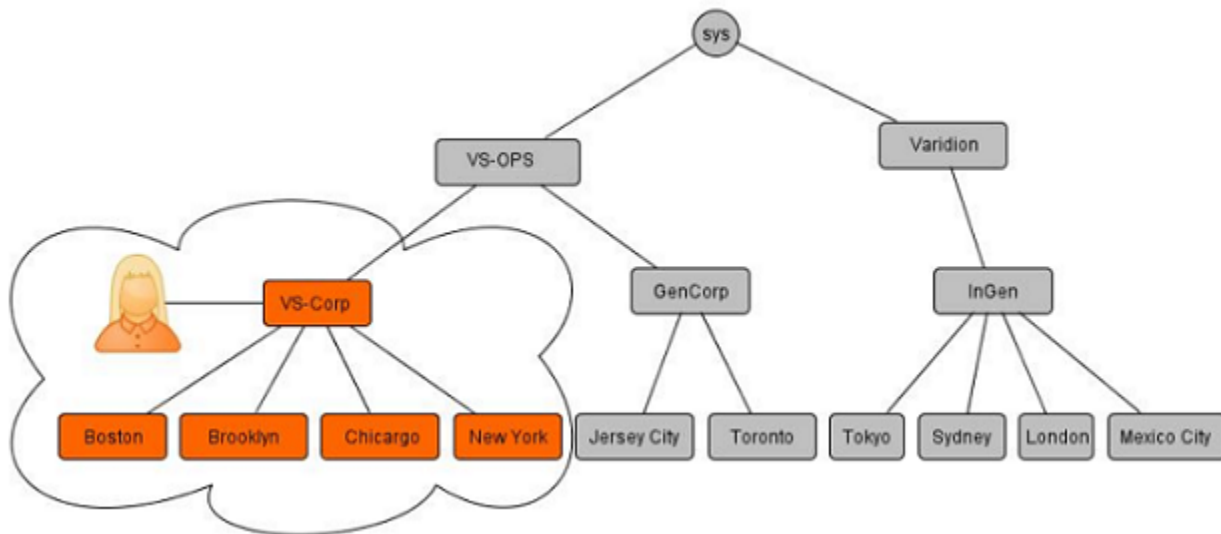
Hierarchy nodes and node types may include:

- 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.

4.1.4. Hierarchies and User Roles

VOSS 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 [Role-based Access](#).

- 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 describes models with **Visible at Lower Hierarchy** set to *true*:

Name	Model Type
AccessProfile	data/DataModel
Adaptation	data/DataModel
AdaptationLog	data/DataModel
BulkAdminDataRefreshPerHierarchy	data/DataModel

continues on next page

Table 1 – continued from previous page

Name	Model Type
BulkAdminFullDataRefresh	data/DataModel
BulkAdminScheduleDataRefresh	data/DataModel
Bundle	data/DataModel
Bundle	data/Relation
ConfigurationTemplate	data/DataModel
Countries	data/DataModel
CredentialPolicy	data/DataModel
FeatureConfigProfile	data/DataModel
FieldDisplayPolicy	data/DataModel
HcsCommandBuilderDAT	data/DataModel
HcsDeviceGroupDAT	data/DataModel
HcsDeviceTypeDAT	data/DataModel
HcsDpDialPlanSchemaDAT	data/DataModel
HcsDpDialPlanSchemaGroupDAT	data/DataModel
HcsLocalizedStringDat	data/DataModel
HcsMovePhoneCustomizationsDAT	data/DataModel
HcsMoveSubCustomizationsDAT	data/DataModel
HcsPrimeCollabREL	data/Relation
LandingPage	data/DataModel
Macro	data/DataModel
MenuLayout	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

- Network Device Lists in the Core Feature Guide
- VOSS Automate Configuration and Sync in the Core Feature Guide

4.2. Navigating the Hierarchy

4.2.1. Overview

A number of Admin Portal features are available to quickly and effectively navigate to a required hierarchy level and to set the context for various actions in the system at that level.

4.2.2. Bread crumbs

Navigate through the hierarchy by using the hierarchy bar at the top of the page. Each hierarchy node selection from a drop-down list on the bar that is a parent node may enable a lower level drop-down list, creating a “bread crumbs” list of the hierarchy path. Long lists show a scroll bar in the drop-down lists.

If more than 2 items are in the drop-down list, a search box shows in the list input box. A *case-insensitive* search can be carried out with a string that is *contained* in the name.

4.2.3. Hierarchy Tree View

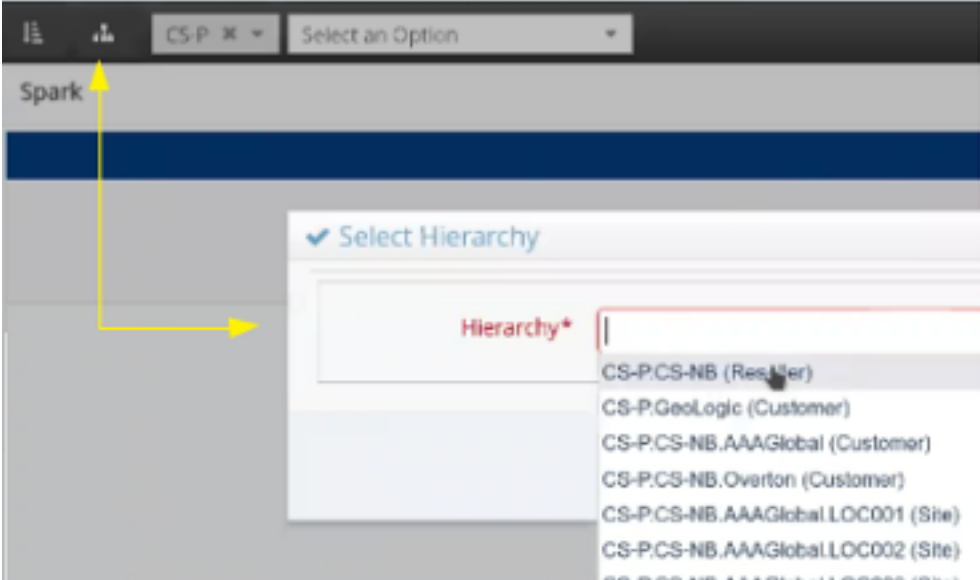
Use the tree view icon on the hierarchy bar at the top of the page to show a tree view of the entire hierarchy. Choose a hierarchy node on the tree to easily navigate to that node.

The nodes in the tree also show its hierarchy type: Provider, Reseller, Customer, Site.

The screenshot displays the VOSS Admin Portal interface. At the top, the breadcrumb navigation shows 'CS-P (Provider)' and 'VOSS Automate Provider'. A left sidebar contains various management options. The main content area features a dialog box titled 'Please select an organization level' with a search filter and buttons for 'Show Current Tree', 'Toggle Resellers', and 'Toggle Customers'. Below these buttons, a tree view shows the hierarchy starting with 'CS-P (Provider)', which is expanded to show 'CS-NB (Reseller)' and 'GeoLogic (Customer)'. Under 'GeoLogic (Customer)', several sites are listed: 'GLGC-Barcelona (Site)', 'GLGC-Belfast (Site)', 'GLGC-Bristol (Site)', 'GLGC-Cardiff (Site)', and 'GLGC-Dublin (Site)'.

4.2.4. Hierarchy Pop-up View

Use the hierarchy pop-up view icon on the hierarchy bar to show a pop-up box with a drop-down list of nodes available from the current hierarchy - according to the hierarchy rules that apply to the current node and user.



The input drop-down box can also be used for a *case insensitive* search with a string *contained* in the name of the required node, thereby filtering the drop-down list.

Since the nodes in the drop-down list also show the node hierarchy type (Provider, Reseller, Customer, Site), the list can therefore also for example be filtered case insensitively to show those for example containing "Site".

4.2.5. List View Hierarchy Links

For list views, the hierarchy level to which an object belongs is indicated in the hierarchy column is called **Located At**.

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 will set the hierarchy to the selected hierarchy in the top "bread crumbs" bar and the items in the list view are filtered accordingly.

Last Name	Email	User Type	Entitlement Profile	Located At
Pjones	pjones@voss-solutions.com	CUCM Local		Overton (Customer)
Build001	OscarBuild001@aaaglobal.com	CUCM Local		Overberg (Site)
Build002	OscarBuild002@aaaglobal.com	CUCM Local		Overberg (Site)
Build003	OscarBuild003@aaaglobal.com	CUCM Local		Overberg (Site)
Jones	pjones@voss-solutions.com	CUCM Local		Overberg (Site)

Note: The hierarchy bar is not refreshed automatically when for example Customers or Sites are deleted by another administrator user on another browser. The bar is refreshed when refreshing the browser.

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. Create a Provider

This procedure creates a provider hierarchy node in VOSS Automate and, optionally, a default provider administrator.

Note:

- References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.
- In VOSS Automate, the provider name is set to the current service provider name in HCM-F (if applicable).

Perform these steps:

1. Log in to VOSS Automate:
 - Enterprise deployment: Log in as entadmin at sys.hcs.
 - Provider deployment: Log in as hcsadmin at sys.hcs.
2. Go to (default menus) **Provider Management > Providers**.
3. On the **Providers** page, click **Add**.
4. On the **Service Provider Details** tab, complete the following fields:

Field	Description
Name	The name of the provider. The name is automatically set to the current service provider name in HCM-F (if applicable). You can keep the existing name or overwrite with a more meaningful name. This field is mandatory. Note: <ul style="list-style-type: none"> Once you've saved the provider, you can't change the provider name. Any spaces in the provider name are converted to under-scores in the provider local administrator name and email, if the Create Local Admin check box is selected.
Decouple SDR Name	Provider deployment only Choose this option to set a Provider name in VOSS Automate that is different from the service provider name in HCM-F. Service provider names that were synchronized from VOSS Automate 8.1(x) or are set to "All Service Providers" can remain unchanged in HCM-F. If you leave clear, the provider name you enter in the Name field is synchronized into HCM-F as the service provider name.
SDR Name	Provider deployment only The service provider name to store in the SDR on HCM-F. This field appears only if Decouple SDR Name is selected.
Description	A description of the provider.
Domain Name	The domain of the provider. For example, provider.com. Used when creating the default local administrator so the administrator can log in with an email ID such as ProviderAdmin@provider.com . This field is mandatory.
Create Local Admin	Defines whether a default local administrator is created.
Cloned Admin Role	For Provider deployments, the HCS default Provider role used to create a new role prefixed with the provider name. For Enterprise deployments, the ENT default Provider role used to create a new role prefixed with the provider name. The Provider role, shown in Default Admin Role field, is assigned to the default local administrator. This field appears only if the Create Local Admin check box is selected.
Default Admin Role	The created provider role that is assigned to the default local administrator. This field is read-only and appears only if the Create Local Admin check box is selected.
Default Admin Password	The password to assign to the default local administrator. This mandatory field appears only if the Create Local Admin check box is selected.
Repeat Default Admin Password	Confirm the default local administrator password. This mandatory field appears only if the Create Local Admin check box is selected.

- On the **Contact Information** tab, enter address, email, and phone information, as appropriate.
- Click **Save**.

4.5. Create a Reseller

Once VOSS Automate is installed, the entadmin administrator (Enterprise deployment) or hcs administrator (Provider deployment) configures the HCM-F device (if applicable), and creates the Provider.

Note:

- Creating a Reseller is optional.
- In VOSS Automate, if the Reseller name matches an OrgUnit in the SDR you can migrate the OrgUnit as a Reseller.
- References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

1. Log in as Provider administrator.

Log in with the Provider administrator's email address, which is case-sensitive. The hcsadmin administrator can find the Provider administrator's email address on the **Admins** form (default menu **User Management > Admins**, then click on the Provider's name).

2. Go to (default menus) Reseller Management > Resellers.**3. On the Resellers form, click Add.****4. On the Reseller Details tab, complete the following fields:**

Option	Description
Name	<p>Mandatory. The name of the reseller.</p> <ul style="list-style-type: none"> 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, if the Create Local Admin checkbox is selected. If the Reseller Name matches the name of an OrgUnit that exists in the SDR, the Migrate from HCM-F to VOSS Automate check box displays. Click Save to migrate this OrgUnit to a reseller at the current hierarchy level. The fields are populated with the values found in the SDR. If you don't want to migrate the OrgUnit, enter a different Reseller Name.
Description	Reseller description
Directory Domain	Reseller 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.
Create Local Admin	Defines whether a default local administrator is created for the reseller.
Cloned Admin Role	The Provider role used to create a new role prefixed with the reseller name. The created Reseller role, shown in the Default Admin Role field, is assigned to the default local administrator user. This field appears only if the Create Local Admin checkbox is selected.
Default Admin Role	The created Reseller role that is assigned to the default local administrator. This field is read-only and appears only if the Create Local Admin checkbox is selected.
Default Admin Password	The password to assign to the default local administrator. This field displays and is mandatory only when Create Local Admin is selected.
Repeat Default Admin Password	Confirm the default local administrator password. This field appears and is mandatory only when Create Local Admin checkbox is selected.

- On the **Contact Information** tab, enter address, email, and phone information as appropriate.
- Click **Save**.

4.6. Create Intermediate Node

An intermediate node is an optional node in the VOSS Automate hierarchy. It is located between the standard hierarchy nodes (Provider, Reseller, Customer, and Site).

An intermediate node 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, no default administrator is created for it. Adding an administrator for an intermediate node is a separate step.

To create an intermediate node:

- Log in as an administrator at the hierarchy level where you want to create the intermediate node.
For example, to create an intermediate node to group sites, log in as the customer administrator.

2. From the **Hierarchy** form click **Add**.
3. Enter the following information for the node:

Field	Description
Name	The name of the node. This field is mandatory. Note: Once you enter a name, it cannot be changed.
Description	A detailed description of the node (optional).

4. Click **Save**.

The intermediate node is created in the hierarchy.

Next Steps

- Define a local administrator for the intermediate node.
- Then create nodes underneath the intermediate node that the intermediate node local administrator can manage.

4.7. Delete a Hierarchy

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

A utility is available under a hierarchy management menu to delete a hierarchy (Provider, Reseller, Customer, Site, IntermediateNode) and all data under it.

If the utility is used at a higher level hierarchy, then select the lower level hierarchy to delete from the drop-down list.

Check box options are available to:

- remove data on selected UC Apps configured on the hierarchy
- remove the hierarchy data from the VOSS Automate system database completely

Note:

- If a site is deleted, an additional cleanup workflow step also removes site related data above the site level.

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

DN	E164	E164 Association	DN Inventory	E164 Inventory	E164 Association Flag	E164 Associations
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

- If no check boxes are selected, the transaction is successful and no data is deleted.

Since there is a risk in using this utility, a confirmation of the action is required by selecting the **Confirmation** drop down box. Click **Save** to carry out the transaction.

4.8. Delete Issues and Purges

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 Cisco Unified Communications Manager model dependencies don't reflect the additional data contained in existing, provisioned dial plans brought into VOSS Automate.

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.

To execute a purge:

1. Log in as a Reseller administrator or higher.
2. Go to (default menus) **Administration Tools > Data Sync** to open 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 Unified CM.
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 VOSS Automate by executing HcsPull from the same menu for Unified CM and Unity Connection, and then running the Overbuild.

4.9. Localization Language

4.9.1. Overview

A default language can be set 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.

4.9.2. 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 (default menus) **User Management > Users** (on the **User Details** tab).

4.9.3. Configure Localization Language

1. Log in as Provider, Reseller, Customer, or Site administrator.
2. Set the hierarchy path to point to the node where you want to set a default language.
3. Go to (default menus) **Hierarchy Management > Localization Language**.
4. Click **Add**.
5. From the **Language** drop-down, choose the default language.
6. Click **Save**.

5. Customer Management

5.1. Manage Customers

This procedure adds a new customer, and updates an existing customer.

Note:

- References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.
- In VOSS Automate, if the customer name matches an existing customer previously configured in HCM-F, you can migrate the existing customer.
- If required, you can disable number management for the 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 (default menus) **User Management > Admins**. 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 (default menus) **Customer Management > Customers**.
4. On the **Customers** page:
 - To add a new customer, click **Add**.
 - To update an existing customer, click on the customer name.
5. Fill out or update the fields on the page:

Field	Description
Customer Name	Mandatory. The name of the customer. Note that when Create Local Admin is selected, any spaces in the customer name are converted to underscores in the Customer local administrator name and email. (Provider deployment) A customer configured in HCM-F and synced in to VOSS Automate may exist at the sys.hsc hierarchy. If customer name matches this customer, the Migrate from HCM-F to VOSS Automate checkbox is displayed. Click Save to migrate this customer to the current hierarchy. Fields are populated with the values configured in HCM-F. If you don't want to migrate the customer, enter a different customer name.
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. Extended name value is synced to the customer record in the Shared Data Repository (SDR). Extended Name is not referenced by other components 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: <ul style="list-style-type: none"> 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.
Public Sector	Set the Customer as a Public Sector customer. Used for License Reporting.
Inactive Billing	Exclude customer from billing (for testing). Used for License Reporting.

Field	Description
Create Local Admin	Defines whether a default local administrator is created for the customer.
Cloned Admin Role	The Provider or Reseller role used to create a new role prefixed with the customer name. The created customer role, shown in the Default Admin Role field, is assigned to the default local administrator user. This field appears only if the Create Local Admin checkbox is selected.
Default Admin Role	The created customer role that is assigned to the default local administrator. This field is read-only, and appears only if the Create Local Admin checkbox is selected.
Default Admin Password	The password to assign to the default local administrator. This field appears and is mandatory only if the Create Local Admin checkbox is selected.
Repeat Default Admin Password	Confirm the default local administrator password. This field appears and is mandatory only if the Create Local Admin checkbox is selected.

Field	Description
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 which can be activated on the Hosted Collaboration Management Fulfillment (HCM-F) server. 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.
Prime Collaboration	Prime Collaboration is the application which monitors equipment used by this customer. Available Prime Collaboration applications must first be configured using the HCM-F User Interface. Then HCM-F synchronization must be executed on VOSS Automate. After the HCM-F data syncs into VOSS Automate, available Prime Collaboration applications will appear in this drop-down. Select an available Prime Collaboration application to monitor Unified Communications applications and customer equipment configured for this customer. To un-associate Prime Collaboration for this customer, choose <i>None</i> .
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. <ul style="list-style-type: none"> • If selected, you cannot add Directory Numbers and E164 Numbers to inventories for this customer. • If <i>not</i> selected, you can add Directory Numbers and E164 Numbers to inventories for this customer.

6. If you enable Number Management for a customer after it was disabled, run the DN Audit Tool. See [Audit Number Inventory](#).
7. Click **Save**.

Note: When deleting a customer, remove any entities associated with the customer, such as LDAP, SSO providers, Devices, and NDLs.

5.2. Network Device Lists (NDLs)

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: HCM-F, CUCM, CUC, Cisco WebEx. In this case, only Cisco HCM-F is required.

Note:

- References to HCM-F and Shared Data Repository (SDR) are only relevant if installed. The HCM-F device is pre-populated in the NDL and should not be changed.
- UC application clusters are linked to a customer only once the NDL is created.

5.2.1. 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.

5.2.2. Choosing a Network Device List (NDL)

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.

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.

5.2.3. Add a Network Device List (NDL)

This procedure adds a new network device list (NDL).

1. Log in as a provider or reseller administrator.
2. Go to (default menus) **Customer Management > Network Device Lists**.
3. Choose a customer on the hierarchy tree where the NDL is to be created.
4. Click **Add**.
5. Enter 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 (+) 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**.

5.2.4. Edit or Delete a Network Device List (NDL)

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.

Related Topics

- VOSS Automate Configuration and Sync in the Core Feature Guide

5.3. CUCM Group Selection

Provider level administrators can manage the Default CUCM 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.

High level administrators carry out these tasks from the **Customer Management > Advanced > CUCM Group Selection** and **CUCM Group Counts** menus.

5.3.1. Select a CUCM Group

1. Log in as a Provider administrator and select **Customer Management > Advanced > CUCM Group Selection**.

2. The list of existing CUCM Group Selection configurations at the Provider hierarchy are listed.

Click **Add** 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 below 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.

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 that an administrator can override this calculated CUCM Group by manually updating the Site Defaults Doc.

5.4. CUCM Group Counts

1. Log in as a Provider administrator and choose **Customer Management > Advanced > CUCM Group Counts**.
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]`.

The 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.

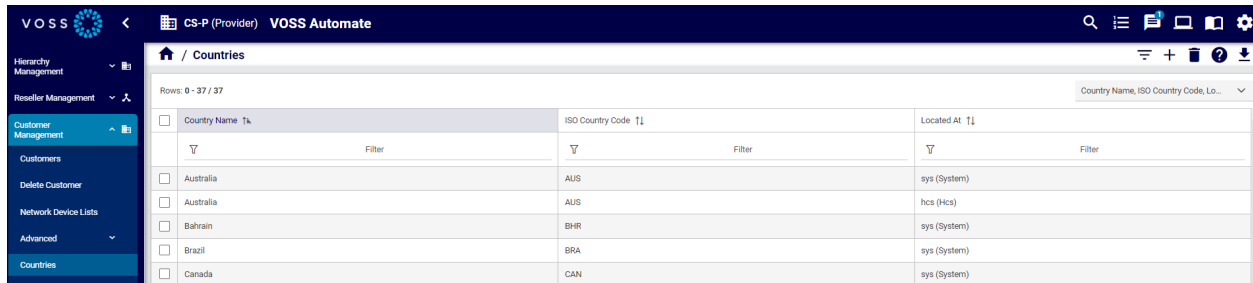
Note: Group Counts values are Phone counts per Device Pool per CUCM Group.

5.5. Countries

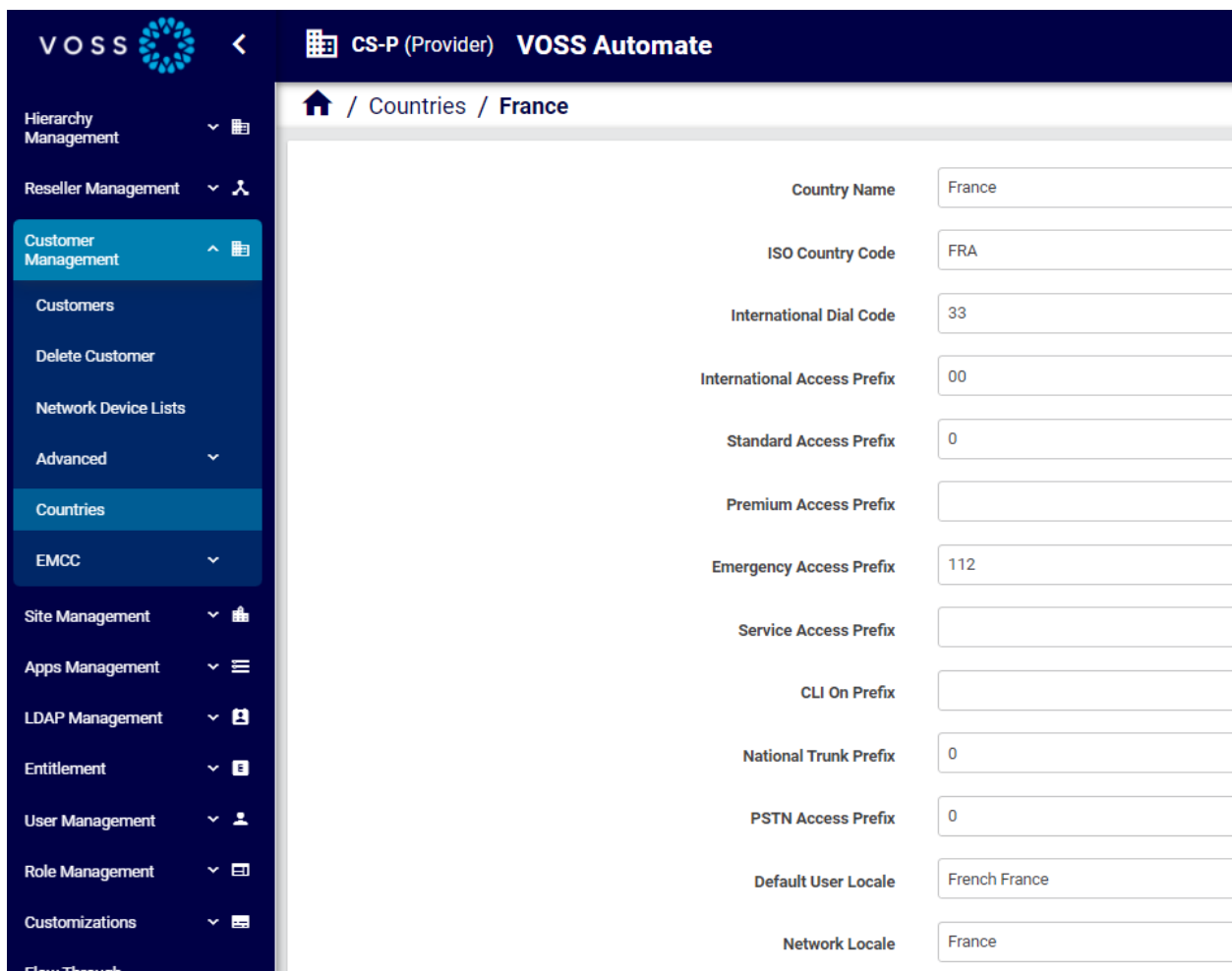
The **Countries** page in VOSS Automate allows you to view, add, or delete country data for your system. This page displays details such as country codes, international dial codes, access prefixes, and network and user locale information.

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).

To access this page, go to **Customer Management > Countries**.



Country Name	ISO Country Code	Located At
Australia	AUS	sys (System)
Australia	AUS	hcs (Hcs)
Bahrain	BHR	sys (System)
Brazil	BRA	sys (System)
Canada	CAN	sys (System)



Country Name	France
ISO Country Code	FRA
International Dial Code	33
International Access Prefix	00
Standard Access Prefix	0
Premium Access Prefix	
Emergency Access Prefix	112
Service Access Prefix	
CLI On Prefix	
National Trunk Prefix	0
PSTN Access Prefix	0
Default User Locale	French France
Network Locale	France

5.6. Extension Mobility Cross Cluster (EMCC)

5.6.1. 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 he/she is 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.

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.

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.
-

HOME Cluster	VISITING Cluster
User Profile	Phone (with Geolocation)
Geolocation Filter	
Roaming Device Pool (with Geolocation)	

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

5.6.2. EMCC Groups

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 geolocations and geolocation 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 screen 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 an 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. Choose **Customer Management > EMCC > EMCC Group**.
3. Click **Add**.
4. Choose the required customer from the **Hierarchy** drop-down list.
5. On the **EMCC Group** screen, enter the mandatory EMCC Group Name in the **Name** field.

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. 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** to add the EMCC group to VOSS Automate.

Once the EMCC Group is created, the following elements are provisioned per country and EMCC route pattern:

- Route list
- Geolocation filter
- SIP profile
- IP phone services
- SIP trunk
- Geolocation
- Route partition
- CSS
- Device pool
- Route pattern

Modify an EMCC Group

1. Log in as Provider administrator or higher.
2. Choose **Customer Management > EMCC > EMCC Group**.
3. Click on the EMCC Group that you want to modify.
4. On the **EMCC Group** screen, 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. Use the Move Up and Move Down buttons as required to assist in creating the EMCC Group.
5. Click **Save** to save the modified EMCC group to the VOSS Automate database.

Delete an EMCC Group

To delete an EMCC Group, click on the Group to delete on the EMCC Group screen and then click **Delete** on the button bar.

5.6.3. EMCC Route Patterns

Add EMCC Route Pattern

1. Log in as provider administrator or higher.
2. Make sure that the hierarchy path is set to the correct customer node.
3. Choose **Customer Management > EMCC > EMCC Route Patterns**.
4. Click **Add** to add an EMCC Route Pattern. The **EMCC Route Patterns** screen is displayed.
5. Enter 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 add the EMCC Route Pattern.

Modify EMCC Route Pattern

1. Log in as provider administrator or higher.
2. Make sure that the hierarchy path is set to the correct customer node.
3. Choose **Customer Management > EMCC > EMCC Route Patterns**.
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.

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** on the button bar.

5.6.4. EMCC Templates

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 path to the correct customer or location node.
3. Choose **Customer Management > EMCC 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) Enter a new **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 path to the correct customer or location node.
3. Choose **Customer Management > EMCC 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.

Delete an EMCC Template

To delete an EMCC Template, click on the template to delete on the EMCC Templates list view, and then click **Delete** on the button bar.

6. Site Management

6.1. Create a Site

Note: The following additional fields are available and shown as summary fields:

- City
- Postal Code
- State
- Extended Name
- External ID
- SiteId
- InternalSiteID(Disabled)

-
1. Log in as provider, reseller, or customer administrator.
 2. Make sure that the hierarchy is set to the customer for whom you are creating the site.
 3. On the **Sites** form (default menu **Site Management > Sites**) click **Add**.
 4. Complete the following fields:

Option	Description
Site Name	The name of the site. This field is mandatory. 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. 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	A description for the site
Create Local Admin	Controls whether a default local administrator is created for the site.
Cloned Admin Role	The customer role used to create a new role prefixed with the site name. The created site role, shown in the Default Admin Role field, is assigned to the default local administrator user. This field appears only if the Create Local Admin check box is selected.
Default Admin Role	The created site role that is assigned to the default local administrator. This field is read-only and appears only if the Create Local Admin check box is selected.
Default Admin Password	The password to assign to the default local administrator. This field appears only if the Create Local Admin check box is selected.
Repeat Default Admin Password	Confirm the default local administrator password. This field appears only if the Create Local Admin check box is selected.
Country	Select the Country from a drop-down of countries. This field is mandatory.
Network Device List	Choose the NDL containing the UC applications and WebEx to be used by the site. Once an NDL has been set for the site, it cannot be removed from the site, nor can the NDL be changed to another NDL.
Auto Push Users to CUCM	If enabled, users are automatically pushed to the Cisco Unified Communications Manager that is associated with the NDL. The default is disabled. Note: You can edit the site later, and select this check box for one of the following reasons: <ul style="list-style-type: none"> • To automatically push users at the site to the Cisco Unified Communications Manager. User surname must be filled in. • To perform an Auto User Push when an NDL is added to the site. • To perform an Auto User Push when a Cisco Unified Communications Manager is associated with an NDL. Only users with user type "End User" are pushed to the Cisco Unified Communications Manager.

5. Click **Save**.

Once saved, the following occurs:

- A Site hierarchy node is created.
- A Location is created.
- Optionally, a default site administrator is created.
- If the **Auto Push Users to CUCM** check box is selected:
 - All users associated with the NDL are pushed to the Cisco Unified Communications Manager associated with the NDL. User surname must be filled in.
 - Only users with user type "End User" are pushed to the Cisco Unified Communications Manager.

6.2. Site Defaults Doc Templates

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

The data in this template is in turn used to generate a customer-level default SDD template called `CUSTOMER_TEMPLATE` for each customer added to the system under the respective provider hierarchy.

When creating a site, a SDD instance is created on the site using the `CUSTOMER_TEMPLATE`. The site level SDD is useful for managing multi-site, multi-country customers and allows a provider administrator (or higher) to define geo-specific information at a site level, allowing multinational sites to stay in sync.

The site level SDD has the same name as the new site, and is also pre-populated with several default values. Site level SDDs 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 defaults.

Administrators with the required permissions can modify the `PROVIDER_TEMPLATE` and `CUSTOMER_TEMPLATE` SDD templates as required in order to customize SDD settings in the template during the creation of lower level SDDs and SDD templates. The default SDD templates are shown in the list view of the **Site Defaults** menu.

Related Topics

- [Site Defaults](#)

6.3. Site Defaults

6.3.1. 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, a VOSS 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 subscribers at the sites (when flow through provisioning is enabled).

6.3.2. Edit Site Defaults

This procedure displays and updates site defaults.

Perform these steps:

1. Log in to VOSS Automate (Admin Portal or Business Admin Portal), as Provider, Reseller, or Customer administrator.
2. Choose an option:
 - From the Business Admin Portal, go to (default menus) **Site Management > Site Defaults**; then, select the relevant site to open the **Site Defaults[site name]** page.
 - From the Admin Portal, go to (default menus) **Site Management > Defaults** to open the **Defaults** page; then, select the relevant site to open the **Defaults[site name]** page.
3. Click through the tabs to modify site default values:
 - General Defaults
 - Device Defaults
 - Line Defaults
 - User Defaults
 - CUC Defaults
 - HotDial Defaults
 - Overbuild Defaults
 - Move Filter Criteria
 - MS Teams
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

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.

6.3.3. Defaults Page

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

You can select the following tabs on this page:

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

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 <i>Least Utilized</i> or <i>Default</i> . 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.

Device Defaults Tab

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

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 subscriber), 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

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	<p>When this check box is selected, the E164 Mask will use the National format of the associated E164 Number.</p> <p>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.</p> <p>Note: For Quick Add Subscriber, set the following value in the E164 Mask field of the relevant phone, device profile and remote destination profile configuration template <code>{{ macro.SDD_QAS_E164Number_MCR }}</code>. See the "Reference CUCM Phone Template" CFT for an example configuration.</p>

Line Defaults Tab

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

Option	Default Value
Default CUCM Line BLF Presence Group	Standard Presence Group
Default CUCM Line Voice-mail 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

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).
Webex App - Use Organization's Domain	<p>Displays only when:</p> <ul style="list-style-type: none"> • The entitlement profile allows the Webex App service • A Webex App server is configured • The subscriber and Webex App user have the same email address • Subscriber does not already have Jabber clients • CUCM calling behavior is not yet configured for the Webex App user <p>Enabling this option hides the following field: Webex App - UC Manager Profile</p> <p>Default (when displayed) is unchecked (clear).</p> <p>When enabled, Webex App provisioning via QAS refers to values generated via the following named macros in the device/spark/User configuration template (CFT):</p> <ul style="list-style-type: none"> • SDD_WtCallBehaviourUcManagerProfile • SDD_WtUseOrgDomain <p>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).</p>
Webex App - UC Manager Profile	<p>Displays only when the following checkbox is clear (not selected): Webex App - Use Organization's Domain</p> <p>Choose the UC Manager profile from the drop-down.</p> <p>Options in the drop-down are the UC manager profiles added via Services > Webex App > Customer Access</p>

CUC Defaults Tab

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

Cisco Unity Connection Localization in the Core Feature Guide.

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: <ul style="list-style-type: none"> • 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

Overbuild Defaults Tab

The Overbuild Defaults tab is visible only to Provider and Reseller administrators.

Settings on this tab:

- Include Site for Overbuild (yes/no)
- Create Internal Number Inventory at CustomerId (yes/no)
- Overbuild Device Control (e.g., Move All Devices, Limit Moved Devices)
- Add additional device pools

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

Overbuild Site Defaults: Overview 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 model filter criteria you can choose (depending on the user type you're syncing in, for example, Microsoft, LDAP, or CUCM), is configured in the Admin Portal, via (default menus):

- Customizations > Model Filter Criteria, or in:
- Flow Through Provisioning Configuration > Model Filter Criteria

Related Topics

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

MS Teams Tab

The table describes settings on this tab:

Option	Description
Manage Licenses and Allow User Staging	<p>This checkbox defines whether Voss Automate may update the MSOL (Microsoft 365) user, typically, the licensing component. When disabled (unchecked), VOSS Automate will never attempt to update a user's license, and in this case, it won't be possible to use Quick Subscriber to license a user and to provide them with baseline MS Teams configuration. The user must be properly licensed through the Microsoft online portal to allow VOSS Automate to provide accurate MS Teams configuration.</p> <p>Additionally, disabling this setting hides the Line URI field in Quick Subscriber when:</p> <ul style="list-style-type: none"> • The user is not licensed for Microsoft Teams • The user's license includes feature group <i>PhoneSystem</i> <p>Enable this setting to allow users to be staged, licensed, and provisioned from Quick Subscriber.</p>
Auto Delete VOSS4UC User	<p>Defines whether to delete the user in VOSS Automate when the MS Azure AD online user is deleted. This only applies to users located at the Site level. Users at Customer level will not be automatically deleted.</p>
Default Tenant Dial Plan	<p>Defines the default tenant dial plan for the site. For details, see <i>Configure Microsoft Tenant Dialplan</i> in the Core Feature Guide.</p>
MS Teams Policies	<p>Policies are synced in to VOSS Automate from MS Teams and are available in the SDD as defaults. You can choose a default policy for a site in the site defaults to automatically assign to subscribers at the site. When creating a subscriber via Quick Subscriber, the site default is used, but you can also edit the configuration template for the Quick Add Group (QAG) to use a policy different to the site defaults, or you can edit a subscriber directly to choose a different policy for that subscriber. See <i>Introduction to Microsoft Teams Policies</i> in the Core Feature Guide</p>
Default Usage Location	<p>The country for default usage.</p>

Related Topics

- [Configure Microsoft Tenant Dialplan in the Core Feature Guide.](#)
- [Introduction to Microsoft Teams Policies in the Core Feature Guide.](#)
- [Quick Subscriber for Microsoft Users in the Core Feature Guide.](#)
- [Microsoft Licenses in the Core Feature Guide](#)

7. Apps Management

7.1. VOSS Insights

7.1.1. Introduction to VOSS Insights Monitoring

Overview

Users with both VOSS Automate and VOSS Insights deployed can enable monitoring of UC applications via the VOSS Automate Admin Portal, from an Insights Arbitrator server integrated with VOSS Automate.

Note: For details around integrating VOSS Automate with the Insights Arbitrator server, see [Arbitrators](#)

Once the integration is set up, you onboard customer server clusters, comprising one or more Cisco Unified Communication Manager (CUCM) CallManager servers and/or Cisco Unity Connection (CUC) servers, to an Arbitrator server for monitoring, from within the VOSS Automate Admin Portal.

The following servers are supported:

- Cisco Unity Connection (CUC) servers
- Cisco Unified Communications Manager (CallManager, or CUCM) servers

Provisioning is supported for these CUCM server types:

- Voice (VOICE_VIDEO)
- IM and Presence Service (IM_P)

Note: The image displays a customer with four CallManager servers that are part of the same cluster. The cluster is onboarded to the Arbitrator server for monitoring purposes.

<input checked="" type="checkbox"/>	Cluster Name	CUCM Server Name	Located At
<input type="checkbox"/>	ELITE-CUCM-CL1	ELITE-CUCM-PUB	ELITETECHS (Customer)
<input checked="" type="checkbox"/>	ELITE-CUCM-CL1	ELITE-IMP-PUB	ELITETECHS (Customer)
<input type="checkbox"/>	ELITE-CUCM-CL1	ELITE-CUCM-SUB	ELITETECHS (Customer)
<input type="checkbox"/>	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 (default menus) **Apps Management > VOSS Insights > Arbitrators**. See [Arbitrators](#)

Note: The Arbitrator server should be at version SP23 or higher.

- View currently configured monitoring set up for server clusters, if any:
 - For CUCM servers, go to (default menus) **Apps Management > CUCM > Servers**, 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.

The screenshot displays the configuration page for a CUCM server cluster in the 'Publisher' tab. The main configuration fields are as follows:

- CUCM Server Name*:** ELITE-IMP-PUB
- Publisher:**
- Cluster Name:** ELITE-CUCM-CL1
- Server Type*:** IM_P
- Sync on Create/Update:**

The **Network Addresses** section contains one entry:

Address Space*	IPV4 Address	Hostname	Domain	Description
SERVICE_PROVIDER_SPACE	172.30.42.17	ELITE-IMP-PUB		

The **Credentials** section contains one entry:

Credential Type*	User ID*	Password*	Repeat Password*	Description
ADMIN	admin	

- For CUC servers, go to (default menus) **Apps Management > CUC > Servers**, then click on a cluster to view monitoring details, including the monitoring Arbitrator server, if any.
- When adding new CUCM or CUC server in a cluster, you can choose an Arbitrator to monitor the servers (via the Monitoring fields for Publisher servers)

Note: At the time of writing (VOSS Automate v21.3), modifying any existing monitoring setup on UC apps is not supported. However, deleting a UC app on VOSS Automate will remove the asset and related configuration from all corresponding VOSS Insights Arbitrator servers.

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 CUCM 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:

Server in the cluster	Onboarding Provisioning
CUCM VOICE Publisher (PUB)	<p>Provisioning on Arbitrator:</p> <ol style="list-style-type: none"> 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): <ul style="list-style-type: none"> • 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 <p>The static probes must exist on the Arbitrator for Arbitrator monitoring to work. The static probes are associated with new assets, using the profiles.</p> <p>Provisioning on the CallManager:</p> <ul style="list-style-type: none"> • Creates the application user. When onboarding multiple servers, you can ignore a <i>fail</i> status at this step Create Cucm App User, since duplicate user creation is ignored. • Updates service parameters
CUCM VOICE Subscriber (SUB)	<p>Provisioning on Arbitrator:</p> <ol style="list-style-type: none"> 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)	<p>Provisioning on Arbitrator:</p> <ol style="list-style-type: none"> 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): <ul style="list-style-type: none"> • 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

Server in the cluster	Onboarding Provisioning
CUCM IM_P Subscriber (SUB)	Provisioning on Arbitrator: <ol style="list-style-type: none"> 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 VOSS Insights documentation.

Groups		Assets				
Group Name		IP Address	Asset Name	Description	Type	Monitor Profile
All groups		172.30.42.17	ELITE-IMP-PUB		Unknown	2 profiles set
AAAGlobal 0		172.30.42.18	ELITE-IMP-SUB		Unknown	1 profile set
AcmeCorp 1		172.30.42.69	ELITE-CUCM-SUB		Unknown	1 profile set
AFD 0		172.30.42.70	ELITE-CUCM-PUB		Unknown	5 profiles set
AUDIO CODES 1		172.30.42.71	ELITE-CUC-PUB		Unknown	2 profiles set
BODYSHOX 5						
CSP Shared Architecture 3						

Probe Groups, Profiles, and Asset Onboarding

The table describes the probe groups and profiles that are added to the VOSS 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

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

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](#)

7.1.2. Arbitrators

Overview

Managing VOSS Insights Arbitrators in VOSS Automate requires the following:

- Set up Arbitrators
- Set up host connection details and credentials (the admin user and password from the Arbitrator)

Note: See the VOSS Insights documentation for Arbitrator setup.

Add a Connection to the Arbitrator Server

This procedure provides connection details to the Arbitrator server to integrate VOSS 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 VOSS Automate.

1. In the VOSS Automate Admin Portal, go to (default menus) **Apps Management > VOSS Insights > Arbitrator**.
2. Click the Plus icon (+) to add an Arbitrator.
3. Fill out Arbitrator details:

Server Name	Name of the VOSS Insights Arbitrator server in VOSS Automate. Field tooltip provides naming convention.
Description	Optional. Provide a description.
Host Name	Host name or IP address of this Arbitrator server, which is used to connect to the Arbitrator.
User Name	Username for a valid admin account; an admin user allowed to log in to the Arbitrator server.
Password / Repeat Password	Password credential of a valid admin account; an admin user allowed to log in to the Arbitrator server.
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 VOSS 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.

Next Steps

CUCM and CUC servers can now be onboarded and enabled for monitoring. See [Onboard Assets](#)

Related Topics

- [Onboard Assets](#)
- [Offboard Assets](#)

Remove an Arbitrator Server

This procedure removes an Arbitrator server from the list of Arbitrator servers configured for integration with VOSS Automate.

1. In the VOSS Automate Admin Portal, go to (default menus) **Apps Management > VOSS Insights > Arbitrator**.
2. View the summary list of available Arbitrators set up for integration with VOSS Automate.
3. Select the relevant Arbitrator, then click **Delete**.
 - The Arbitrator server is removed from VOSS Automate app servers (Unified CM, Unity Connection).
 - The integration details for this Arbitrator server is removed from VOSS Automate.
 - On the **Monitoring** group of the UC app server publisher form, the **Insights Arbitrator** checkbox is removed.
 - Created pull/purge data syncs on VOSS Automate are removed.

7.1.3. Onboard Assets

If VOSS 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 VOSS Automate.

Note: At the time of writing (VOSS Automate 21.3), modification of any existing monitoring on UC Apps is not supported. However, once a CUCM or CUC server is created, use the Onboard/Offboard Asset tools to enable/disable monitoring.

1. In the VOSS Admin Portal, go to **Apps Management > VOSS Insights > Onboard Assets**.
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.

Related Topics

- [Probe Groups, Profiles, and Asset Onboarding](#)
- [Add a CUCM Server](#)
- [Cisco Unity Connection \(CUC\) Servers](#)

Additional Onboarding Tools for Single Clusters and Servers

VOSS 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** menus. 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.

7.1.4. Offboard Assets

Overview

CUCM and CUC server clusters that have been integrated with VOSS 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.

Related Topics:

- [Introduction to VOSS Insights Monitoring](#)
- [Arbitrators](#)
- [Onboard Assets](#)

Offboard Assets

This procedure allows a batch removal of the clusters associations by Arbitrator server.

1. In the VOSS Admin Portal, choose the relevant customer hierarchy.
2. Go to (default menus) **Apps Management > VOSS Insights > 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.

-
- VOSS Automate makes the following updates on the associated Arbitrator when a CUCM or CUC server (asset) is unassociated from a VOSS 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 VOSS Automate)
 - Removes profiles in VOSS 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, via the **Apps Management** menu (for CUCM or CUC > Server).

Delete a UC App to Offboard the Asset

When a CUCM or CUCM server or cluster that was integrated with a VOSS Insights Arbitrator server is deleted, the asset, customer-specific probes, profiles, credentials, and related data are removed from the Arbitrator.

The VOSS Insights Arbitrator data syncs for the UC app are also removed.

Additional Offboard Tool for Single Servers

VOSS 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

7.2. SMTP Server

7.2.1. 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**.
4. Click the toolbar Plus sign (+) to add a new SMTP server.
5. On the **SMTP Server** form, configure details for the new SMTP server:
 - Add name for the SMTP server.
 - Add a description for the email account.
 - Enter the SMTP server hostname and port number.
 - Select **Secure** to use the SSL protocol for establishing a connection to the SMTP server.
 - Enter username and password credentials for establishing a connection to the SMTP server.

Related Topics

- Email in the Core Feature Guide
- Global Settings in the Core Feature Guide

7.3. VOSS Phone Server Management

7.3.1. VOSS Phone Server Overview

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 CUCM dialplan designs may be utilised through the VOSS4UC 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 VOSS 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 tftp 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.

VOSS 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 CUCM Virtual Machines in an HCS/CUCM environment. Redundancy is an option, providing data replication between servers.

7.3.2. Managing VOSS Phone Servers

Adding phones requires three areas of configuration. These are all automated by VOSS 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 - VOSS Automate manages the Cisco CUCM 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 VOSS 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 VOSS 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.

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.

See:

- [VOSS Phones](#)
- [Adding Phone Types](#)

7.3.3. Adding 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. VOSS Automate has 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 VOSS4UC without the need for software updates or patches.

8. Cisco Apps Management

8.1. CUCM (Cisco Unified Communications Manager)

8.1.1. CUCM Configuration

Overview

Cisco Unified Communications Manager (CUCM) devices provide the core call processing capabilities for HCS, and are a critical part of the VOSS Automate provisioning workflows. You must configure the CUCM devices before you complete the dial plan (if applicable), user, subscriber, line, and phone configuration.

CUCM devices can be dedicated to a specific customer, or they can be shared between multiple customers. CUCM 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 select which CUCM is 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

To share the CUCM across multiple customers, add the CUCM at the Provider or Reseller level. To dedicate the CUCM to a single customer, add the CUCM at the Customer level.

When setting up CUCM as a dedicated instance, you can opt to set up CUCM after you create the customer.

Servers within a CUCM Cluster

Within a CUCM cluster, you can configure the following nodes:

- Cisco Unified Communications Manager Publisher
- Cisco Unified Communications Manager Subscriber
- IM and Presence Service Publisher
- IM and Presence Service Subscriber

Configure a CUCM Publisher node before configuring any other type node.

Configure an IM and Presence Service Publisher node before configuring an IM and Presence Service Subscriber node.

Sync with VOSS Automate

Configuring a CUCM device on VOSS Automate creates a scheduled data sync to import model data from the device into VOSS Automate. The scheduled data sync ensures that the VOSS 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, will be reflected in VOSS 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 Subscriber Management activities as well.
- Some license-related models will now be excluded from CUCM imports by default:
 - device/cucm/LicensedUser
 - device/cucm/LicensingResourceUsage
 - device/cucm/HcsLicense

The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule from **Apps Management > CUCM > Schedules**. 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 from **Apps Management > Advanced > Perform Publisher Actions**, or from **Administration Tools > Data Sync**.

Important: Allow the initial data sync to complete before doing more configuration on VOSS Automate that requires information from CUCM.

Note: On Provider deployments, references to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

When you set up an IM and Presence Service server, VOSS Automate does not communicate directly with the IM and Presence Service server. The information provided is pushed to HCM-F and Service Assurance (if installed) for monitoring purposes.

The performance of a data sync can be improved by controlling the types of data that are synced. See [Controlling a Data Sync with a Model Type List](#) for more information.

For details on Change Notification Sync in VOSS Automate and on switching between Full Sync and Change Notification Sync, refer to the topic on the Change Notification Feature (CNF) following [Introduction to Change Notification Sync](#).

Field Mappings in CUCM

When setting up a CUCM device with LDAP integration, you can map CUCM user data to VOSS 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 VOSS Automate must exactly match the field name entered in the mapping in the CUCM in the Custom User Field Name field. If the field names do not match, the field is skipped during the sync.

8.1.2. Add a CUCM Server

This procedure adds and configures a CUCM server (Cisco Unified Communications Manager) within a CUCM cluster.

Note: References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

1. Log in to the VOSS Admin portal with the appropriate hierarchy administrator credentials.

Note:

- Log in as a Provider or Reseller administrator if you're creating a shared instance.
 - Log in as a Customer, Provider, or Reseller administrator to create a dedicated instance.
-

2. Set the hierarchy path to the correct level:
 - Create a shared instance at the Provider or Reseller level.
 - Create a dedicated instance at the Customer level.
3. Go to (default menus) **Apps Management > CUCM > Servers**.
4. Click **Add**.
5. Configure server details on the **Base** tab:
 - a. At **CUCM Server Name**, fill out the CUCM server name.

Note: A CUCM server that has been configured in HCM-F and synced into VOSS Automate may exist at the *sys.hcs* hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS Automate** checkbox displays.

To migrate this server to the current hierarchy level, click **Save**. The fields are populated with the values configured in HCM-F. If you don't want to migrate the server, enter a different server name.

- b. If you're configuring a publisher node, select the **Publisher** checkbox. This displays an additional tab (Publisher tab).

- c. For a CUCM 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 CUCM Subscribers, choose the CUCM cluster from the **Cluster Name** drop-down menu.
- d. At **Server Type**, choose an option, either **VOICE_VIDEO** or **IM_P**.
- e. To trigger a sync (auto-import) of the UC app server when saving the form, select **Sync on Create/Update**.
- f. Expand **Network Addresses**, and add network addresses, one or more:
 - At **Address Space**, choose **SERVICE_PROVIDER_SPACE**.

Note: If NAT is used, you will also need to add a **APPLICATION_SPACE** network address (repeat these steps and for address space, choose **APPLICATION_SPACE**).

- The **Hostname** field is automatically populated with the CUCM server Name. Edit it if necessary.
- Fill out the IP address of the CUCM server in the **IPv4 Address** field.

Note: Either the hostname or the IP address is required. Ensure the hostname or IP address does not contain a trailing blank space since VOSS 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 CUCM application.
- Provide an optional description for the network address.
- g. Expand **Credentials**, then add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
 - Fill out the user ID and password that you configured when installing the CUCM.
 - For **Access Type**, choose RO (Read-only) or RW (Read or Write). The default is RO.
 - Provide an optional description for the credential.

Note:

- Access type is relevant only for SNMP since SNMP credentials are pushed to the UC application.
- ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage CUCM.
- PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.
- Expiration of the ADMIN account results in failed data syncs between CUCM and VOSS Automate.
- The CUCM Admin Account requires the following roles (can be added in a group):
 - * For normal AXL Add, Update, Delete transactions you need: *Standard AXL API Access*
 - * For the Extension Mobility Login/Logout you need: *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) you need: *Standard CCM Admin Users*

6. Fill out fields on the **Publisher** tab:

Note: This tab displays only if you've selected the **Publisher** checkbox on the **Base** tab.

Field	Description
Prime Collab	Choose the Prime Collaboration management application monitoring this cluster. To un-associate Prime Collaboration for this cluster, choose None .
Call Processing ID	The Call Processing ID of this cluster
SDR Cluster ID	The SDR CUCM cluster ID, as shown on SDR Configuration > SDR CUCM Clusters .
Version	Choose the version of the Unified CM Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Multi-Tenant	Read-only field. 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 Unified CM 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 Unified CM are entitled to. Note: A violation of the Entitlement Profile does not prevent a user from being synced to VOSS Automate from Unified CM. However, subsequent updates to the user fail until the user's configuration satisfies the restrictions set in the Entitlement Profile.
Enable Change Notification Sync	Select this check box to enable Change Notification. By enabling this, 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. See the note below this table.
Monitoring	For new servers and if Arbitrator servers are available, monitoring can be enabled for this CUCM on VOSS 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 VOSS 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 CUCM network device is created in VOSS Automate. (If installed, a cluster and CUCM

are created in the SDR.)

9. Test the connection between CUCM and VOSS Automate.

Related Topics

- For details on monitoring and VOSS Insights, refer to *Introduction to VOSS Insights Monitoring*.
- For more information on Change Notification Feature (CNF) see *Introduction to Change Notification Sync*.

Test a CUCM and VOSS Automate Connection

Once you've added a CUCM server, you should test the connection between the CUCM server and VOSS Automate.

1. In the VOSS Automate Admin Portal, to to (default menus) **Apps Management > Advanced > CUCM Network Device**.
2. Click the CUCM you just added.
3. Choose **Action > Test Connection**.
4. If the test fails, and you used a hostname, ensure that VOSS 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 CUCM from this page. To change any configuration of the CUCM, edit it via **Apps Management > CUCM > Servers** in VOSS Automate.
 - After updating DNS servers, you'll need to restart the selenium service on the platform CLI:

```
app start selenium
```
-

8.1.3. Delete a CUCM Server

Deleting a Cisco Unified Communications Manager (CUCM) Server in VOSS Automate also deletes local data that has been synced to it from the Cisco Unified Communications Manager Server, including:

- Users
- Configuration parameters
- Dial Plan Information (if applicable)

8.1.4. Set Up IM and Presence Service Servers

This procedure configures IM and Presence Service servers within a Cisco Unified Communications Manager cluster.

Note: References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

Perform these steps:

1. Log in as the appropriate hierarchy administrator.

Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.
2. Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.
3. Choose **Apps Management > CUCM > Servers**.
4. Click **Add**.
5. Enter the IM and Presence Service server name in the **CUCM Server Name** field.

Note: An IM and Presence Service server that has been configured in HCM-F and synced into VOSS Automate may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS Automate** check box is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.
6. From the **Server Type** drop-down, choose **IM_P**.
7. 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.
8. Select the Cisco Unified Communications Manager cluster from the **Cluster Name** drop-down.
9. Expand **Network Addresses**.
 - a. 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. Enter the IP address of the IM and Presence Service 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 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.
10. Expand **Credentials**.
 - a. Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.

- 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.

ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage IM & Presence Service. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

11. Click **Save**.

8.1.5. Headset Enablement

To enable the Cisco Headset Service for a Unified CM server listed under **Apps Management > CUCM > Servers**. Choose **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.

See: [Headsets](#).

8.1.6. Clone an Instance of a CUCM Device Model

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 Unified CM or to a different Cisco Unified CM.

If you clone to a different Cisco Unified CM, make sure that all device model fields have values that are appropriate for the target Cisco Unified CM. For example, make sure calling search spaces specified in the source instance exist on the target Cisco Unified CM.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Do one of the following:
 - If you logged in as provider or reseller administrator, choose **Apps Management > CUCM > {device_model_type}**.
 - If you logged in as customer administrator, choose **Apps Management > Advanced > {device_model_type}**.
3. From the device model list, click 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 Cisco Unified CM from the **CUCM** drop-down menu.
6. Enter a unique name for the new instance of the device model in the **Name** field.
 7. Modify other fields as required.

For more detailed information about the 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 Cisco Unified CM.

8.1.7. Multi-Cluster or Single Cluster Configurations

Overview

Previously, IM and Presence Service (previously known as CUP) was set up in a cluster separate from the Cisco Unified Communications Manager (CUCM) cluster, in a configuration known as *multi-cluster*.

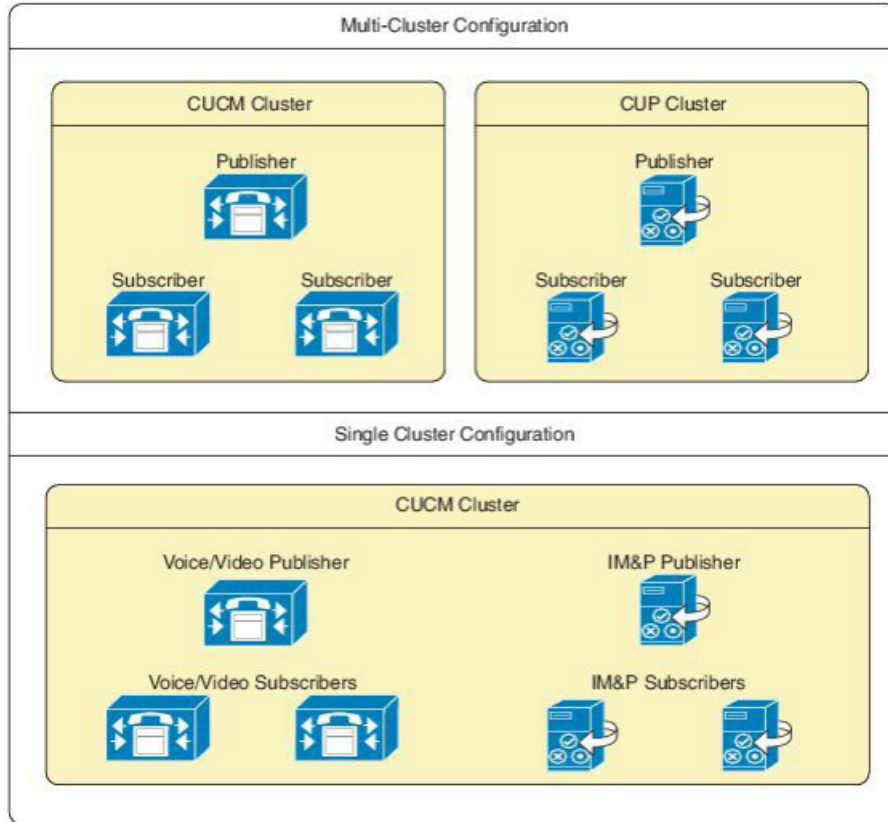
However, the IM and Presence Service servers are set up as part of the CUCM cluster itself, in what is called a *single-cluster* configuration.

Benefits of a Single-Cluster Configuration

VOSS Automate recommends a single-cluster configuration, which service providers are encouraged to use for any new clusters.

Single-cluster configurations have these benefits:

- Correctly represents the CUCM cluster with its IM and Presence Service servers in the management layer
- Eliminates the confusion that *multi-cluster* configurations can cause for administrators when Cisco Prime Collaboration Assurance (PCA) and other tools show these servers in different clusters.



Deprecation of Multi-Cluster Configurations

Multi-cluster configurations are deprecated and strongly discouraged. However, VOSS Automate continues to support multi-cluster configurations for backward compatibility and upgrades.

Converting Multi-Cluster Configurations to Single Cluster

This procedure migrates your CUP (also known as IM and Presence Service) nodes to a CUCM cluster (single-cluster configuration - the recommended option).

Migrating CUP nodes to a CUCM cluster is hierarchy-specific:

- A Customer CUP node can only be migrated to a Customer CUCM 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 CUCM 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 CUCM cluster
- Multiple subscribers can be migrated to the same CUCM 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.
 - For a shared configuration, set the hierarchy to Provider or Reseller node.
 - For a dedicated configuration, set the hierarchy to a Customer node.
3. Go to (default menus) **Apps Management > CUP (deprecated) > Migrate CUP to CUCM Cluster**.
4. From the **From CUP Cluster** drop-down, choose the CUP cluster you wish to migrate.
5. From the **To CUCM Cluster** drop-down, choose the CUCM cluster to which you want to migrate the CUP cluster.
6. Click **Save**.

The migrated CUP server is removed from the list under **Apps Management > CUP > Servers** and now appears under **Apps Management > CUCM > Servers** as server type **IM_P**.

The cluster name for the migrated servers is now the same as the CUCM cluster name.

8.1.8. Configure Date Time Groups

Use Date Time Groups to define time zones for the various devices that are connected to Cisco Unified CM. Each device exists as a member of only one device pool, and each device pool has only one assigned Date Time Group.

Cisco Unified CM automatically configures a default Date Time Group that is called CMLocal. CMLocal synchronizes to the active date and time of the operating system on the server where Cisco Unified Communications Manager is installed. You can change the settings for CMLocal as desired. 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.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set 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. Perform one of the following:
 - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Date Time Groups**.
 - If you logged in as a customer administrator, choose **Device Management > Advanced > Date Time Groups**.
5. Click **Add**.
6. Provide the following information:

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.

7. Click **Save**.

8.1.9. Time Periods

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: VOSS 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.

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. Choose an appropriate option, based on your login:
 - Provider or Reseller administrator? Go to (default menus) **Apps Management > CUCM > Time Periods**.
 - Customer administrator? Go to (default menus) **Apps Management > Advanced > Time Periods**.
4. Choose an appropriate option:
 - To add a new time period, click **Add**, then go to Step 5.
 - To edit an existing time period, choose 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 nonsite 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 only appears when a time period is added; it does not appear when you edit 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. The 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:

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

- From the **Start Day** drop-down menu, choose a day of the week on which this time period starts.
- 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

- From the **Start Month** drop-down menu, choose a month of the year on which this time period starts.
- 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.
- From the **End Month** drop-down menu, choose a month of the year on which this time period ends.
- 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.
-

8.1.10. Time Schedules

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: VOSS 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. Choose an appropriate option, based on your login:
 - Provider or Reseller administrator? Go to (default menus) **Apps Management > CUCM > Time Schedules**.

- Customer administrator? Go to (default menus) **Apps Management > Advanced > Time Schedules**.

4. Choose an appropriate action:

- To add a new time schedule, click **Add**, then go to Step 5.
- To edit an existing time schedule, choose 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 window appears, select the NDL for the time schedule from the drop-down menu. The window appears when you are on a nonsite 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 only appears when a time schedule is added; it does not appear when you edit a time schedule.

6. Enter a unique name for the new time schedule in the **Name** field, or modify the existing Name if desired. This field is mandatory. 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 box, choose a time period for the time schedule.

10. Repeat Steps 8 and 9 to add another time period to the time schedule.

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 cannot 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 you delete a time schedule, check carefully to ensure that you are deleting the correct time schedule. You cannot retrieve deleted time schedules. If you accidentally delete a time schedule, you must rebuild it.

8.1.11. Configure Locations

This procedure adds locations.

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 Cisco Unified CM to manage call admission control. Sites are used by VOSS Automate to logically group resources.

Perform these steps:

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 location.
4. Navigate to Locations:
 - If you're logged in as a provider or reseller administrator, choose **Device Management > CUCM > Locations**.
 - If you're logged in as customer administrator, choose **Device Management > Advanced > Locations**.
5. Click **Add**.
6. On the **Location Information** tab, enter the **Name** of the Location. This field is mandatory.
7. Click the **Intra-Location** tab, and complete at minimum, the mandatory *Intra-Location Fields*.
8. Click the **Between Locations** tab, and complete at minimum, the mandatory *Between Locations Fields*.
9. Click the **RSVP Settings** tab, and complete at minimum, the mandatory *RSVP Settings Fields*.
10. Click **Save**.

Intra-Location Fields

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 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.

Between Locations Fields

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.

RSVP Settings Fields

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	<p>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.</p> <p>Choose from the following available settings:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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.

8.1.12. Configure Regions

This procedure adds, edits, and deletes a region.

Note:

- Regions can only be added at a Customer or Site hierarchy level.
- Regions added directly on Cisco Unified Communications Manager (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.

Perform these steps:

1. Log in as Provider, Reseller or Customer administrator.
2. Go to (default menus) **Apps Management > CUCM > Regions**.
3. Choose the hierarchy (Customer or Site).
4. Choose an option:
 - To delete a region, click on the name of the relevant region, then click **Delete**. Click **Yes** to confirm.
 - To edit an existing region, click on the name of the relevant region. Go to step 5.

- To 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.
 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**.

8.1.13. Configure Device Pools

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, Edit, or Delete a Device Pool

1. Log in to the Admin Portal as Provider, Reseller, or Customer administrator.
2. If you're logged in as:
 - Provider or Reseller administrator: Go to (default menus) **Apps Management > CUCM > Device Pools**.
 - Customer administrator: Go to (default menus) **Apps Management > Advanced > CUCM > Device Pools**.
3. Choose an option:

<p>To add a new device pool</p>	<ul style="list-style-type: none"> • Click Add. • Choose the network device list (NDL) where you want to add the new device pool. <hr/> <p>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.</p> <hr/> <ul style="list-style-type: none"> • 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.
<p>To edit a device pool</p>	<ul style="list-style-type: none"> • Click on the relevant device pool in the list. • Go to step 4.
<p>To delete a device pool</p>	<ul style="list-style-type: none"> • 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

5. Click **Save**. The route partition appears in the device pool list.

Device Pool Settings Tab

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. <ul style="list-style-type: none"> • 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 Tab

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.

Roaming Sensitive Settings Tab

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

Option	Description
SRST Reference *	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Default value: None</p>
Connection Monitor Duration	<p>This setting defines the time that the Cisco Unified IP Phone monitors its connection to Unified CM before it unregisters from SRST and reregisters to Unified CM.</p> <p>To use the configuration for the enterprise parameter, you can enter “&#129;1” or leave the field blank. The default value for the enterprise parameter equals 120 seconds.</p> <p>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.</p>
Single Button Barge	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Default value: Default</p>
Join Access Lines	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Default value: Default</p>
Physical Location	<p>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.</p> <p>Default value: None</p>

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 Tab

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 Tab

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 Tab

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.

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	Unified CM applies the prefix that you enter in this field to calling party numbers that use Subscriber 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 Unified CM to strip from the calling party number of Subscriber type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to globalize the calling party number of Subscriber 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 Tab

Option	Description
National Prefix	<p>Unified CM applies the prefix that you enter in this field to calling party numbers that use National for the Called Party Numbering Type.</p> <p>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.</p> <p>Tip:</p> <p>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.</p> <p>Tip:</p> <p>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.</p>
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	<p>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.</p> <p>Tip:</p> <p>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.</p> <p>Tip:</p> <p>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.</p>
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.

Option	Description
Unknown Prefix	<p>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.</p> <p>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.</p> <p>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.</p>
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	<p>Unified CM applies the prefix that you enter in this field to called numbers that use Subscriber 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.</p> <p>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.</p> <p>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.</p>
Subscriber Strip Digits	Enter the number of digits, that you want Unified CM to strip from the called party number of Subscriber type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to transform the called party number of Subscriber 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.

Caller ID For Calls From This Phone Tab

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 Unified CM receives a call from a device in this device pool on an inbound line, Unified CM 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 Unified CM routes the call. For example, a transformation pattern can change a phone extension to appear as an E.164 number.

Connected Party Settings Tab

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. Unified CM 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.

Redirecting Party Settings Tab

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.

8.1.14. SIP Trunks

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.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (CUCM) is configured.
3. Choose an option:
 - If you're logged in as a Provider or Reseller admin, go to (default menus) **Apps Management > CUCM > SIP Trunks**.
 - If you're logged in as a Customer admin, go to (default menus) **Apps Management > Advanced > SIP Trunks**.
4. Do you want to . . .
 - Add a new SIP trunk? Click **Add**, 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 menu, select the hostname, domain name, or IP address of the Unified CM where you want to add 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 Unified CM located at the node, and all the Unified CM nodes in the hierarchies above the node where you're adding the SIP trunk.

To provision a Unified CM server, see the Installation Tasks section of Installing Cisco Unified Communications Manager.

6. In the **Device Name** field, enter a unique name for the new SIP trunk (or modify the existing device name, as applicable).
7. On the **Device Information** tab, complete at minimum, the mandatory *Device Information Tab*.
8. On the **Call Routing General** tab, complete at minimum, the mandatory *Call Routing General Tab*.
9. On the **Call Routing Inbound** tab, complete the required *Call Routing Inbound Tab*.
10. On the **Call Routing Outbound** tab, complete the required *Call Routing Outbound Tab*.
11. On the **SP Info** tab, complete the required *SP Info Tab*.
12. On the **GeoLocation** tab, complete at minimum, the mandatory *GeoLocation Tab*.
13. Click **Save** to save a new or updated SIP trunk.

The SIP trunk appears in the SIP trunk list. The SIP trunk is automatically reset on the Unified CM as soon as 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 Unified CM 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.

SIP Trunks Field Reference

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: <ul style="list-style-type: none"> • 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

Option	Description
Media Resource Group List	<p>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.</p> <p>Default value: None</p>
Location *	<p>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.</p> <p>Choose the appropriate location for this trunk:</p> <ul style="list-style-type: none"> • 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. <p>Default value: Hub_None</p>
AAR Group	<p>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.</p> <p>Default value: None</p>
Tunneled Protocol	<p>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).</p> <p>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.</p> <p>Default value: None</p>
QSIG Variant	<p>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.</p> <p>From the drop-down menu, select one of:</p> <ul style="list-style-type: none"> • 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 <p>Default value: No Changes</p>

Option	Description
ASN.1 ROSE OID Encoding	<p>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.</p> <p>From the drop-down menu, select one of</p> <ul style="list-style-type: none"> • 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 <p>Default value: No Changes</p>
Packet Capture Mode	<p>This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.</p> <p>From the drop-down menu, select one of:</p> <ul style="list-style-type: none"> • 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 nonencrypted 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. <p>Default value: None</p>
Packet Capture Duration	<p>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.</p> <p>To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.</p> <p>Default value: 0 (zero), Range is from 0 to 300 minutes</p>

Option	Description
Media Termination Point Required	<p>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 reoriginate 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.</p> <p>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.</p> <p>Default value: False (Cleared)</p>
Retry Video Call as Audio	<p>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.</p> <p>Default value: True (Selected)</p>
Path Replacement Support	<p>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.</p> <p>Default value: False (Clear)</p>
Transmit UTF-8 for Calling Party Name	<p>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.</p> <p>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.</p> <p>Default value: False (Cleared)</p>

Option	Description
Transmit UTF-8 Names for QSIG APDU	<p>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.</p> <p>Default value: False (Cleared)</p>
Unattended Port	<p>Select this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port.</p> <p>Default value: False (Cleared)</p>
SRTP Allowed	<p>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.</p> <p>Caution:</p> <p>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.</p> <p>Default value: False (Cleared)</p>
Consider Traffic on This Trunk Secure	<p>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.</p> <p>From the drop-down menu, select one of:</p> <ul style="list-style-type: none"> • When using both sRTP and TLS • When using sRTP Only - Displays when you select the SRTP Allowed check box. <p>Default value: When using both sRTP and TLS</p>

Option	Description
Route Class Signaling Enabled	<p>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.</p> <p>From the drop-down menu, select one of:</p> <ul style="list-style-type: none"> • 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. <p>Default value: Default</p>
Use Trusted Relay Point	<p>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.</p> <p>Select one of:</p> <ul style="list-style-type: none"> • 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. <p>Default value: Default</p>
PSTN Access	<p>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.</p> <p>Default value: True (Selected)</p>
Run On All Active Unified CM Nodes	<p>Select this check box to enable the trunk to run on every node.</p> <p>Default value: False (Cleared)</p>

Call Routing General Tab

Option	Description
Remote-Party-ID	<p>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.</p> <p>Note:</p> <p>Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled.</p> <p>Outgoing SIP Trunk Calls</p> <p>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.</p> <p>Incoming SIP Trunk Calls</p> <p>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.</p> <p>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.</p> <p>Note:</p> <p>The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.</p> <p>Default value: True (Selected)</p>

Option	Description
Asserted-Identity	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)</p>

Option	Description
Asserted-Type	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Note: These headers get sent only if the Asserted- Identity check box is selected. Default value: Default</p>
SIP Privacy	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Note: These headers get sent only if the Asserted Identity check box is selected. Default value: Default</p>

Call Routing Inbound Tab

Option	Description
Significant Digits	<p>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.</p> <p>Choose the number of significant digits to collect, from 0 to 32, or choose 99 to indicate all digits.</p> <p>Note: Unified CM counts significant digits from the right (last digit) of the number that is called. Default value: 99</p>
Connected Line ID Presentation	<p>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</p> <ul style="list-style-type: none"> • 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. <p>Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default</p>
Connected Name Presentation	<p>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</p> <ul style="list-style-type: none"> • 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. <p>Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default</p>
Calling Search Space	<p>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.</p> <p>Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAAdmin Parameters. Default value: None</p>

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 In-bound	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

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)

Option	Description
Connected Party Transformation CSS	<p>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.</p> <p>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.</p> <p>Default value: None</p>
Use Device Pool Connected Party Transformation CSS	<p>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.</p> <p>Default value: True (Selected)</p>

Call Routing Outbound Tab

Option	Description
Called Party Transformation CSS	<p>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.</p> <p>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.</p> <p>Default value: None</p>
Use Device Pool Called Party Transformation CSS	<p>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.</p> <p>Default value: True (Selected)</p>
Calling Party Transformation CSS	<p>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.</p> <p>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.</p> <p>Default value: None</p>
Use Device Pool Calling Party Transformation CSS	<p>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.</p> <p>Default value: True (Selected)</p>
Calling Party Selection	<p>Choose the directory number that is sent on an outbound call. Select one of the following options to specify which directory number is sent:</p> <ul style="list-style-type: none"> • 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. <p>Default value: Originator</p>

Option	Description
Calling Line ID Presentation	<p>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.</p> <p>Select one of</p> <ul style="list-style-type: none"> • 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. <p>Default value: Default</p>
Calling Name Presentation	<p>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.</p> <p>Select one of</p> <ul style="list-style-type: none"> • 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. <p>Note: This service is not available when QSIG tunneling is enabled.</p> <p>Default value: Default</p>
Calling and Connected Party Info Format *	<p>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.</p> <p>From the drop-down menu, select one of:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Default value: Deliver DN only in connected party</p>

Option	Description
Redirecting Diversion Header Delivery - Outbound	<p>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.</p> <p>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.</p> <p>Default value: False (Cleared)</p>
Use Device Pool Redirecting Party Transformation CSS	<p>Select this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to this device.</p> <p>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).</p>
Redirecting Party Transformation CSS	<p>Allows you to localize the redirecting party number on the device.</p> <p>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.</p>
Caller Information - Caller ID DN	<p>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:</p> <ul style="list-style-type: none"> • 55XXXX = 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. <p>You can also enter the international escape character +.</p> <p>Default value: None</p>
Caller Information - Caller Name	<p>Enter a caller name to override the caller name that is received from the originating SIP Device.</p> <p>Default value: None</p>
Caller Information - Maintain Original Caller ID DN and Caller Name in Identity Headers	<p>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.</p> <p>Default value: False (Cleared)</p>

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: <ul style="list-style-type: none"> • 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

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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Default value: None</p>
Destination - Destination Address IPv6	<p>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:</p> <ul style="list-style-type: none"> • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is selected. <p>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.</p> <p>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.</p> <p>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.</p> <p>Default value: None. If IPv4 field above is completed, this field can be left blank.</p>

Option	Description
Destination - Destination port	<p>Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0.</p> <p>Note:</p> <p>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.</p> <p>Default value: 5060</p>
Sort Order *	<p>Indicate the order in which the prioritize multiple destinations. A lower sort order indicates higher priority. This field requires an integer value.</p> <p>Default value: Empty</p>
MTP Preferred Originating Codec	<p>Indicate the preferred outgoing codec by selecting one of:</p> <ul style="list-style-type: none"> • 711ulaw • 711alaw • G729/G729a • G729b/G729ab <p>Note:</p> <p>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.</p> <p>This field is used only when the Media Termination Point Required check box is selected on the Device Information tab.</p> <p>Default value: 711ulaw</p>
BLF Presence Group *	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>Tip:</p> <p>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.</p> <p>Default value: Standard Presence Group</p>

Option	Description
SIP Trunk Security Profile *	<p>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.</p> <p>Default value: Non Secure SIP Trunk Profile</p>
Rerouting Calling Search Space	<p>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.</p> <p>Default value: None</p>
Out-Of-Dialog Refer Calling Search Space	<p>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).</p> <p>Default value: None</p>
SUBSCRIBE Calling Search Space	<p>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.</p> <p>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.</p> <p>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.</p> <p>To configure a SUBSCRIBE calling search space specifically for this purpose, configure a calling search space as you do all calling search spaces.</p> <p>Default value: None</p>
SIP Profile *	<p>From the drop-down list box, select the SIP profile that is to be used for this SIP trunk.</p> <p>Default value: Standard SIP Profile</p>

Option	Description
DTMF Signaling Method	<p>Select one of:</p> <ul style="list-style-type: none"> • 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. <p>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</p>
Normalization Script	<p>From the drop-down menu, choose the script that you want to apply to this trunk.</p> <p>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</p>
Normalization Script - Enable Trace	<p>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 scripiter produces SDI trace.</p> <p>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)</p>
Script Parameters	<p>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.</p>
Recording Information	<p>Enter one of</p> <ul style="list-style-type: none"> • 0 - None (default) • 1 - This trunk connects to a recording-enabled gateway • 2 - This trunk connects to other clusters with recording-enabled gateways

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)

Delete a SIP Trunk

To delete a SIP trunk:

1. Log in as provider, reseller or customer administrator.
2. Choose an option:
 - If you logged in as Provider or Reseller administrator, go to **Apps Management > CUCM > SIP Trunks**.
 - If you logged in as Customer administrator, go to **Apps Management > 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 Cisco Unified Communications Manager (CUCM) 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.
2. Perform one of:
 - If you logged in as Provider or Reseller administrator, go to **Apps Management > CUCM > SIP Trunks**.
 - If you logged in as Customer administrator, go to **Apps Management > Advanced > SIP Trunks**.

3. From the list of SIP trunks, click the SIP trunk to be reset, then choose **Action > Reset**.

8.1.15. 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 Unified Communications Manager, 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:
 - If you logged in as provider or reseller administrator, choose **Apps Management > CUCM > SIP Trunks**.
 - If you logged in as customer administrator, choose **Apps Management > Advanced > SIP Trunks**.
3. From the list of trunks, click the SIP trunk to be restarted, then click **Action > Restart**.

8.1.16. Route Groups

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. Choose an option:
 - If you logged in as Provider or Reseller administrator, go to (default menus) **Apps Management > CUCM > Route Groups**.
 - If you logged in as Customer administrator, go to (default menus) **Apps Management > Advanced > Route Groups**.
3. Do you want to ..
 - Add a 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.
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 CUCM 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 CUCM 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 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.

7. Click the Plus icon (+) to open the **Members** box.
8. Choose an option:
 - To add a device to the route group, go to Step 9.
 - To modify the priority of a device, go to Step 10.
 - To 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 a SIP trunk or gateway is added, 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.

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. Choose an option:

- If you logged in as Provider or Reseller administrator, choose **Apps Management > CUCM > Route Groups**.
- If you logged in as Customer administrator, choose **Apps Management > Advanced > Route Groups**.

3. From the list of trunks, select the route group you wish to delete.

4. Click **Delete**, then click **Yes** to confirm.

8.1.17. 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.

Perform these steps:

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. Choose an option:
 - If you logged in as provider or reseller administrator, choose **Apps Management > CUCM > Device Pools**.
 - If you logged in as customer administrator, choose **Apps Management > Advanced > 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. Click the **Local Route Group Settings** tab.
6. In the grid, from the **Local Route Group** drop-down menu, select the local route group.
7. In the grid, from the **Route Group** drop-down menu, select the route group or gateway.
8. To save the new local route association, click **Save**.

8.1.18. Route Lists

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 (Unified CM) 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:

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. Choose an option:
 - If you logged in as Provider or Reseller administrator, choose **Apps Management > CUCM > Route Lists**.
 - If you logged in as Customer administrator, choose **Apps Management > Advanced > Route Lists**.
3. Choose an appropriate option:
 - To add a new route list, click **Add**, then go to Step 4.
 - To 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 Field Reference](#).
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 Field Reference](#).
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 Field Reference

Field	Description
CUCM *	Select a Unified CM for the route list. This field is mandatory.
Name *	<p>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.</p> <p>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.</p>
Description	A description of the route list.
Call Manager Group Name *	<p>Select a Unified CM Group. Default is the default field. You can choose from Default, None, or select a group. This field is mandatory.</p> <p>Note: The route list registers with the first Unified CM in the group (which is the Primary Unified CM).</p>
Route List Enabled	<p>Select to enable the route list. This is the default.</p> <p>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.</p>
Run on Every Node	Select to enable the active route list to run on every node.
Route Group Items	See "Route Group Items fields".

Route Group Field Reference

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. 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 type numbering plan. Choose one of the following options: <ul style="list-style-type: none"> • Cisco CallManager - 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 subscriber by using a shortened subscriber number.

Field	Description
Calling Party Numbering Plan	<p>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.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - 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.
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	<p>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.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - 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 subscriber by using a shortened subscriber number.

Field	Description
Called Party Numbering Plan	<p>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.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - 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.

8.1.19. CUCM Translation Patterns

Overview

The Cisco Unified Communications Manager (CUCM) default dial plan translation patterns are deployed as part of the default dial plan translation patterns that ship with the VOSS 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 VOSS Automate to update translation patterns and route patterns. For details, see the "Provider HCS Dial Plan Management Support Guide".

Configure CUCM Translation Patterns

This procedure updates the CUCM translation patterns that are provisioned by the dial plan schema and adds new translation patterns from VOSS Automate that are not part of the standard dial plan package.

Note: For more information on CUCM 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. Choose an option, depending on your login:
 - If you're logged in as a Provider or Reseller administrator, go to (default menus) **Apps Management > CUCM > Translation Patterns**.
 - If you're logged in as a Customer administrator, go to (default menus) **Apps Management > Advanced > Translation Patterns**.
4. Choose an option:
 - To add a new translation pattern, click **Add**, then go to Step 5.
 - To 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 Unified Communications Manager (CUCM) 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 CUCMs located at the hierarchy node where you're adding the translation pattern, and all CUCMs in hierarchies above this hierarchy node.

When adding a translation pattern at a site, the CUCM 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, 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 of the **Translations Patterns** page.

Tip: Use the Corresponding CUCM attribute information provided in the tables to manually verify in the CUCM 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 Page

This page adds and edits CUCM translation patterns.

To access this page:

- If you're logged in as a Provider or Reseller administrator, go to (default menus) **Apps Management > CUCM > Translation Patterns**.
- If you're logged in as a Customer administrator, go to (default menus) **Apps Management > Advanced > Translation Patterns**.

You can select the following tabs on this page:

- *Pattern Definition Tab*
- *Calling Party Transformations Tab*
- *Connected Party Transformations Tab*
- *Called Party Transformations Tab*

Pattern Definition Tab

Option	Description
MLPP Precedence *	<p>From the drop-down menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this translation pattern:</p> <ul style="list-style-type: none"> • 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. <p>Default: Default Corresponding Unified CM Attribute: MLPP Precedence.</p>
Route Class *	<p>From the drop-down menu, choose a route class setting for this translation pattern:</p> <ul style="list-style-type: none"> • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data <p>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 Cisco Unified Communications Manager 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.</p> <p>Default: Default Corresponding Unified CM Attribute: Route Class.</p>
Calling Search Space	<p>From the drop-down menu, choose the calling search space for which you are adding a translation pattern, if necessary.</p> <p>Default: None Corresponding Unified CM Attribute: Calling Search Space.</p>

Option	Description
Use Originator's Calling Search Space	<p>To use the originator's calling search space for routing a call, select the Use Originator's Calling Search Space check box.</p> <p>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.</p> <p>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.</p> <p>Default: Clear</p> <p>Corresponding Unified CM Attribute: Use Originator's Calling Search Space.</p>
Block this pattern	<p>Indicates whether you want this translation pattern to be used for routing calls (such 8[2-9]XX) or for blocking calls.</p> <p>Default: Clear (meaning translation pattern is used for routing calls).</p> <p>Corresponding Unified CM Attribute: Block this pattern.</p>
Block Reason	<p>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:</p> <ul style="list-style-type: none"> • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded <p>Default: No Error</p> <p>Corresponding Unified CM Attribute: <entry box next to Block this pattern>.</p>
Provide Outside Dial Tone	<p>Outside dial tone indicates that Unified CM routes the calls off the local network. Select this check box for each translation pattern that you consider to be off network.</p> <p>Default: Selected</p> <p>Corresponding Unified CM Attribute: Provide Outside Dial Tone.</p>
Urgent Priority	<p>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.</p> <p>Default: Clear</p> <p>Corresponding Unified CM Attribute: Urgent Priority.</p>

Option	Description
Do Not Wait for Interdigit Timeout on Subsequent Hops	<p>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), Unified CM does not start the interdigit timer after it matches any of the subsequent patterns.</p> <p>Note: Unified CM 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, Unified CM does not start the interdigit timer after it matches any of the subsequent patterns.</p> <p>Note: Unified CM 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.</p> <p>Default: Clear Corresponding Unified CM Attribute: Do Not Wait for Interdigit Timeout On Subsequent Hops.</p>
Route Next Hop By Calling Party Number	<p>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.</p> <p>Default: Clear Corresponding Unified CM Attribute: Route Next Hop By Calling Party Number.</p>

Calling Party Transformations Tab

Option	Description
Use Calling Party's External Phone Number Mask	<p>Select the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.</p> <p>Default: Default Corresponding Unified CM Attribute: Use Calling Party's External Phone Number Mask.</p>
Calling Party Transform Mask	<p>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.</p> <p>Default: None Corresponding Unified CM Attribute: Calling Party Transform Mask.</p>
Prefix Digits (Outgoing Calls)	<p>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 +.</p> <p>Note: The appended prefix digit does not affect which directory numbers route to the assigned device.</p> <p>Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).</p>

Option	Description
Calling Line ID Presentation *	<p>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.</p> <p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>For more information about this field, see topics related to calling party number transformations settings in the Cisco Unified Communications Manager System Guide.</p> <p>Note:</p> <p>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.</p> <p>Default: Default</p> <p>Corresponding Unified CM Attribute: Calling Line ID Presentation.</p>

Option	Description
Calling Name Presentation *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>For more information about this field, see calling party number transformations settings in the Cisco Unified Communications Manager System Guide.</p> <p>Default: Default Corresponding Unified CM Attribute: Calling Name Presentation.</p>
Calling Party Number Type *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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 subscriber by using the shortened subscriber name. <p>Default: Unified CM Corresponding Unified CM Attribute: Calling Party Number Type.</p>

Option	Description
Calling Party Numbering Plan *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>Default: Unified CM Corresponding Unified CM Attribute: Calling Party Numbering Plan.</p>

Connected Party Transformations Tab

Option	Description
Connected Line ID Presentation *	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Default: Default Corresponding Unified CM Attribute: Connected Line ID Presentation.</p>
Connected Name Presentation *	<p>(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:</p> <ul style="list-style-type: none"> • 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. <p>For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide.</p> <p>Default: Default Corresponding Unified CM Attribute: Connected Name Presentation.</p>

Called Party Transformations Tab

Option	Description
Discard Digits	<p>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.</p> <p>Default: None</p> <p>Corresponding Unified CM Attribute: Discard Digits.</p>
Called Party Transform Mask	<p>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.</p> <p>Default: None</p> <p>Corresponding Unified CM Attribute: Called Party Transform Mask.</p>
Prefix Digits (Outgoing Calls)	<p>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.</p> <p>Note:</p> <p>The appended prefix digit does not affect which directory numbers route to the assigned device.</p> <p>Default: None</p> <p>Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).</p>
Called Party Number Type *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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 subscriber by using a shortened subscriber number. <p>Default: Unified CM</p> <p>Corresponding Unified CM Attribute: Called Party Number Type.</p>

Option	Description
Called Party Numbering Plan *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>Default: Unified CM Corresponding Unified CM Attribute: Called Party Numbering Plan.</p>

8.1.20. How to Configure Cisco Unified Communications Manager Route Patterns

1. Log in as provider, reseller, or customer administrator.
2. Make sure the hierarchy path is set to the node where you want to add or edit the route pattern.
3. Perform one of:
 - If you are logged in as provider or reseller administrator, choose **Device Management > CUCM > Route Patterns**.
 - If you are logged in as customer administrator, choose: **Device Management > Advanced > Route Patterns**.
4. Perform one of:
 - To add a new route pattern, click **Add**, then go to Step 5.
 - To edit an existing route pattern, click on the 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 a route pattern is added; it does not appear when you edit a route pattern.

Important:

If you are adding or editing a route pattern at any hierarchy node above a site level, the only Unified CMs that appear in the **CUCM** drop-down list are Unified CMs that are located at the node where you are adding the route pattern, and all Unified CMs in hierarchies above the node where you are adding the route pattern. If you are adding or editing a route pattern at a site level, the Unified CM that appears in the **CUCM** drop-down list is the Unified CM 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 Unified CM, the drop-down list is empty and a route pattern can not be added to the site.

6. In the **Route Pattern** field, enter the route pattern, or modify the existing route pattern if desired. This field is mandatory. 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 desired 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:

Make sure that the combination of route pattern, route filter, and partition is unique within the Unified CM cluster.

8. In the **Description** field, enter a description for the route pattern and route partition if desired. The 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 tab as appropriate (see below):
10. Click **Save** when complete to save the new or updated route pattern.

Route Pattern: Pattern Definition Fields

Tip:

Use the Corresponding Cisco Unified Communications Manager (Unified CM) Attribute information provided in the table to manually verify in the Unified CM GUI that fields have been mapped correctly.

Option	Description
MLPP Precedence *	<p>From the drop-down menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern:</p> <ul style="list-style-type: none"> • 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 <p>Default: Default Corresponding Unified CM Attribute: MLPP Precedence.</p>
Apply Call Blocking Percentage	<p>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.</p> <p>Note: The Apply Call Blocking Percentage field gets enabled only if the MLPP level is immediate, priority, routine, or default.</p> <p>Default: Clear Corresponding Unified CM Attribute: Apply Call Blocking Percentage.</p>

Option	Description
Call Blocking Percentage	<p>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.</p> <p>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.</p> <p>Note: The Call Blocking Percentage field gets enabled only if the Apply Call Blocking Percentage check box is selected.</p> <p>Default: None Corresponding Unified CM Attribute: <Entry box next to Apply Call Blocking Percentage>.</p>
Route Class *	<p>From the drop-down menu, choose a route class setting for this route pattern:</p> <ul style="list-style-type: none"> • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data <p>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.</p> <p>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.</p> <p>If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class.</p> <p>Default: Default Corresponding Unified CM Attribute: Route Class.</p>
Route List (Mandatory if gateway or trunk is not specified)	<p>Choose the route list for which you are adding a route pattern. Default: None Corresponding Unified CM Attribute: Gateway/Route List.</p>
Gateway/Trunk (Mandatory if route list is not specified)	<p>Choose the gateway or trunk list for which you are adding a route pattern.</p> <p>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.</p> <p>Default: Clear Corresponding Unified CM Attribute: Gateway/Route List.</p>

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: <ul style="list-style-type: none"> • 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.

Option	Description
Require Forced Authorization Code	<p>If you want to use forced authorization codes with this route pattern, select the check box.</p> <p>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.</p> <p>Default: Clear</p> <p>Corresponding Unified CM Attribute: Require Forced Authorization Code.</p>
Authorization Level *	<p>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.</p> <p>Default: 0</p> <p>Corresponding Unified CM Attribute: Authorization Level</p>
Require Client Matter Code	<p>If you want to use client matter codes with this route pattern, select this check box.</p> <p>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.</p> <p>Default: Clear</p> <p>Corresponding Unified CM Attribute: <Entry box next to Authorization Level>.</p>

Route Pattern: Calling Party Transformations Fields

Option	Description
Use Calling Party's External Phone Number Mask	<p>Select the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.</p> <p>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.</p> <p>Default: Default Corresponding Unified CM Attribute: Use Calling Party's External Phone Number Mask</p>
Calling Party Transform Mask	<p>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.</p> <p>Default: None Corresponding Unified CM Attribute: Calling Party Transform Mask</p>
Prefix Digits (Outgoing Calls)	<p>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 +.</p> <p>Note: The appended prefix digit does not affect which directory numbers route to the assigned device.</p> <p>Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).</p>

Option	Description
Calling Line ID Presentation *	<p>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.</p> <p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>For more information about this field, see topics related to calling party number transformations settings in the Cisco Unified Communications Manager System Guide.</p> <p>Default: Default</p> <p>Corresponding Unified CM Attribute: Calling Line ID Presentation.</p>
Calling Name Presentation *	<p>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.</p> <p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>For more information about this field, see calling party number transformations settings in the Cisco Unified Communications Manager System Guide.</p> <p>Default: Default</p> <p>Corresponding Unified CM Attribute: Calling Name Presentation.</p>
Calling Party Number Type *	<p>Choose the format for the number type in calling party directory numbers.</p> <p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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 subscriber by using the shortened subscriber name. <p>Default: Unified CM</p> <p>Corresponding Unified CM Attribute: Calling Party Number Type.</p>

Option	Description
Calling Party Numbering Plan *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>Default: Unified CM Corresponding Unified CM Attribute: Calling Party Numbering Plan.</p>

Route Pattern: Connected Party Transformations Fields

Option	Description
Connected Line ID Presentation *	<p>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.</p> <p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide.</p> <p>Default: Default Corresponding Unified CM Attribute: Connected Line ID Presentation.</p>

Option	Description
Connected Name Presentation *	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide.</p> <p>Default: Default Corresponding Unified CM Attribute: Connected Name Presentation.</p>

Route Pattern: Called Party Transformations Fields

Option	Description
Discard Digits	<p>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.</p> <p>Default: None Corresponding Unified CM Attribute: Discard Digits.</p>
Called Party Transform Mask	<p>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.</p> <p>Default: None Corresponding Unified CM Attribute: Called Party Transform Mask.</p>
Prefix Digits (Outgoing Calls)	<p>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.</p> <p>Note: The appended prefix digit does not affect which directory numbers route to the assigned device.</p> <p>Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).</p>

Option	Description
Called Party Number Type *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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 subscriber by using a shortened subscriber number. <p>Default: Unified CM Corresponding Unified CM Attribute: Called Party Number Type.</p>
Called Party Numbering Plan *	<p>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.</p> <p>Choose one of:</p> <ul style="list-style-type: none"> • 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. <p>Default: Unified CM Corresponding Unified CM Attribute: Called Party Numbering Plan.</p>

8.1.21. CTI Route Points

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.

Perform these steps:

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. To open the CTI Route Points list view, choose an option:
 - Logged in as a Provider or Reseller admin? Go to (default menus) **Apps Management > CUCM > CTI Route Points**.
 - Logged in as Customer admin? Go to (default menus) **Apps Management > Advanced > CTI Route Points**.
4. Choose an option:
 - To view the details on an existing CTI route point, click an entry in the list view.

Home / CTI Route Points / CTIRP32323

Common Device Configuration	<input type="text"/>
Calling Search Space	<input type="text"/>
Location *	Cu1Si1-Location
User Locale	<input type="text"/>
Media Resource Group List	<input type="text"/>
Network Hold MOH Audio Source	<input type="text"/>
User Hold MOH Audio Source	<input type="text"/>
Use Trusted Relay Point Required Field *	Default
Calling Party Transformation CSS	<input type="text"/>
Geolocation	<input type="text"/>
Use Device Pool Calling Party Transformation CSS	<input checked="" type="checkbox"/>

Line

> 82010008 Cu1Si1-Feature-PT

- To add a new CTI route point, click **Add**. Go to step 5.
5. Complete at least the mandatory fields. See [CTI Route Points Field Reference](#).
 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 Field Reference](#).

7. Click **Save**.

CTI Route Points Field Reference

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 Unified Communications Manager 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 Unified CM 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 Unified CM uses the Media Resource Group that is defined in the device pool.

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 Unified CM 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 Unified CM 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 *	<p>Enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. This field is mandatory. Choose one of the following values:</p> <ul style="list-style-type: none"> • 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. <p>A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.</p>
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.

CTI Route Points Line Field Reference

Field	Description
Directory Number *	<p>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.</p> <p>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.</p> <p>When saving the CTI route point, the combination of directory number and route partition name displays as a summary header in the Line section.</p>
Route Partition *	<p>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.</p> <p>When saving the CTI route point, the combination of directory number and route partition name displays as a summary header in the Line section.</p>
Index	<p>This field is the line position on the device. If left blank, an integer is automatically assigned.</p>
External Phone Number Mask	<p>Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line.</p> <p>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.</p>
Line Text Label	<p>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.</p> <p>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.</p>
Display (Internal Caller ID)	<p>Leave this field blank to have the system display the extension.</p> <p>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.</p>
ASCII Display (Caller ID)	<p>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.</p>
Ring Setting (Phone Active)	<p>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:</p> <ul style="list-style-type: none"> • Use system default • Disable • Flash only • Ring once • Ring • Beep only

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 Unified CM logs missed calls in the call history for the shared line appearance on the phone.

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.

8.1.22. Softkey Templates

Introduction

Softkey templates manage softkeys that are used by the Cisco Unified CM IP Phones, for example 7970. There are two types of softkey templates:

- standard
- customized

VOSS Automate includes the following Unified CM system softkey templates, which cannot be modified or deleted:

- Cisco Assistant with Feature Hardkeys
- Cisco Chaperone Phone with Feature Hardkeys
- 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.

How to 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. See: [Controlling a Data Sync with a Model Type List](#).

```
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** check box. 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.
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**.

8.1.23. Call Park Management

Overview

The 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 Unified CM cluster. If clusterwide call park is disabled, the call park numbers are only available to devices on the nominated Unified CM 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 in the Directed Call Park Configuration window.

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 window.

Adding Call Parks

To add call parks:

1. Go to (default menus) **Apps Management > CUCM** then choose either **Clusterwide Call Park** or **Clusterwide Directed Call Park**.
2. Click **Add**.
3. Browse to the required Site level.
4. Enter, at minimum, 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**.

8.1.24. Media Resources

VOSS Automate allows for the management of the following media resources in Unified CM:

- 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.
-

Add a Media Termination Point (MTP)

VOSS Automate supports the following media termination point type: Cisco IOS Enhanced Software Media Termination Point

To add a MTP:

1. Navigate to the required customer or site level.
2. Select the Unified CM from the **CUCM** drop-down list.
3. Enter a **MTP Name**
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 Unified CM 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**

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
- **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**
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

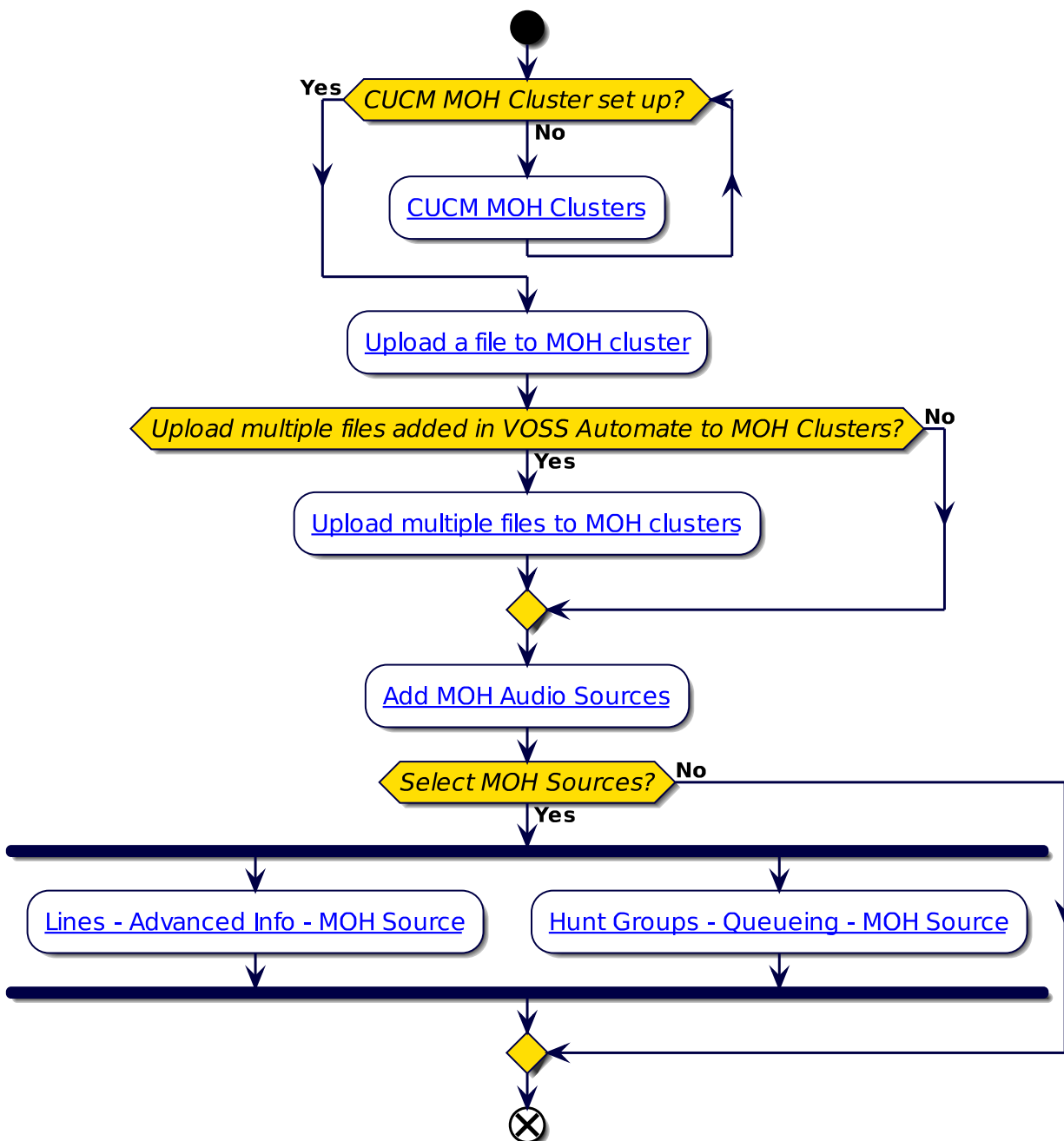
Use the **Delete** button to delete a Conference Bridge.

8.2. CUCM Music On Hold (MOH)

8.2.1. Music on Hold (MOH) File Management

Overview

VOSS 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 Unified CM (CUCM).



Managing MOH files involves:

1. Adding a CUCM MOH cluster for uploading MOH files.
2. Uploading MOH .wav files to VOSS Automate, and (optionally) to the CUCM MOH cluster. VOSS Automate syncs the file to CUCM once it's added to the CUCM MOH cluster.
3. Adding MOH audio sources for use in VOSS Automate (for example, to manage lines and hunt groups).

Note: Deleting a .wav file from VOSS Automate does not remove the file from CUCM MOH clusters.

A MOH file you're adding is uploaded to the VOSS Automate database, and if you selected a MOH cluster,

the file is also added to the MOH cluster (to the publisher, and to any subscriber servers flagged as music servers). A data sync is triggered to add the files to CUCM, and any MOH files on CUCM are imported to VOSS Automate in the sync. These MOH files are available for selection when adding or managing MOH audio source files.

Call Managers (CUCM), MOH Files, NDLs, and Upgrading VOSS Automate

When uploading MOH files at site level, the CUCM MOH cluster is automatically selected based on the site Network Device List (NDL).

Since data syncs export and import MOH files between VOSS Automate and CUCM, when upgrading from a previous version of VOSS 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 (default menus) **Administration Tools > Data Sync**. Data sync entries are prefixed with the name of the API (CMCCS - Call Manager Control Center Services)

See [Introduction to Data Sync](#)

Add a CUCM MOH Cluster

This procedure adds a CUCM MOH cluster.

Note: MOH files are uploaded to the CUCM MOH cluster.

1. Log in to the Admin Portal.
2. Go to (default menus) **Apps Management > CUCM Music On Hold > 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:

Cluster Name	Add a name for the CUCM MOH cluster. You can use the same name as the CUCM cluster, or a unique name.
Publisher Server Name	Choose a CUCM publisher server from the list of available CUCM 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 CUCM 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 CUCM server GUI.
Publisher Password	Specify the password of the publisher username.
CUCM Subscriber Details	Click the Plus icon (+) to add CUCM subscriber servers (one or more), and specify details for each subscriber server you're adding. These CUCM subscriber servers are part of the CUCM cluster. For each server you add, you will need to provide the following details: <ul style="list-style-type: none"> 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 CUCM MOH cluster.

View MOH Files

This procedure displays the list of files that exist on the Call Manager Publisher.

Note:

- Files uploaded to MOH clusters in VOSS 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:

- Log in to the Admin Portal as a Provider, Customer, or Reseller admin.
- Go to (default menus) **Apps Management > List MOH Audio Files**.
- 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 VOSS 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 VOSS Automate, or after you've added the file to VOSS 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:

- Log in to the Admin Portal.
- Go to (default menus) **Apps Management > CUCM Music On Hold > Manage Files and Upload to MOH Cluster**.
- In the list view, click the Plus icon (+) to open the **Manage Files And Upload to MOH Cluster / New Record** page.
- 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.

-
- 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 VOSS 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 VOSS Automate can be re-uploaded to the same CUCM MOH cluster, or to another CUCM MOH cluster.
 - Deleting a .wav file from VOSS 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 (default menus) **Apps Management > CUCM Music On Hold > Upload Multiple Files to MOH Clusters**.
3. On the **Upload Multiple Files to MOH Clusters** page:
 - 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.

4. Save your changes.

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 (default menus) **Apps Management > CUCM Music On Hold > Add MOH Audio Source** to open the **Add MOH Audio Source** page.
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 VOSS 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, VOSS 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 VOSS Automate may be viewed, updated, or deleted via (default menus) **Apps Management > CUCM Music On Hold > 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 subscribers. See Directory Number Advanced Information in [Lines](#)
 - Managing hunt groups for subscribers. See Queuing in [Add a Hunt Group](#)
-

View and Manage MOH Audio Sources

1. Log in to the Admin Portal.
2. Go to **Apps Management > CUCM Music On Hold > 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 <i>1</i> .
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.

8.3. CUCM FAC Management

8.3.1. Forced Authorization Codes (FAC)

This Unified CM 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 codes, the deployed dial plan must to be setup in a way that enables the codes to be used. For more details on the use of FAC codes and Unified CM functionality refer to the Cisco UCM feature guides.

VOSS Automate provides full support for FAC codes 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 codes 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 VOSS 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.

8.3.2. Using Device Models to Manage FAC

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 VOSS 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):

Add a FAC Code

1. Browse to the appropriate hierarchy level for the FAC code (e.g. Customer or Site).
2. Navigate to the FAC Code menu item which will give a 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. Navigate to the FAC Code menu item which will give a list of existing codes. Use the filters and/or hierarchy breadcrumb to locate the code to modify and then select it.
2. Edit the settings and click **Save**.

Delete an Existing FAC Code

1. Navigate to the FAC Code menu item which will give a 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**.

8.3.3. Using VOSS Automate to Manage FAC

Overview

The VOSS 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 need 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 VOSS 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 a FAC

1. Navigate to the required customer or site level.
2. From the **Forced Authorization Codes** form (default menu **Apps Management > CUCM FAC Management > Forced Authorization Codes**).
3. Click **Add**.
4. Complete the following mandatory settings (see form **Help notes** for additional information):

A Provider Admin can customize the form help by cloning, editing and saving the help text on the **Customize Help** form to a lower hierarchy level.

Field Name	Description
Name*	A unique name describing the FAC code, e.g. Customer code + Subscriber 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. Open the **Forced Authorization Codes** form (default menu **Apps Management > CUCM FAC Management > 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 button bar.

¹ See [Customize Authorization Levels](#)

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. Open the **Sync FAC Codes Cross Clusters** form (default menu **Apps Management > CUCM FAC Management > Sync FAC Codes Cross Clusters**).
3. Choose **Confirm**.
4. Click **Save**.

8.3.4. Customize Authorization Levels

Open the **Customize Authorization Levels** form (default menu **Apps Management > CUCM FAC Management > 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.

8.4. CUC (Cisco Unity Connection)

8.4.1. Cisco Unity Connection (CUC) Servers

Overview

Cisco Unity Connection (CUC) devices provide voicemail services for HCS deployments, and can be dedicated to a customer or shared across multiple customers.

To dedicate a CUC to a single customer	Configure the CUC at the customer hierarchy node.
To 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.

Scheduled Data Syncs

Configuring a CUC device on VOSS Automate creates a scheduled data sync to import model data from the device into VOSS 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 (via **Apps Management > CUC > Schedules**).

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 **Apps Management > Advanced > Perform Publisher Actions**, or from **Administration Tools > Data Sync**.

Important: Allow the initial data sync to complete before doing more configuration on VOSS Automate that requires information from CUC.

The performance of a data sync can be improved by controlling the types of data that are synced. See [Controlling a Data Sync with a Model Type List](#) for more information.

Note: References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

Add a CUC Server

To add a CUC server:

1. Log in as the appropriate hierarchy administrator.
 - Provider or Reseller admins can create a shared instance.
 - Customer, Provider, or Reseller admins can create a dedicated instance.
2. Choose the relevant hierarchy.
 - You can create a shared instance at the Provider or Reseller level.
 - You can create a dedicated instance at the Customer level.
3. Go to (default menus) **Apps Management > CUC > Servers**.
4. Click **Add**.
5. Enter a Cisco Unity Connection server name in the **CUC Server Name** field.

Note: A CUC server that has been configured in HCM-F and synced into VOSS Automate may exist at the *sys.hcs* hierarchy.

If the server name you enter matches this server, the **Migrate from HCM-F to VOSS Automate** check box is displayed.

Click **Save** to migrate this server to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

6. Select the **Publisher** check box if you are configuring a publisher node.

Note: The **Publisher** tab is populated only when the **Publisher** check box is selected.

Provide details for the **Publisher** tab:

Field	Description
Prime Collab	Select the Prime Collaboration management application monitoring this cluster. To unassociate Prime Collaboration for this cluster, select None .
Call Processing ID	The Call Processing ID of this cluster
Cluster ID	The Cluster ID of this cluster.
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. The available versions depend on the version of HCM-F that has been configured.
Port	The port on the Cisco Unity Connection server to connect to. Default is 8443.
Monitoring	For new servers and if arbitrator servers are available, monitoring can be enabled for this Unity Connection server on VOSS Insights. The arbitrator server check boxes 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 VOSS Insights. The arbitrator checkboxes will then reflect the asset status.

Note: For details on monitoring and VOSS Insights, see [Introduction to VOSS Insights Monitoring](#).

7. Fill in the **Cluster Name** field with the name you want for this cluster. A new cluster is created with this name. This field is mandatory.

Note: If the **Publisher** check box is not selected, the **Cluster Name** field appears as a drop-down list, from which you choose an existing cluster.

8. Expand **Network Addresses**.

- a. Choose the SERVICE_PROVIDER_SPACE address space.
- b. The **Hostname** field is automatically populated with the Cisco Unity Connection Server Name. Edit it if necessary.
- c. Enter the IP address of the Cisco Unity Connection 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 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 Cisco Unity Connection 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 PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
- b. Fill in the user ID and password that you configured when you installed the Cisco Unity Connection.
- 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.
 - ADMIN credentials are used by VOSS Automate to access the Cisco Unity Connection REST API interface for provisioning synchronization.
 - PLATFORM credentials are used by HCM-F (HLM service) to set the deployment mode and restart the publisher.
 - ADMIN, HTTP, and SNMP are required for PCA to manage Cisco Unity Connection. These credentials must be manually configured in Cisco Unity Connection, then configured in VOSS Automate's **Device Management > CUC > Servers > Credentials** section.
 - PLATFORM and ADMIN are required for Service Inventory to generate reports for UC applications.

10. Click **Save**.

Delete a CUC Server

Deleting a Cisco Unity Connection (CUC) Server in VOSS Automate also deletes local data that has been synced to it from the Cisco Unity Connection Server, including:

- Users
- Configuration parameters
- Dial Plan information (if applicable)

8.5. CER (Cisco Emergency Responder)

8.5.1. Configure Cisco Emergency Responder (CER)

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.
 - References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.
-

To configure CER:

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. Choose **Apps Management > CER > Servers**.

4. Perform one of the following:
 - 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.

Note: A Cisco Emergency Responder server that has been configured in HCM-F and synced into VOSS Automate may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS Automate** check box is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

6. Select the **Publisher** check box if you are configuring a publisher node.

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 cannot 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.

9. Fill out the fields on the **Publisher** tab:

Field	Description
Version	Select the version of the Cisco Emergency Responder Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Multi-Tenant	Read-only field. 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

8.5.2. Associate CER with Customers

Prerequisites:

- A customer must be configured.
- 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. Choose **Device Management > CER > Servers**.
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 check box to the left of each customer to be associated with the CER cluster.

Note: To remove one or more customer associations from the CER cluster, clear the box for each customer to be disassociated from the cluster.

6. Click **Save**.

8.5.3. View Associated Clusters on CER Servers

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. Choose **Device Management > CER > Servers**.
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.

8.6. UCCX (Cisco Contact Center Express)

8.6.1. Configure Contact Center Express (UCCX) Server

Overview

Reseller level and higher administrators can view and manage Cisco 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 Network Device Lists be updated with the UCCX server references.
- Cisco Unified CM (CUCM) and UCCX server integration should also be carried out as pre-configuration for this feature to work correctly.

Related Topics

- [Contact Center](#)

Add a UCCX Server

1. Log in as Provider administrator or higher and navigate to the required hierarchy.
2. Go to (default menus) **Apps Management > UCCX > Servers**.
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 Cisco UCM Application users to be used for agent device association. Typically this would be the RMCM application user (CCX Resource Manager, Unified CM Telephony user), but could also include others for call recording and so on.

Run a Pull Data Sync from the UCCX Server

Once the Contact Center Express (UCCX) server is added, you can run a pull data sync from the server to VOSS Automate. This can be done from the Contact Center Server input interface menu: **Actions > Sync**.

VOSS Automate also automatically creates two default Data Sync instances to manage and schedule data synchronization between the device and VOSS Automate. These can be seen from the **Data Sync** list view:

<code>SyncUccx- <host></code>	Use this sync to schedule or manually sync data between the server and VOSS Automate.
<code>PurgeUCcx- <host></code>	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 .

The 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 VOSS Automate.

8.7. Webex

8.7.1. 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, so that user capability can be managed. 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.

Add a Cisco Webex server

This procedure adds and configures the server.

Note: For more information about conferencing, see [Introduction to Conferencing](#).

1. Log in as Provider or Reseller administrator.
2. Go to (default menus) **Apps Management > WebEx > Servers**.
3. Click **Add**.
4. Complete, at minimum, the mandatory [Webex Server Field Reference](#).

5. Click **Save**.
6. Test the connection to the Webex server:
 - Select **Apps Management > Advanced > WebEx Network Device**.
 - Click in the row for the relevant Webex server; then, choose **Action > Test Connection**.

Webex Server Field Reference

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.

8.8. Prime Collab (Cisco PCA)

8.8.1. Role Mapping for Prime Collaboration Assurance

Service providers deploying VOSS Automate use role-based access control (RBAC) to restrict certain management actions to a specific set of users. Administrators at each level have access to the information in all hierarchy levels below them.

Prime Collaboration Assurance roles are hierarchical in the following order:

1. Super Administrator - Includes all privileges of System Administrator, Network Administrator, Operator, and Help Desk, along with the Super Administrator permissions.
2. System Administrator.

3. Network Administrator - Includes all privileges of Operator and Help Desk, along with the Network Administrator permissions.
4. Operator - Read-only administrative access.
5. Help Desk.

VOSS Automate roles map to the Prime Collaboration Assurance roles shown in the following table. You can find Roles in VOSS Automate under **Role Management > Roles**. The three drop-down lists that are important in VOSS Automate are **Hierarchy Type**, **Service Assurance Role Type**, and **HCS Component Access**.

Prime Collaboration Assurance roles are shown in this table in hierarchical order from top to bottom. The role shown in BOLD represents the highest role available.

Role Mapping Between VOSS Automate and Prime Collaboration Assurance

Hierarchy Type in VOSS Automate	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
Provider	Administrator	Fulfillment and Service Assurance	Super Administrator , System Administrator, Network Administrator	Provider roles are always the top organization unit in the VOSS Automate navigation tree. The Provider roles can see all devices, including shared devices such as Cisco Unified Border Element (SP Edition). A Provider with this role has Administrative level access to VOSS Automate and Prime Collaboration Assurance.
				A Provider with this role has Administrative
		Service Assurance Only		level access to VOSS Automate and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Provider with this role has Administrative level access to VOSS Automate.
	Operator	Fulfillment and Service	Operator , Help Desk	A Provider with this role has Administrative level read-only access to VOSS Automate and Prime Collaboration Assurance.

Hierarchy Type in VOSS Automate	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
		Service Assurance Only		A Provider with this role has Administrative level read-only access to VOSS Automate and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Provider with this role has Administrative level read-only access to VOSS Automate.
Reseller	Administrator	Fulfillment and Service Assurance	Network Administrator	These roles can only see the customer information that belongs to your Reseller organization. A Reseller with this role has Administrative level access to VOSS Automate and Prime Collaboration Assurance.
		Service Assurance Only	Network Administrator	A Reseller with this role has Administrative level access to VOSS Automate and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Reseller with this role role has Administrative level access to VOSS Automate.

Hierarchy Type in VOSS Automate	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
	Operator	Fulfillment and Service Assurance	Operator, Help Desk	A Reseller with this role has Administrative level read-only access to VOSS Automate, Hosted Collaboration Mediation-Fulfillment, and Prime Collaboration Assurance.
		Service Assurance Only	Operator, Help Desk	A Reseller with this role has Administrative level read-only access to VOSS Automate and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Reseller with this role has Administrative level read-only access to VOSS Automate and Hosted Collaboration Mediation-Fulfillment.
Customer	Administrator	Fulfillment and Service Assurance	Network Administrator	With this role you can only see your own customer information. A Customer with this role has Administrative level access to VOSS Automate, Hosted Collaboration Mediation-Fulfillment, and Prime Collaboration Assurance.
		Service Assurance Only	Network Administrator	A Customer with this role has Administrative level access to VOSS Automate and Prime Collaboration Assurance.

Hierarchy Type in VOSS Automate	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
		Fulfillment Only	Not Applicable	A Customer with this role has Administrative level access to VOSS Automate and Hosted Collaboration Mediation-Fulfillment.
	Operator	Fulfillment and Service Assurance	Operator, Help Desk	A Customer with this role has Administrative level read-only access to VOSS Automate, Hosted Collaboration Mediation-Fulfillment, and Prime Collaboration Assurance.
		Service Assurance Only	Operator, Help Desk	A Customer with this role has Administrative level read-only access to VOSS Automate and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Customer with this role has Administrative level read-only access to VOSS Automate and Hosted Collaboration Mediation-Fulfillment.

8.8.2. Prime Collaboration Assurance Integration

These workflow steps allow you to integrate VOSS Automate with Prime Collaboration Assurance (PCA).

Prerequisites:

- Review role mapping for PCA to understand how your VOSS Automate roles map to PCA roles.
- In PCA, enable SFTP (disabled by default).
- Ensure that the smuser account is available in PCA, and you can and you can log in. The default SFTP credential in PCA is smuser/smuse.

Perform these steps:

1. Configure PCA.
2. Set up PCA to monitor the Unified Computing System.
3. Add the Service Provider space and Application space under Address space information when adding Cisco Unity Connection (CUC) and Cisco IM and Presence server to VOSS Automate. PCA uses the server's service provider space to monitor the applications. See [Set Up IM and Presence Service Servers](#).
4. Add Cisco IM and Presence Service subnode information to VOSS Automate if you have multiple instances of Cisco IM and Presence Service deployed.
5. Ensure that your UC applications have all required credentials. At minimum, credentials are required for Administration, platform, SNMP, JTAPI, and HTTP.

Note: Other credentials may be required, depending on what you're monitoring. For more information about the required protocols, support, and credentials to set up devices for PCA monitoring, see:

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/collaboration/setting_up_devices/PCA_12-1/Setting_up_Devices_for_Cisco_Prime_Collaboration_Assurance.html

6. Synchronize your customer information with VOSS Automate. See *Add a CUCM Server* for more information.
7. (Optional) Ensure that the Session Border Controller has the required credentials in Hosted Collaboration Mediation-Fulfillment(HCMF).
8. Ensure that the CPE (analog gateway, or LBO deployed at CPE) has the required credentials in VOSS Automate under Devices.
9. Enter the SNMP commands manually on the Local Break Out (LBO) gateway or analog gateway. This task is required to manage the LBO gateway and analog gateway in PCA.

Note: IOS default command builder does not generate SNMP commands. The administrator must enter SNMP commands.

10. Add PCA to VOSS Automate (default menus: **Apps Management > Prime Collab > Servers**). Administration and SFTP credentials are required.
11. Onboard the customer to PCA, using the Cisco Unified Communications Manager (CUCM) admin interface.
 - CHPA pushes SNMP, Syslog, and Billing server configuration information to your VOSS Automate automatically.
 - In HCMF (Provider deployments), the CHPA pushes SNMP, Syslog, and Billing server configuration information to your VOSS Automate automatically.
 - Add Syslog and SNMP configurations manually for CUC and IM and Presence Service before onboarding.

Note: Configure these credentials in CUCM nodes to ensure a successful CHPA configuration:

- Administration credentials for CUCM
- Platform credentials for CUCM
- SNMP and HTTP credentials for CUCM
- SFTP for PCA

This configuration is pushed to CUCM:

- The SNMP community string
- CDR (SFTP of the PCA server)
- Syslog configuration

JTAPI credentials are optional credentials used for TelePresence session monitoring. They are used to retrieve session status information from TelePresence devices. Create a JTAPI user in the CUCM with the required permission to receive JTAPI events on endpoints. The credentials must be manually configured in CUCM.

PCA manages multiple call processor clusters and as a result you must ensure that the cluster IDs are unique.

12. Sync Active Directory users with VOSS Automate.

Note: Only users at the provider hierarchy are pushed to PCA.

13. To confirm whether the Cisco HCM-F (if installed) push and subsequent Device Discovery were successful, verify that the devices are managed in PCA.

Review the Current Inventory table at **Operate > Device Work Center** (Prime Collaboration Assurance 10.5.1) or **Device Inventory > Inventory Management** (Prime Collaboration Assurance 11.5 or later).

Devices appear in **Inventory Management** with the Managed status.

For details on the Prime Collaboration Assurance Inventory table, see the **Manage Inventory** section of Cisco Prime Collaboration Assurance Guide Advanced, available at:

<http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-user-guide-list.html>.

Note: In Cisco HCM-F (if installed), you may receive a **Credential-related error message**, but there can be other reasons for this error, such as a firewall issue. We recommend that you use PCA to verify that devices are managed.

If a device is not going into the managed state successfully, refer to the **Troubleshooting** section of the **Discover Devices** chapter in Cisco Prime Collaboration Assurance Guide Advanced for troubleshooting tips.

A list of the devices supported by PCA is available at:

<http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-device-support-tables-list.html>.

14. Check the PCA dashboard.

See **UC Performance Monitor Dashboards** in the Cisco Prime Collaboration Assurance Guide Standard or Cisco Prime Collaboration Assurance Guide Advanced and Analytics Guide.

15. Monitor components and devices with Prime Collaboration Assurance.

8.9. IOS

8.9.1. IOS Device Management

In VOSS 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.

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.

Perform these steps:

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 [Set up 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 a 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](#).

8.9.2. Command Builders

You can build a repository of IOS commands to be run when certain events, such as adding an IOS device, occur. 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.

To set up a Command Builder:

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. Choose **Apps Management > IOS > Command Builder**.
4. Click **Add**.
5. Provide the following information:

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**.

Clone a Command Builder

This procedure clones 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.

To clone a command builder:

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. Choose **Apps Management > IOS > Command Builder**.
4. Click the Command Builder name you want 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.

Perform these steps:

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. Choose **Apps Management > IOS > Commands**. A table containing the Command Builders that have been triggered is displayed. The table contains this information:

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:

To 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. Choose **Apps Management > IOS > Consolidate Commands**.
4. Click **Add**.
5. On the **Consolidate Commands** screen, complete at minimum, the mandatory *Consolidate Commands Fields*.
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.

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 Fields

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 *	<p>Choose the device types for which you want to consolidate commands.</p> <p>IOS Device Choose this to get commands for the IOS device and any SIP Local Gateway or Analog Gateway hosted on that device.</p> <p>SIP Local Gateway Choose this to get commands only for the SIP Local Gateway.</p> <p>Analog Gateway Choose this to get commands only for the Analog Gateway. You do not get commands for devices that have been deleted.</p> <p>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.</p>

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.

Because the variables that are 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.

To regenerate IOS commands:

1. Log in as provider, reseller, or customer administrator.
2. Choose one of the following depending on the device for which you want to regenerate IOS commands:
 - **Apps Management > IOS > IOS Devices** for an IOS Device and any gateways it hosts.
 - **Apps Management > IOS > SIP Local Gateways** for a SIP Local Gateway.
 - **Apps Management > IOS > 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](#).

8.9.3. LBO and Analog Gateway Configuration and Generated Events

LBO and Analog Gateway Configuration and Corresponding Events

Event	Configuration
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

8.9.4. Local Break Out and Analog Gateway Events, IOS Commands, and Variables

Local Break Out and Analog Gateway Events

Default IOS Commands	Notes
HcsAddIOSDeviceEVT An IOS Device is added.	
<pre> 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 </pre>	<p>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.</p>

Default IOS Commands
HcsDeleteIOSDeviceEVT An IOS Device is deleted.
<pre> conf t no voice service VoIP no voice class codec 1 end </pre>

Default IOS Commands	Available Variables
<pre> 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 </pre>	<p>pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.</p>

Default IOS Commands	Available Variables
<pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.</p> <p>pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.</p> <p>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.</p>

Default IOS Commands	Available Variables
<p>HcsAddAnalogGatewayEndpointModEVT An Endpoint Module is added for the Analog Gateway.</p> <pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.</p> <p>pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.</p> <p>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.</p>

Default IOS Commands
<p>HcsDeleteAnalogGatewayEVT An Analog Gateway is deleted.</p> <pre> 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 </pre>

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointEVT An Analog Gateway Endpoint is deleted.	
<pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>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.</p>

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointModEVT An Analog Gateway Endpoint Module is deleted.	
<pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>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.</p>

8.9.5. MGCP Analog Gateway Events and IOS Commands

MGCP Analog Gateway Events

Default IOS Commands	Available Variables
<p>HcsAddAnalogGatewayEVT Adds an Analog MGCP Gateway.</p> <pre> conf t hostname {{pwf.GatewayDAT.domainName}} ccm-manager config server {{ fn.one macro. ↳HcsCucmsAssociatedToNDRMCR}} ccm-manager config mgcp call-agent {{ fn.one macro. ↳HcsCucmsAssociatedToNDRMCR}} 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 </pre>	<p>pwf.GatewayDAT.networkInterface returns the Network Interface based on the configuration in the Gateway.</p>

Default IOS Commands	Available Variables
<p>HcsAddAnalogGatewayEndpointEVT Adds an Endpoint for the Analog MGCP Gateway.</p> <pre> 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 </pre>	<p>pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.</p> <p>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.</p>

Default IOS Commands	Available Variables
<p>HcsAddAnalogMGCPGatewayEndpointModEVT Adds an Endpoint Module for the Analog MGCP gateway.</p> <pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.</p> <p>pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.</p> <p>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.</p>

Default IOS Commands	Available Variables
<p>HcsDeleteAnalogGatewayEVT Deletes an Analog MGCP Gateway.</p> <pre> conf t no mgcp call-agent {{ fn.one macro. ↳HcsCucmsAssociatedToNDRMCR}} 2427 service-type. ↳mgcp version 1.0 no ccm-manager config server {{ fn.one macro. ↳HcsCucmsAssociatedToNDRMCR}} 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 </pre>	<p>pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.</p>

Default IOS Commands	Available Variables
<p>HcsDeleteAnalogGatewayEndpointEVT Deletes an Endpoint for the Analog MGCP Gateway.</p> <pre> 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 </pre>	<p>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.</p>

Default IOS Commands	Available Variables
HcsDeleteAnalogMGCPGatewayEndpointModEVT Deletes an Endpoint Module for the Analog MGCP Gateway.	
<pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>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.</p>

Default IOS Commands	Available Variables
HcsUpdateAnalogGatewayEVT Updates the Analog MGCP Gateway.	
<pre> 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 </pre>	<p>pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.</p>

Default IOS Commands	Available Variables
HcsUpdateAnalogGatewayEndpointEVT Updates the Endpoint for the Analog MGCP Gateway.	
<pre> 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 </pre>	<p>pwf.PORT_NUM - This is the FXS port number of the analog gateway device.</p> <p>pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange.</p> <p>pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.</p>

8.9.6. 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:

- 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.

8.9.7. Set up an IOS Device

Perform these steps:

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. Choose **Device Management > IOS > IOS Devices**.
4. Click **Add**.
5. Provide the following information:

Field	Description
IOS Device Name	Enter the name for the IOS Device. This field is mandatory.
Description	Enter a description for the IOS Device.
Prime Collaboration	Select the Prime Collaboration to manage the IOS Device.

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

If NAT is used, also configure an APPLICATION_SPACE network address.

If a double NAT is deployed, also configure a CUSTOMER_SPACE network address.

7. Optionally, expand **Credentials**.

- 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. Provide an optional description for the credential.

SNMP credentials are used by PCA to manage the IOS Device. CLI credentials are used to log in to the IOS Device.

Note:

SNMP configuration must be done manually on the IOS Device.

8. Click **Save**.

8.9.8. Analog Gateways

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.

8.9.9. Set up an Analog Gateway

Pre-requisites

- Add an IOS device in VOSS Automate at the Customer level hierarchy. To add an IOS device, see [Set up an IOS Device](#).
- If applicable, ensure that the site-level dial plan is applied on the site where the gateway is being added.

Note: VOSS Automate supports SCCP and MGCP protocols. It does not support BRI endpoints. Do not add slots or modules or subunits for BRI.

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Choose **Apps Management > IOS > Analog Gateways**.
3. Click **Add**.
4. Choose the required hierarchy path from the drop-down and click **OK**.
5. On the **Gateway** tab, complete, at minimum, the mandatory [Gateway Fields](#).
6. On the **Gateway Units** tab, click + to expand **Modules**, and complete, at minimum, the mandatory [Gateway Units - Modules Fields](#).
7. On the **Endpoints** tab, click + to expand the SCCP or MGSP endpoints, and complete, at minimum, the mandatory:
 - [SCCP Endpoints Fields](#).
 - [MGCP Endpoints Fields](#).

Note: Gateway endpoints will be shown in the following order on the **Endpoints** tab of the form:

Slot > Subunit > Port Number, for example:

```
0-0-0
0-0-1
2-0-0
2-0-1
2-0-2
```

8. On the **Config** tab, click + to expand the **Product Specific Configuration Layout**, and complete the required [Config: Product Specific Configuration Layout Fields](#).
9. Click **Save**.

There are few scenarios that show the expected behaviour of an Analog gateway when adding, deleting, or modifying a 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.

Gateway Fields

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): <ul style="list-style-type: none"> • VG202: 2 ports • VG204: 4 ports • VG224: 24 ports • VG310: 24 ports • VG320: 48 ports • VG350: 144/160 ports • VG400: 8 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 *	Choose the call manager group from the drop-down list. For example: Default . This is a mandatory field. 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](#).

Field	Description
Gateway Network Interface *	<p>Enter a Gateway Network Interface. For example: FastEthernet0/0, FastEthernet0/1, GigabitEthernet0/0, GigabitEthernet0/1 or **GigabitEthernet0/2. This is a mandatory field.</p> <p>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.</p>
Call Disconnect Timeout *	<p>Enter the time unit for Call Disconnect Timeout. For example: 2. This is a mandatory field.</p> <p>Note: The time unit always is in seconds. Do not enter any negative timer values.</p>
CP Tone *	<p>Choose the call progress tone (country code) from the drop-down list. For example: in (for India). This is a mandatory field.</p> <p>Note: CP Tone is an FXS configuration parameter that supports each analog device in the gateway.</p>
Signal *	<p>Choose a signal from the drop-down list. For example: loop-start or ground-start. This is a mandatory field.</p> <p>Note: Signal is an FXS configuration parameter that supports each analog device in the gateway.</p>

Gateway Units - Modules Fields

Field	Description
Slot *	<p>Choose the required value from the drop-down list. For example: 0. This is a mandatory field</p> <p>Note:</p> <ul style="list-style-type: none"> • 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 *	<p>Choose the available module from the drop-down list. For example: NM-4VWIC-MBRD.</p> <p>Note:</p> <p>Only modules that are available for the slot appear in the list.</p>
Subunits *	Click + to expand Subunits. This is a mandatory field.
Subunit Position *	<p>Choose the subunit position from the drop-down list. For example: 0.</p> <p>Note:</p> <p>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.</p>
Subunit *	Choose the subunit from the drop-down list. For example: VIC3-2FXS-E/DID-SCCP.

Note: When managing Gateways Units for Analog Gateways on the on the Legacy Admin GUI, the Slot number and Subunit Position may disappear from the form, but values are captured.

SCCP Endpoints Fields

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: <i>Endpoint for slot/subunit/port n/n/n gateway @domain</i> 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.

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	<p>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.</p> <p>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.</p>
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)	<p>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.</p> <p>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.</p>
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)	

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 Subscriber 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: Subscriber 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 [Phones](#).

MGCP Endpoints Fields

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: <i>Endpoint for slot/subunit/port n/n/n gateway @domain</i> . 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.

Field	Description
Use Trusted Relay Point	Choose one of the following values: <ul style="list-style-type: none"> • 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 Party 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.

Field	Description
SMDI Port Number (0 - 4096) *	Enter the first SMDI port number of the T1 span. If you set this parameter to a non-zero 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: Subscriber 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 Fields

Field	Description
Key	Enter the Key for the product-specific configuration Layout. For example stcap-pRegCap.
Value	Enter the Key for the product-specific configuration layout. For example: 0.

8.9.10. Add Port to Analog Gateway

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.

Supported Ports

- 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) are also supported

To add a port to an analog gateway:

1. Go to (default menus) **Apps Management > IOS > Add port to Analog Gateway**.
2. Choose a site.
3. Fill out fields on the form:
 - Add a URI at **Gateway Domain**, and add a description for the analog gateway.
 - Choose owner user ID, and INI inventory filter.
 - In **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.
-

- In **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.

8.9.11. SIP Gateway Port

View, Add, or Delete a Gateway Port

This procedure displays, updates, and deletes existing gateway ports, and adds new gateway ports.

1. Go to (default menus) **Apps Management > IOS > 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:

- In **LBO Gateway Name**, choose the gateway where you will add the new port.
- In **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.
-

- In **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 (default menus) **Apps Management > IOS > Commands**. You can paste these commands into the gateway. Commands for updates and deletes can also be found in the **Commands** log.

8.9.12. IOS Gateway Manual Configuration

This procedure adds a PRI Trunk to connect to the PSTN.

VOSS 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:

- 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

```

8.10. UC Prep Management**8.10.1. Introduction to UC Prep****Overview**

The UCPrep Profile tool further streamlines the preparation process of deployment of Cisco applications with VOSS Automate Provider and Enterprise so that administrators will not have to repeat the same configuration tasks each time they stage or build a UC Application.

The 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 multiple sets of static configuration data can be set up and stored. The UCPREP Profile tool use can vary from provider to provider and even by customer within a provider.

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.

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, then the input form tab for that configuration can remain empty.

Caveats

- The push of data needs to be run at the level of the apps.
- None of the work has been done to apply required fields from the perspective of UC Apps to the data model.

UCPrep Menu Descriptions

When the feature is exposed on an administrator menu, a list of menu items are available to carry out the UCPrep tasks.

A typical workflow would be that one or more UCPrep Profiles are set up for use and then pushed to 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.

Menu Name	Description and Notes
UCPrep Profile Push	This is the menu element 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 Time-zones	List of time zones 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	The collection of configuration templates that are utilized 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.

8.10.2. UCPrep Profiles

UCPrep Profiles [Standard UC Deployment USA] Save Delete Help Back Action ▾

UCPrep Profile **CUCM Date Time Groups** **CUCM Group** **CUCM Host Adjustment** **CUCM SIP Trunk Security Profiles** **CUCM SIP Profile** **More ▾**

UC Prep Profile Name	Standard UC Deployment USA
UC Prep Profile Notes	Standard set of UC deployment for USA Country-wide. Date Time Groups: NY, Chicago, Denver, Phoenix, Los Angeles. CUCM Groups - PubOnly. CUC User Templates - Standard, Advanced.

From the **UCPrep Profiles** menu, the list view shows 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 UC Prep Profile Name must be unique. The **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 Reference

Name	Field Description
UC Prep Profile Name	The friendly name for the UCPrep Profile. This is the name populated into the push tooling above.
UC Prep Profile Notes	A field available to enter helpful information describing the UCPrep Profile. This is the field populated to the push tooling above.

8.10.3. UCPrep Profile Push

UCPrep Profile Push

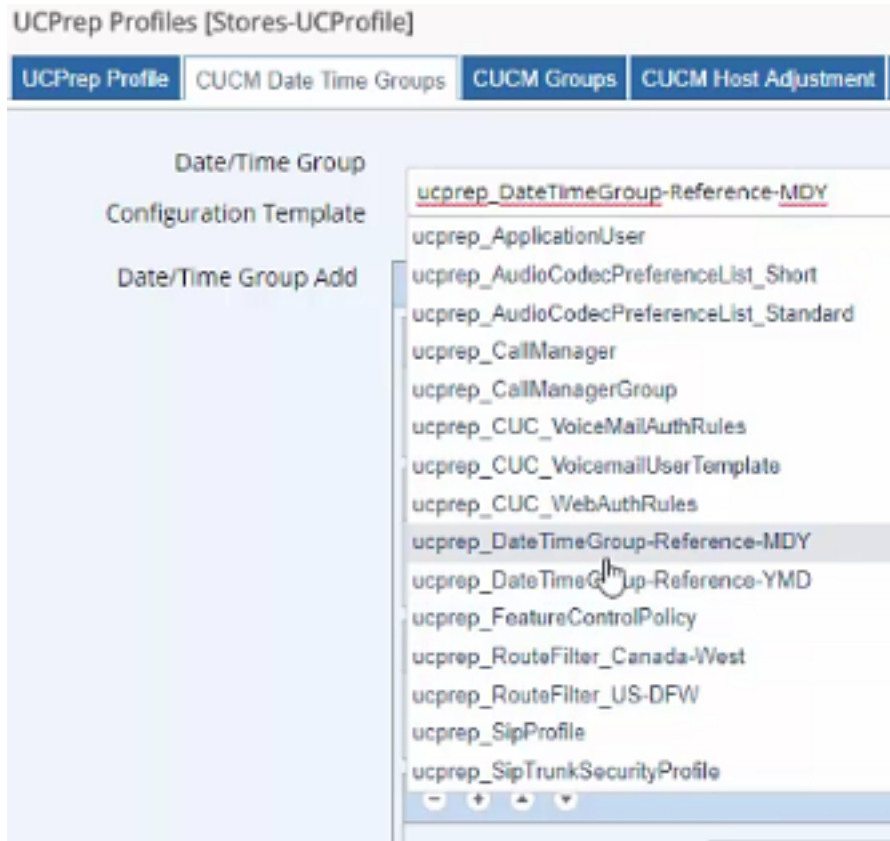
UC Prep Profile:	Standard UC Deployment USA
Profile Description	Standard set of UC deployment for USA Country-wide. Date Time Groups: NY, Chicago, Denver, Phoenix, Los Angeles. CUCM Groups - PubOnly. CUC User Templates - Standard, Advanced.
Target Call Manager	["10.5.31.21", "8443"]
Target Unity	["10.5.31.22", "443"]

UCPrep Profile Push Reference

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.

8.10.4. Date Time Groups

- 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 in the **UCPrep Configuration Templates** menu.
- The **UCPrep Friendly Timezones** menu 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.



Date Time Groups Reference

Field	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.

8.10.5. Call Manager Groups

In order for the Member drop-downs to function, a UCPrep Profile must be cloned to the level of the UC Applications.

Note that in this example, the UCPrep Profile that is built is entered at the “Axis” customer application level.

The screenshot displays the 'Standard CUCM Group' configuration page. At the top, there are navigation tabs: 'UCPrep Profile', 'CUCM Date Time Groups', 'CUCM Group' (selected), 'CUCM Host Adjustment', 'CUCM SIP Trunk Security Profiles', and 'More'. Below the tabs, there are buttons for 'Save', 'Delete', 'Help', 'Back', and 'Action'. The main content area is titled 'Standard CUCM Group' and contains two sub-panels. Each sub-panel has a 'Call Manager Group Name' field and a 'Members (In Order)' list. The first sub-panel, 'Sub1Sub2', has members 'CM_3121CUCMSub1' and 'CM_3121CUCMSub2'. The second sub-panel, 'Sub2Sub1', has members 'CM_3121CUCMSub2' and 'CM_3121CUCMSub1'.

The order in which the members are added indicate primary and secondary members of the group.

Call Manager Groups Reference

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.

8.10.6. Call Manager Host Adjustment

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.

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back

UCPrep Profile CUCM Date Time Groups CUCM Group CUCM Host Adjustment CUCM SIP Trunk Security Profiles CUCM SIP Profile CUCM Audio Codec Preferences CUCM Application Users More ▾

Call Manager Hostname

Current ID

New Host Identifier

Call Manager Universal Device Template

Call Manager Universal Line Template

Starting Directory Number

Ending Directory Number

Auto-registration Enabled on this Cisco Unified Communications Manager

Current ID

New Host Identifier

Call Manager Universal Device Template

Call Manager Universal Line Template

Starting Directory Number

Ending Directory Number

Auto-registration Enabled on this Cisco Unified Communications Manager

Call Manager Host Adjustment Reference

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.

8.10.7. Call Manager SIP Trunk Security Profiles

The input form on the tab shows the fields commonly requiring modification.

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back Action ▾

UCPrep Profile CUCM Date Time Groups CUCM Group CUCM Host Adjustment CUCM SIP Trunk Security Profiles CUCM SIP Profile More ▾

Sip Trunk Security Profile

Name

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Accept presence subscription

Accept out-of-dialog refer

Accept unsolicited notification

Accept replaces header

Incoming SIP Port

Call Manager SIP Trunk Security Profiles Reference

Name	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: <ul style="list-style-type: none"> • Non Secure • Authenticated • Encrypted
Incoming Transport Type	Drop-down providing options: <ul style="list-style-type: none"> • TLS • TCP and UDP
Outgoing Transport Type	Drop-down providing options: <ul style="list-style-type: none"> • 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.

8.10.8. Call Manager SIP Profiles

Where values or time settings are shown in the fields of the form when adding a profile, these are the static values corresponding with the Call Manager defaults.

Call Manager SIP Profiles

Name: Custom_SIP_Profile

Description: Custom SIP Profile

Use Fully Qualified Domain Name in SIP Requests:

Phone Parameters: Timer Register Expires (seconds): 3600

Phone Parameters: Timer Register Delta: 5

Phone Parameters: Timer Keep Alive Expires (seconds): 120

Phone Parameters: Timer Subscribe Delta (seconds): 5

Phone Parameters: Timer Subscribe Expires (seconds): 120

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)":

Trunk Configuration: SIP Rel1XX Options: Send PRACK for all 1xx Messages

Trunk Configuration: Calling Line Identification Presentation: Default

Trunk Configuration: Session Refresh Method:

Trunk Configuration: Enable ANAT:

Trunk Configuration: Deliver Conference Bridge Identifier:

SDP Information: Allow Presentation Sharing using BFCP:

Call Manager SIP Profiles Reference

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 <ul style="list-style-type: none"> • Disabled • Send PRACK if 1xx Contains SDP • Send PRACK for all 1xx Messages
Trunk Configuration: Calling Line Identification Presentation	Drop-down providing options <ul style="list-style-type: none"> • Default • Strict From URI presentation Only • Strict Identity Headers presentation Only
Trunk Configuration: Session Refresh Method	Drop-down providing options <ul style="list-style-type: none"> • 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

8.10.9. Call Manager Audio Codec Preferences

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back Action ▾

UCPrep Profile CUCM Date Time Groups CUCM Group CUCM Host Adjustment CUCM Audio Codec Preferences More ▾

Audio Codec Preference List +

- +

Configuration

Template to Apply

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:

UCPrep Configuration Templates [ucprep_AudioCodecPreferenceList_test] Save Delete Help Back Action ▾

Name*

Description

Foreach Elements

Schema Defaults

Target Model Type*

Merge Strategy

device/cucm/AudioCodecPreferenceList

Codec Names *

-	+	<input type="text" value="AMR-WB (7k-24k)"/>
-	+	<input type="text" value="AMR (5k-13k)"/>
-	+	<input type="text" value="MP4A-LATM 128k"/>
-	+	<input type="text" value="AAC-LD (MP4A Generic)"/>
-	+	<input type="text" value="MP4A-LATM 64k"/>
-	+	<input type="text" value="MP4A-LATM 56k"/>
-	+	<input type="text" value="L16 256k"/>
-	+	<input type="text" value="MP4A-LATM 48k"/>
-	+	<input type="text" value="G.729 8k"/>
-	+	<input type="text" value="G.729a 8k"/>
-	+	<input type="text" value="GSM Half Rate 6k"/>
-	+	<input type="text" value="G.723.1 7k"/>

Name *

Description *

Call Manager Audio Codec Preferences Reference

Name	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.

8.10.10. Call Manager Application Users

- Application Users can initially be set up from the **UCPrep Application User** menu, 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**.

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back Action ▾

UCPrep Profile | CUCM Date Time Groups | CUCM Group | CUCM Host Adjustment | CUCM SIP Trunk Security Profiles | CUCM SIP Profile | CUCM Application Users More ▾

Application Users

User ID: CustomCTIUser ▾

Password:

Repeat Password:

Controlled Devices: +

CTI Controlled Device Profiles: +

Group Permissions:

Group: Standard CTI Enabled ▾

Group: Standard CTI Secure Connection ▾

User ID: SinglewireUser ▾

Password:

Repeat Password:

Controlled Devices: +

CTI Controlled Device Profiles: +

Group Permissions:

Group: Third Party Application Users ▾

Call Manager Application Users Reference

Field Name	Description
Application Users	Mechanism for adding an unlimited number of 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.

8.10.11. Call Manager Feature Control Policies

Feature Control Policies are defined by entering policy names and selecting features from the list of check boxes.

Feature Control Policy

Policy Name: FCP-ALL

Policy Description: All Features Enabled

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

Policy Name: BargeOnly

Policy Description: Barge Only Enabled

Barge

Call Back

Call Pickup

Call Manager Feature Control Policies Reference

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	<ul style="list-style-type: none"> • 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

8.10.12. Call Manager Route Filters

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back Action ▾

UCPrep Profile CUCM Date Time Groups CUCM Group CUCM Route Filters More ▾

Route Filters +

- +

Route Filter

Template to ▾

Apply

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:

UCPrep Configuration Templates [ucprep_RouteFilter] Save Delete Help Back Action ▾

Name*

Description

Foreach Elements

Schema Defaults

Target Model Type*

Merge Strategy

device/cucm/RouteFilter

Dial Plan Name *

Name *

Member

Digits	<input type="text" value="204"/>
Operator *	<input type="text" value="=="/>
Dial Plan Tag Name *	<input type="text" value="AREA-CODE"/>
Priority *	<input type="text" value="1"/>

Digits	<input type="text" value="250"/>
Operator *	<input type="text" value="=="/>
Dial Plan Tag Name *	<input type="text" value="AREA-CODE"/>
Priority *	<input type="text" value="2"/>

Digits	<input type="text" value="289"/>
Operator *	<input type="text" value="=="/>
Dial Plan Tag Name *	<input type="text" value="AREA-CODE"/>
Priority *	<input type="text" value="3"/>

Digits	<input type="text" value="306"/>
Operator *	<input type="text" value="=="/>
Dial Plan Tag Name *	<input type="text" value="AREA-CODE"/>
Priority *	<input type="text" value="4"/>

Digits	<input type="text" value="41[68]"/>
Operator *	<input type="text" value="=="/>
Dial Plan Tag Name *	<input type="text" value="AREA-CODE"/>
Priority *	<input type="text" value="5"/>

Call Manager Route Filters Reference

Name	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.

8.10.13. Unity Authentication Policies

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back : Action ▾

UCPrep Profile CUCM Date Time Groups CUCM Group CUCM Host Adjustment CUCM SIP Trunk Security Profiles Unity Authentication Policies More ▾

Update Voice Mail Authentication Rules

Voice Authentication Rule CFT

Update Web Authentication Rules

Web Authentication Rule CFT

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:

UCPrep Configuration Templates [ucprep_CUC_VoiceMailAuthRules]

Save Delete Help Back Action ▾

Name*	ucprep_CUC_VoiceMailAuthRules
Description	CUC Voice Authentication Rule
Foreach Elements	+ <input type="text"/>
Schema Defaults	+ <input type="text"/>
Target Model Type*	device/cuc/AuthenticationRule
Merge Strategy	Additive ▾
device/cuc/AuthenticationRule	
Trivial Cred Checking	((False)) ▾
Max Hacks	0
Object Id	<input type="text"/>
Max Days	0
Min Length	3
Hack Reset Time	30
Expiry Warning Days	15
Lockout Duration	30
URI	▾
Location Object Id	{{ pwf.LocationObjectId }}
Min Duration	1440
Display Name	Recommended Voice Mail Authentication Rule
Prev Cred Count	0
Location URI	/vmrest/locations/connectionlocations/{{ pwf.LocationObjectId }} ▾

Unity Authentication Policies Reference

Field Name	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.

8.10.14. Unity User Templates

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.

UCPrep Profiles [Standard UC Deployment USA - AXIS] Save Delete Help Back Action ▾

UCPrep Profile CUCM Date Time Groups CUCM Group CUCM Host Adjustment CUCM SIP Trunk Security Profiles CUCM SIP Profile Unity User Templates More ▾

Unity User Template

Alias: Standard_Voicemail_User

Display Name: Standard Voicemail User

Based On Template: voicemailusertemplate ▾

Phone System: PhoneSystem ▾

Class Of Service: Voice Mail User COS ▾

Partition: 3122cucpub Partition ▾

Search Scope: 3122cucpub Search Space ▾

Message Aging Policy: Default System Policy ▾

CUC User Template: ucprep_CUCVoicemailUserTemplate ▾

CFT

Alias: Advanced_Voicemail_User

Display Name: Advanced Voicemail User

Based On Template: voicemailusertemplate ▾

Phone System: PhoneSystem ▾

Class Of Service: Voice Mail User COS ▾

Partition: 3122cucpub Partition ▾

Search Scope: 3122cucpub Search Space ▾

Message Aging Policy: Do Not Age Messages ▾

CUC User Template: ucprep_CUCVoicemailUserTemplate ▾

CFT

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.

9. Microsoft Apps Management

9.1. Introduction to Microsoft UC Integration

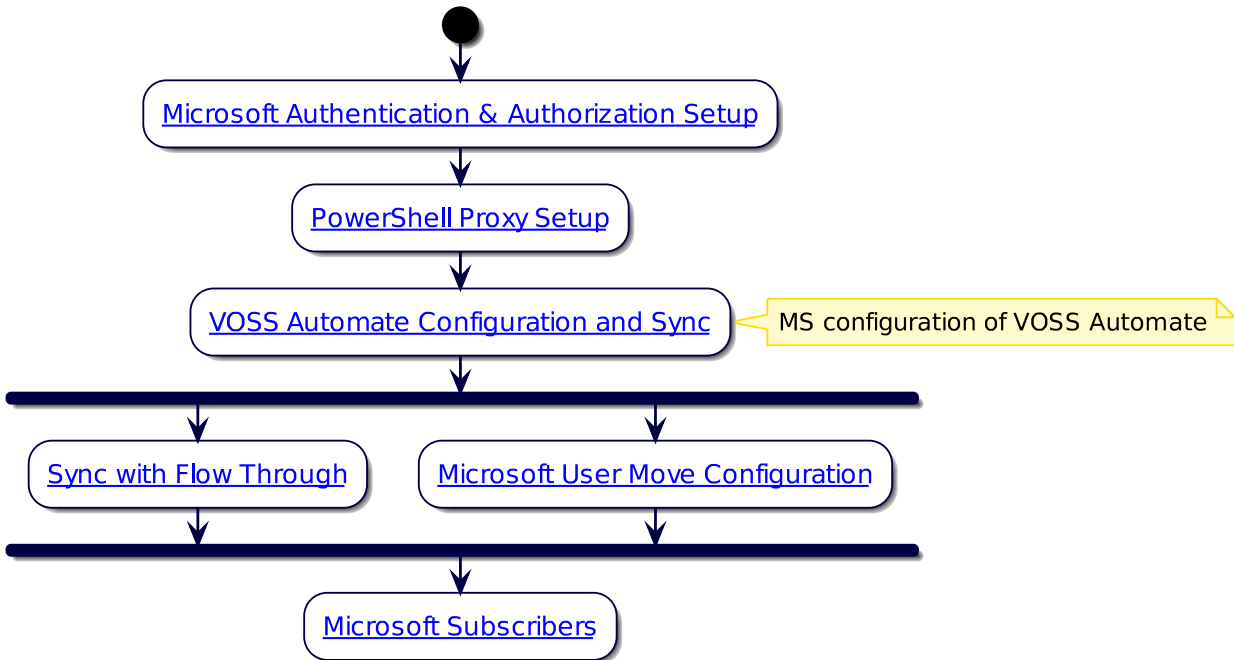
This section introduces Microsoft Unified Communications (UC) integration with VOSS Automate.

VOSS 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.

VOSS Automate can be used to manage multiple applications within Microsoft's UC stack, including:

- Azure Active Directory
- 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 VOSS Automate.

Microsoft Overview Flowchart**Related Topics**

- *Microsoft Configuration*
- *Microsoft Authentication and Authorization Setup*
- *PowerShell Proxy Setup*
- *Configure Microsoft Tenant Connection Parameters*
- *Microsoft Licenses*
- *Introduction to Microsoft Teams Dialplan Management*
- *Configure Microsoft Tenant Dialplan*
- *Introduction to Microsoft Teams Policies*
- *Overbuild for Microsoft*
- *Model Filter Criteria*
- *Flow Through Provisioning*

9.2. Microsoft Authentication and Authorization Setup

9.2.1. Overview

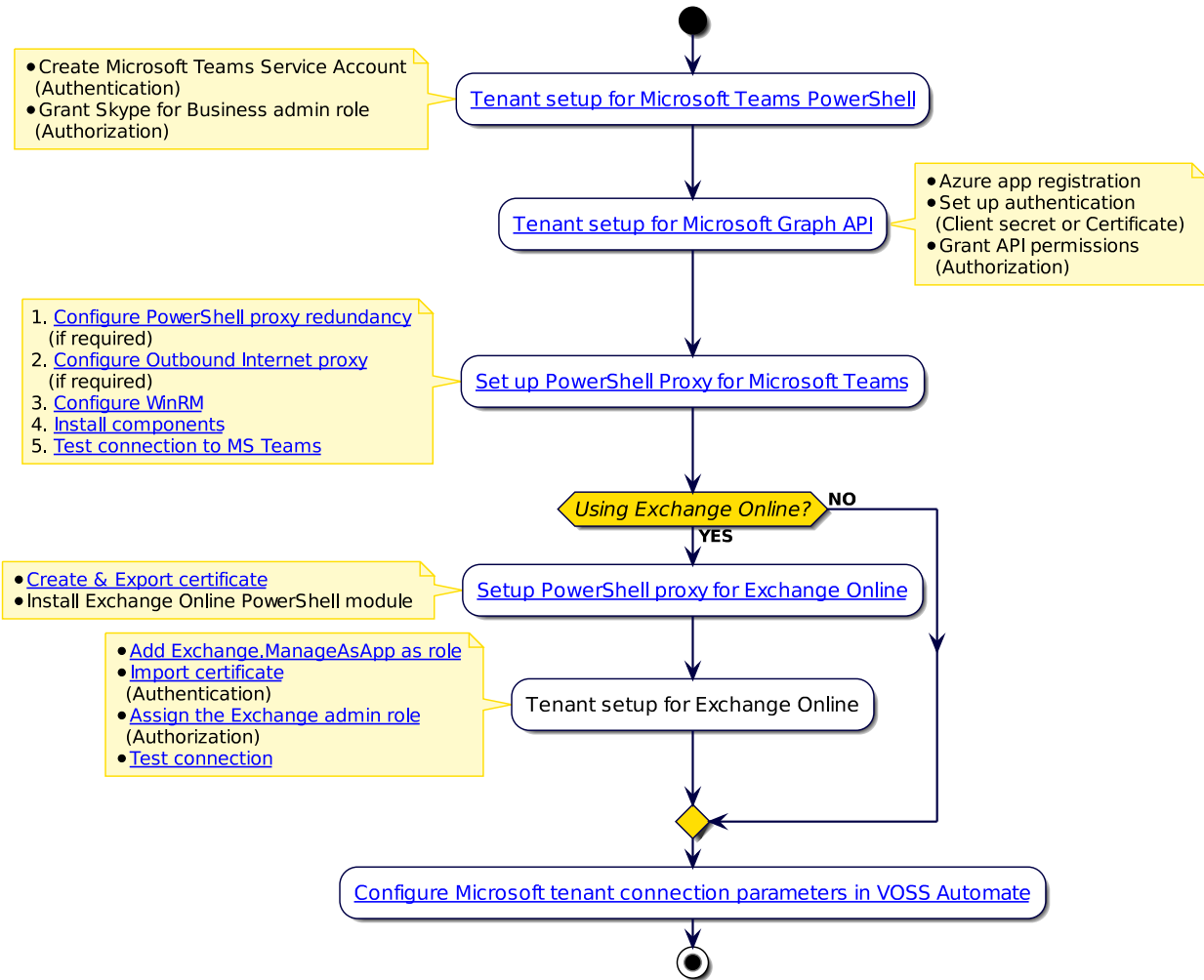
To allow VOSS Automate to manage and provision Microsoft applications, VOSS Automate must be able to authenticate with Azure Active Directory, PowerShell proxy servers (one or more) Microsoft Teams, and Microsoft Exchange Online.

Note: For details around the URLs, ports, and protocols that VOSS 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.

9.2.2. Authentication and Authorization Setup Workflow

The flowchart provides a high-level overview of the process to set up VOSS Automate authentication and authorization for managing Microsoft applications.



The table describes the devices configured for authentication and authorization:

Device	Description
Microsoft Graph API	Used for managing cloud-based apps. VOSS Automate uses Microsoft Graph API to interact with Microsoft Azure Active Directory. Registering VOSS Automate as an application object in the Azure portal provides authentication and authorization for VOSS Automate.
PowerShell Proxy Servers	VOSS Automate accesses and provisions Microsoft Teams using PowerShell. Authentication and authorization are enforced on the PowerShell proxy and in the Microsoft 365 tenant.
Microsoft Teams	VOSS Automate uses the PowerShell proxy server and the Microsoft Teams PowerShell module to manage MS Teams settings. PowerShell scripts authenticate to Microsoft Teams using Basic Authentication, and credentials associated with a service account in the tenant.
Exchange Online	VOSS Automates uses the PowerShell proxy server and Microsoft Exchange Online PowerShell module to manage MS Exchange Online components. VOSS Automate authenticates using app-only authentication, which requires a certificate and private key installed on the PowerShell proxy.

9.2.3. Microsoft Graph API

VOSS Automate uses the Microsoft Graph API (if available) to manage cloud-based applications, such as Azure Active Directory.

Note: When available, the Microsoft Graph API is the preferred choice, for the following reasons:

- Greater simplicity
- Intervening proxy is not required
- Lower latency
- More secure authentication options
- More granular permissions management

As the Microsoft Graph API matures, VOSS 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.

9.2.4. Windows PowerShell and PowerShell Proxy Servers

If the Microsoft Graph API is not available, and for on-premise applications, VOSS Automate uses Windows PowerShell, along with PowerShell management modules provided by Microsoft. In this case, VOSS Automate requires access to at least one Windows computer to use as the PowerShell proxy server.

VOSS Automate manages Microsoft Teams and Microsoft Exchange Online using the PowerShell proxy servers running Windows PowerShell. The PowerShell proxy servers 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 VOSS 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.

Authentication and authorization may be enforced in two places:

- On the PowerShell proxy
- In the Microsoft 365 tenant

When using Windows PowerShell for Microsoft apps management, VOSS Automate creates separate PowerShell sessions via the PowerShell proxy servers for each Microsoft application being managed for a specific customer tenant or domain.

All PowerShell sessions for a particular customer may be hosted by the same PowerShell proxy server, or you can configure a separate PowerShell proxy server for each PowerShell session. Optionally, the PowerShell proxy servers hosting the PowerShell sessions may be dedicated for this purpose exclusively.

WinRM and WSMAN

Windows Server includes the “Windows Remote Management” (WinRM) service, which implements the “Web Services-Management” protocol (WSMan):

- VOSS Automate connects to the WinRM service on the PowerShell proxy and provides credentials for an elevated local service account on that server
- The WinRM service executes commands from the set provided by the Microsoft Teams and Microsoft Exchange PowerShell modules.

Once connected, VOSS Automate pushes PowerShell scripts (which it generates “on the fly”) to the PowerShell proxy, and instructs WinRM to execute the scripts and return the results. The Microsoft Teams and Exchange Online Management PowerShell modules (provided by Microsoft) then connect to the Microsoft 365 tenant.

PowerShell Proxy Deployment Topologies

PowerShell Proxy Server Domain Membership

PowerShell proxy servers may be joined to an Active Directory domain.

Domain membership is required if you're using VOSS Automate to manage or extract data from any on-premises component, such as Skype for Business Server, on-premises Active Directory, or on-premises Exchange Server.

Domain membership is optional in all other scenarios.

Redundancy

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 VOSS Automate and the PowerShell proxy servers.

Load balancer requirements:

- Must forward incoming HTTP and HTTPS requests on TCP ports 5985 and 5986
- 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 VOSS 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.

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.

9.2.5. Azure Active Directory

VOSS Automate uses the Microsoft Graph API at <https://graph.microsoft.com> over TCP port 443 to interact with Azure Active Directory.

Microsoft's application registration process provides authentication and authorization services for VOSS Automate. For details, see [VOSS Automate App Registration in Azure](#)

You can configure the permissions granted to the VOSS Automate application based on the management use cases for which VOSS Automate has been designated. For example, you can grant permission to VOSS Automate to manage end user license assignments, or you can withhold that permission (in which case VOSS Automate will only be able to view existing license assignments, limiting the VOSS Automate workflows available to you).

The table describes the permissions that VOSS Automate requires:

Permission	Description
User.Read.All	Allows the app to read the full set of profile properties, group membership, reports and managers of other users in your organization. Use cases: <ul style="list-style-type: none"> • List Azure AD Users • Retrieve Azure AD user properties • Retrieve Azure AD user license details
User.ReadWrite.All	Allows the app to read and write the full set of profile properties, group membership, reports and managers of other users in your organization. Also allows the app to create and delete non-administrative users. Does not allow reset of user passwords. Use cases: <ul style="list-style-type: none"> • Update Azure AD user properties • Update Azure AD user license assignment
Organization.Read.All	Allows the app to read the organization and related resources. Related resources include things like subscribed SKUs and tenant branding information. Use cases: <ul style="list-style-type: none"> • List subscribed SKUs (subscribed, used, and available licenses) • Retrieve subscribed SKU details, including service plans included in the SKU

9.2.6. Microsoft Teams

VOSS Automate uses the PowerShell proxy and the Microsoft Teams PowerShell module to manage Microsoft Teams end user, service, device policies, and telephony settings.

The PowerShell scripts authenticate to the Microsoft Teams tenant using Basic Authentication.

Note: The Microsoft Teams PowerShell module currently only supports Basic Authentication.

The PowerShell scripts authenticate using the credentials associated with a service account in the tenant. The tenant service account must be granted sufficient privileges to perform Microsoft Teams end user, service, and device management, and it must not have multi-factor authentication enabled.

Note: To enhance the security of the connection between the PowerShell proxy server(s) and your Microsoft Teams tenant, you may wish to consider using Conditional Access to restrict management access by the service account to specific static IP addresses associated uniquely with your PowerShell proxy server(s).

For more information around Conditional Access, see [What is Conditional Access in Azure Active Directory? | Microsoft Docs](#).

You must assign at minimum the following role to the service account used for managing Microsoft Teams:

Role	Description
Skype for Business Administrator	<p>Provides full access to all Teams and Skype features, Skype user attributes, manages service requests, and monitors service health.</p> <p>Use cases:</p> <ul style="list-style-type: none"> • List Teams Users • Retrieve Teams user identity, attributes, and assigned policies • Update Teams user attributes and assigned policies • Enable / disable Enterprise Voice for Teams users • Create, read, update and delete Teams policies • Create, read, update, and delete Teams Enterprise Voice configuration, including Voice Routing Policies, PSTN Usages, Voice Routes, PSTN Gateways, and Tenant Dialplans • Create, read, update, and delete Teams Call Queues and Teams Auto Attendants • Create, read, update, and delete Teams endpoints, including Teams Phones, Common Area Phones, Collaboration Bars, and Teams Rooms

9.2.7. Exchange Online

VOSS Automate uses the PowerShell proxy server, along with Microsoft's Exchange Online PowerShell module, to manage Exchange Online user mailboxes, shared mailboxes, room mailboxes, and distribution groups.

VOSS Automate uses app-only authentication for Microsoft Exchange Online.

Note: For more information about app-only authentication, see [App-only authentication | Microsoft Docs](#).

For app-only authentication, you will need to create an X.509 certificate with a private key. The certificate and private key must be installed on the PowerShell proxy server.

When registering the VOSS Automate Application Object with Azure AD, you will upload the certificate (with only the public key) and assign Exchange Online API permissions and an appropriate RBAC role to the application.

You will then provision the certificate's thumbprint in VOSS Automate so that VOSS Automate can pass the thumbprint to the PowerShell proxy. The PowerShell proxy uses the certificate identified by the thumbprint to authenticate with Exchange Online.

Azure AD permission for managing Exchange Online

VOSS Automate requires the following Azure AD permission to manage Exchange Online:

Azure AD permission	Description
Exchange.ManageAsApp	Allows a registered application to access Exchange Online resources

RBAC role for managing Exchange Online

VOSS Automate requires the following RBAC role for managing Exchange Online:

RBAC Role	Description
Exchange Administrator	Users with this role have global permissions within Microsoft Exchange Online. Also 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 allows for all operations on all MS Exchange models; that is: Access Profile type: `device/msexchangeonline/*`

For details, see [Access Profile Permissions and Operations](#).

9.3. Create Microsoft Teams Service Account on Azure

This procedure creates the Microsoft Teams service account for VOSS Automate on Azure, and assigns the following role: *Skype for Business Administrator*.

Note: The PowerShell Proxy uses the Microsoft Teams service account to manage Microsoft Teams.

Prerequisites:

- You will need at least the “User administrator” role.

To create the MS Teams service account

- Use your User Administrator credentials to sign into the [Azure portal](#).
- Choose the tenant in which VOSS Automate will manage Microsoft Teams.

Note: If you have access to multiple tenants, select the relevant tenant via the **Directory + Subscription** filter.

- Go to **Favorites > Users**.

Note: If **Users** is not listed in your Favorites, search for it in **All services**.

4. From the toolbar, select **New user**, then select **Create user**.
5. Fill out user details:

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 VOSS Automate. See [Configure Microsoft Tenant Connection Parameters](#)

- Enter a user name in the **User name** field (e.g. "voss-svc").
- Select a domain, and enter a name (e.g. "VOSS Automate Service Account").

Note: You can choose any domain in the drop-down, including the default "*.onmicrosoft.com" domain.

- Create a password for the account.
- Under **Groups and roles**, choose the default role, **User**, which is a live link.
- In the **Directory roles** dialog, search for "Skype", then select the **Skype for Business Administrator** checkbox, and click **Select**.

6. Click **Create**.

Related Topics

- [Introduction to Microsoft UC Integration](#)
- [Microsoft Configuration](#)
- [PowerShell Proxy Setup](#)
- [Configure Microsoft Tenant Connection Parameters](#)

9.4. VOSS Automate App Registration in Azure

9.4.1. Overview

This procedure registers VOSS Automate as an application object in Azure Active Directory (AD), adds a client secret and/or a certificate (for authentication with the Microsoft identity platform), configures API permissions, creates, exports, and uploads a self-signed certificate, and adds VOSS Automate to the Exchange administrator role.

Note: The application object describes VOSS Automate to Azure AD, allowing the Azure AD service to issue authentication tokens to the VOSS Automate service.

Prerequisites

- [Create Microsoft Teams Service Account on Azure](#)

The table describes the tasks involved in this procedure:

Azure or PowerShell?	Task
Azure portal	Step 1: Register VOSS Automate application Step 2: Configure Microsoft Graph authentication method (certificate and/or client secret) Step 3: Add MS Graph API and application permissions
Azure & PowerShell (Optional)	(Optional - Exchange Online only) Step 4: Setup for managing Exchange Online Note that steps 4 through 8 are only required if you're using VOSS Automate to manage Microsoft Exchange.
Azure portal	(Optional - Exchange Online only) Step 5: Configure manifest and update API permissions
PowerShell Proxy server	(Optional - Exchange Online only) Step 6: Create, install, and export the self-signed certificate
Azure portal	(Optional - Exchange Online only) Step 7: Upload certificate and add application to Exchange administrator role
PowerShell Proxy server	(Optional - Exchange Online only) Step 8: Test the connection from PowerShell server to Microsoft Exchange

Important: When performing this task, take note of the following values, which you'll need to set up the tenant connection in VOSS Automate:

- Directory (tenant) ID (**Tenant ID** field in VOSS Automate)
- Application (client) ID (**Client ID** field in VOSS Automate)
- Client secret (**Secret** field in VOSS Automate)

You can retrieve your Tenant and Client IDs from your Azure Active Directory portal at any time. But you'll need to save your client secret in a secure location because it will be exposed only once. From a security perspective, treat these values as if they were administrative login credentials.

9.4.2. Step 1: Register Application with Azure AD

This step registers your application (VOSS Automate in this case) as an application in Azure Active Directory. This will allow Microsoft Graph to access Azure AD.

1. Use your Global Administrator credentials to sign into the [Azure portal](#) .
2. Choose the tenant in which you want to register the VOSS Automate application.

Note: If you have access to multiple tenants, use the **Directory + Subscription** filter in the toolbar to choose the relevant tenant.

3. Select Azure AD service.

Note: Locate the service via **Favorites > Azure Active Directory**, or locate it in **All services**.

4. Go to **Manage**, select **App registrations > New registration**.
5. Enter a name for your application, for example “VOSS Automate”.

Note: Your application users may see this name. You can change it later.

6. Select **Accounts in this organization only**.
You can ignore the **Redirect URI** section.
7. Click **Register**.
8. Go to *Step 2: Configure Microsoft Graph Authentication*

9.4.3. Step 2: Configure Microsoft Graph Authentication

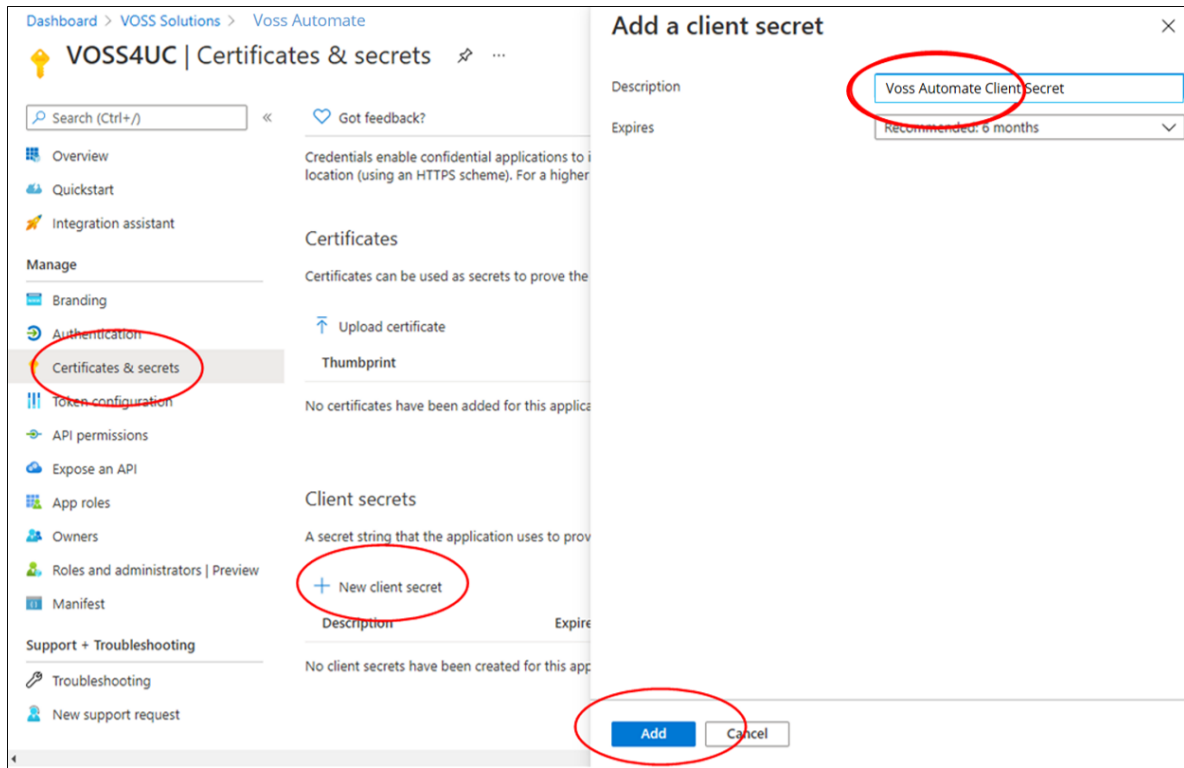
There are two authentication methods available for Microsoft Graph:

- Client secret
- Certificate

Note: You can use either of these authentication methods, or both. Microsoft’s recommendation is to use certificate authentication for Microsoft Graph. A client secret takes precedence, if used; else, the certificate authentication is used (if available).

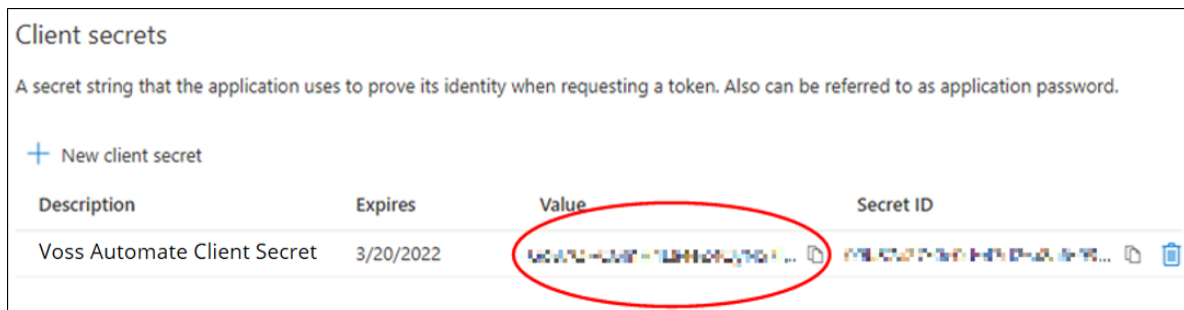
Add Client Secret Authentication

1. In Azure portal, go to **Manage > Certificates & secrets > New client secret**.
2. On the **Add a client secret** form, add a description, and choose an expiry option.
3. Click **Add**.



Important: Make a note of the client secret and keep it in a safe location. You won't be able to retrieve it if you lose it, and you need this value to set up VOSS Automate.

If you lose the client secret you'll have to delete it and repeat the steps for creating a new one.



4. Go to *Step 3: Add Microsoft Graph API Permissions*

Add Certificate Authentication

This procedure adds and exports a self-signed certificate public key in VOSS Automate, and uploads the certificate to Azure.

1. Log in to the Admin Portal as a Customer administrator or higher.
2. Go to (default menus) **Administration Tools > Certificate Management**.
3. Click **Add**; then, fill out certificate details.
 1. On the **Base** tab:

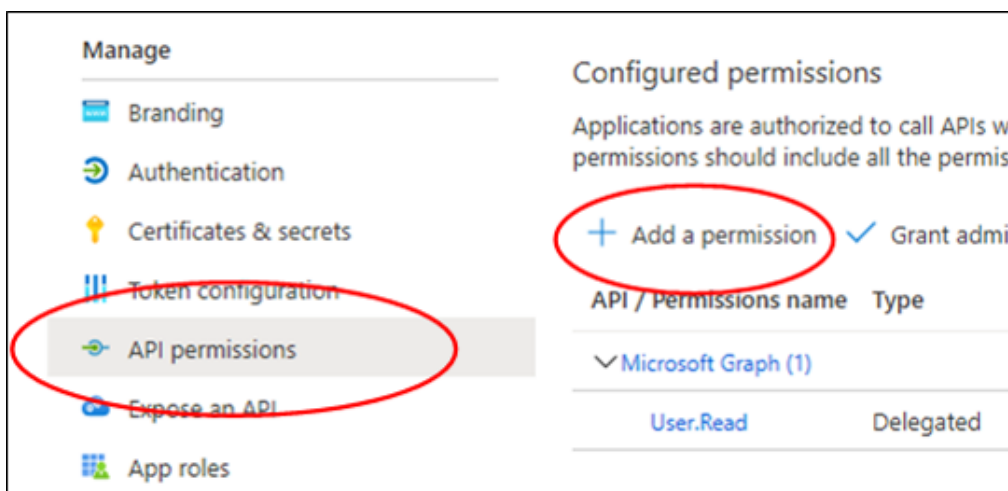
- Fill out a name and a description for the certificate.
 - Ensure the following checkbox is clear to ensure the certificate is self-signed: **Generate Certificate Signing Request**
 - In **Valid To** specify a value, in seconds, to define the validity period of the certificate from the time from generation. The default value is 315360000 seconds (10 years).
 - In **Serial Number**, choose a value or leave the default.
 - In **Key Length**, input a value of 2048 or greater for Azure to accept the certificate for authentication.
2. On the **Certificate Information** tab, fill out details for the certificate, including the name of the host being authenticated by the certificate, country code, state, city, organization, and organization unit.

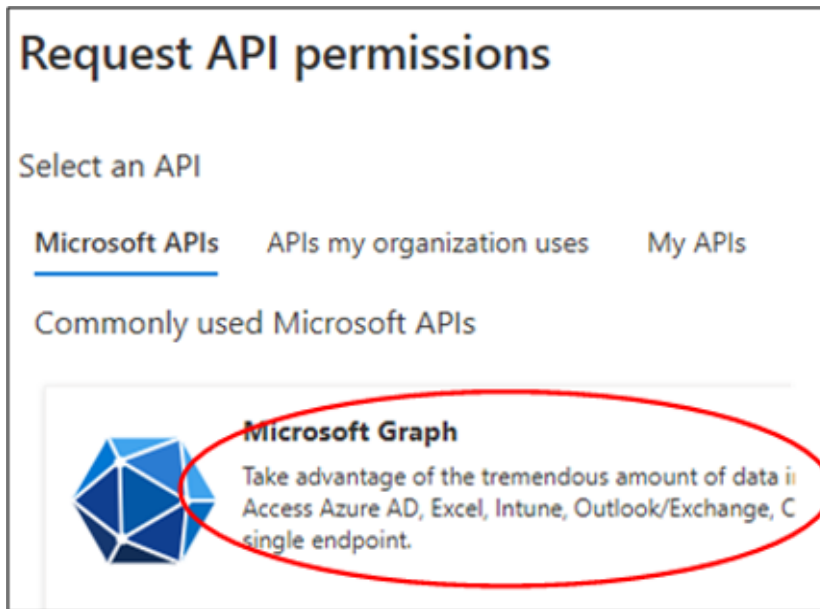
Note: All fields are mandatory.

4. Save the certificate.
5. Click **Action > Export Public Key** to export a file containing the public key.
6. Log in to the Azure portal, then go to **Certificates & secrets**.
7. On the **Certificates** tab, click **Upload certificate**, then browse to the certificate you exported from the VOSS Automate Admin Portal.
8. Copy the certificate thumbprint. You will need the certificate thumbprint (along with the tenant ID and client ID from Azure) to configure the Microsoft tenant connection parameters.
9. Go to [Step 3: Add Microsoft Graph API Permissions](#)

9.4.4. Step 3: Add Microsoft Graph API Permissions

1. In Azure portal, go to **Manage > API permissions > Add a permission**.



2. Select **Microsoft Graph**.3. Select **Application permissions**.

4. Choose relevant permissions.

The table describes Azure Active Directory, Minimum Required Permissions. Choose only the permissions required to enable VOSS Automate management:

Management use case	Required permission
List Azure AD users	User.Read.All
Retrieve Azure AD user properties	User.Read.All
Retrieve Azure AD user license details	User.Read.All
Update Azure AD user properties	User.ReadWrite.All
Update Azure AD user license assignment	User.ReadWrite.All
List subscribed SKUs (subscribed, used, and available licenses)	Organization.Read.All
Retrieve subscribed SKU details, including service plans included in the SKU	Organization.Read.All

5. Click **Add permissions**.

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Start typing a permission to filter these results

Permission	Admin consent required
> AccessReview	
> AdministrativeUnit	
> AgreementAcceptance	
> Agreement	
> APIConnectors	

Add permissions Discard

6. Go to **Configured permissions > Grant admin consent for <your tenant>**.

7. Click **Yes** to confirm.

The status of each of the listed permissions changes from **Not granted** to **Granted**.

Refresh
Got feedback?

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in VOSS Solutions? This will update any existing admin consent records this application already has to match what is listed below.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission
✓ Grant admin consent for VOSS Solutions

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for VOSS S...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for VOSS S...

8. Go to *Step 4: (Optional - Exchange Online only) Setup for Managing Exchange Online*

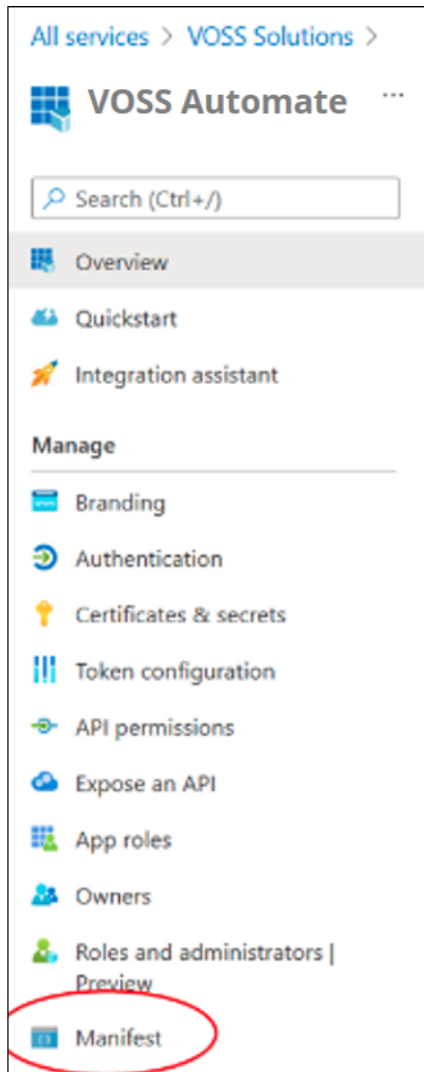
9.4.5. Step 4: (Optional - Exchange Online only) Setup for Managing Exchange Online

Note: Steps 4 (this step) through 8 (Test the connection) are only required if you're using VOSS Automate to manage Microsoft Exchange.

- Complete steps 1 - 3:
 - *Step 1: Register Application with Azure AD*
 - *Step 2: Configure Microsoft Graph Authentication*
 - *Step 3: Add Microsoft Graph API Permissions*
- *Create Microsoft Teams Service Account on Azure*
- *PowerShell Proxy Setup*
- Go to *Step 5: (Optional - Exchange Online only) Configure Manifest and Update API Permissions*

9.4.6. Step 5: (Optional - Exchange Online only) Configure Manifest and Update API Permissions

1. In the Azure portal, go to **All services > Azure Active Directory**.
2. Go to **Manage > App registrations**.
3. On the **Owned applications** tab, choose your application.
4. Go to **Manage > Manifest** to open the **Manifest** page.



5. On the **Manifest** page, scroll down until you locate the line containing the following text:
requiredResourceAccess.
6. Place your cursor at the beginning of the next line, then paste the following text at that location:

```
{
  "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
  "resourceAccess": [
    {
      "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
      "type": "Role"
    }
  ]
},
```

The image shows the change after you paste the text:

```
49 "publisherDomain": "VossSolutions0365.onmicrosoft.com",
50 "replyUrlsWithType": [],
51 "requiredResourceAccess": [
52   {
53     "resourceAppId": "00000003-0000-0000-c000-000000000000",
54     "resourceAccess": [
55       {
56         "id": "e1fe6dd8-ba31-4d61-89e7-88639da4683d",
57         "type": "Scope"
58       },
59       {
60         "id": "df021288-bdef-4463-88db-98f22de89214",
61         "type": "Role"
62       },
63       {
64         "id": "7ab1d382-f21e-4acd-a863-ba3e13f7da61",
65         "type": "Role"
66       }
67     ]
68   },
69 ],
70 "samlMetadataUrl": null,
71 "signInUrl": null,
```

```
49 "publisherDomain": "VossSolutions0365.onmicrosoft.com",
50 "replyUrlsWithType": [],
51 "requiredResourceAccess": [
52   {
53     "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
54     "resourceAccess": [
55       {
56         "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
57         "type": "Role"
58       }
59     ]
60   },
61   {
62     "resourceAppId": "00000003-0000-0000-c000-000000000000",
63     "resourceAccess": [
64       {
65         "id": "e1fe6dd8-ba31-4d61-89e7-88639da4683d",
66         "type": "Scope"
67       },
68       {
69         "id": "df021288-bdef-4463-88db-98f22de89214",
70         "type": "Role"
71       },
72       {
73         "id": "7ab1d382-f21e-4acd-a863-ba3e13f7da61",
74         "type": "Role"
75       }
76     ]
77   }
78 ],
```

7. Click **Save**.

8. Verify and update API permissions:

- Go to **Manage > API permissions**.
- Verify the following:
 - Check that the Microsoft Graph permissions you configured are still present.
 - Check that **Exchange.ManageAsApp** now appears.
- Note that the status of **Exchange.ManageAsApp** is **Not granted for...**

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
 - API permissions**
 - Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions show include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for VOSS Solutions

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (3)				
Directory.Read.All	Application	Read directory data	Yes	Granted for VOSS Soluti...
User.Read	Delegated	Sign in and read user profile	No	Granted for VOSS Soluti...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for VOSS Soluti...
▼ Office 365 Exchange Online (1)				
Exchange.ManageAsApp	Application	Manage Exchange As Application	Yes	Not granted for VOSS S...

- Select **Grant admin consent for <your tenant>**, and click **Yes**.
- Confirm that the status of **Exchange.ManageAsApp** has changed to **Granted for . . .**

▼ Office 365 Exchange Online (1)				
Exchange.ManageAsApp	Application	Manage Exchange As Application	Yes	Granted for VOSS Soluti...

9. Go to *Step 6: (Optional - Exchange Online only) Create, install, and export the self-signed certificate*

9.4.7. Step 6: (Optional - Exchange Online only) Create, install, and export the self-signed certificate

On the PowerShell Proxy, you will need to create and install a self-signed certificate with a private key, and then export the certificate without its private key.

1. Sign into the PowerShell Proxy ensuring that you use the service account you created for VOSS Automate (e.g. WSMAN-svc). (This ensures the certificate is created and stored in the right account.)
2. Open an elevated PowerShell window.
3. Use the following PowerShell commands:

To create the certificate and install in the current user store:

```
$mycert = New-SelfSignedCertificate -DnsName 'your public domain' -
↪ CertStoreLocation 'cert:\CurrentUser\My' -NotAfter (Get-Date).AddYears(1) -
↪ KeySpec KeyExchange
```

Note: In place of 'your public domain', update the text with your 'public domain'

Example:

```
$mycert = New-SelfSignedCertificate -DnsName 'voss-solutions.com' -
↪ CertStoreLocation 'cert:\CurrentUser\My' -NotAfter (Get-Date).AddYears(1) -
↪ KeySpec KeyExchange
```

(continues on next page)

(continued from previous page)

To export the certificate to a .cer file:

```
$mycert | Export-Certificate -FilePath "$($env:USERPROFILE)\mycert.cer"
```

To extract the certificate thumbprint:

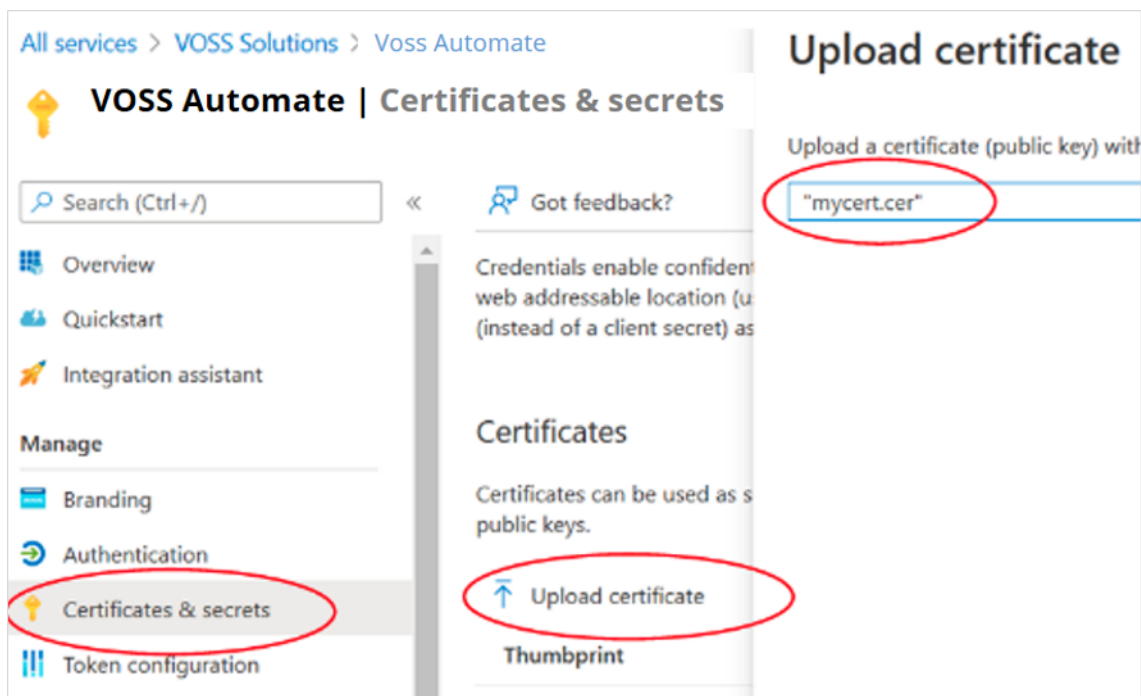
```
$mycert.Thumbprint
```

Note: The PowerShell command to extract the certificate thumbprint displays the certificate thumbprint. You will need this value when setting up the connection parameters in VOSS Automate, so copy it, and save it for later.

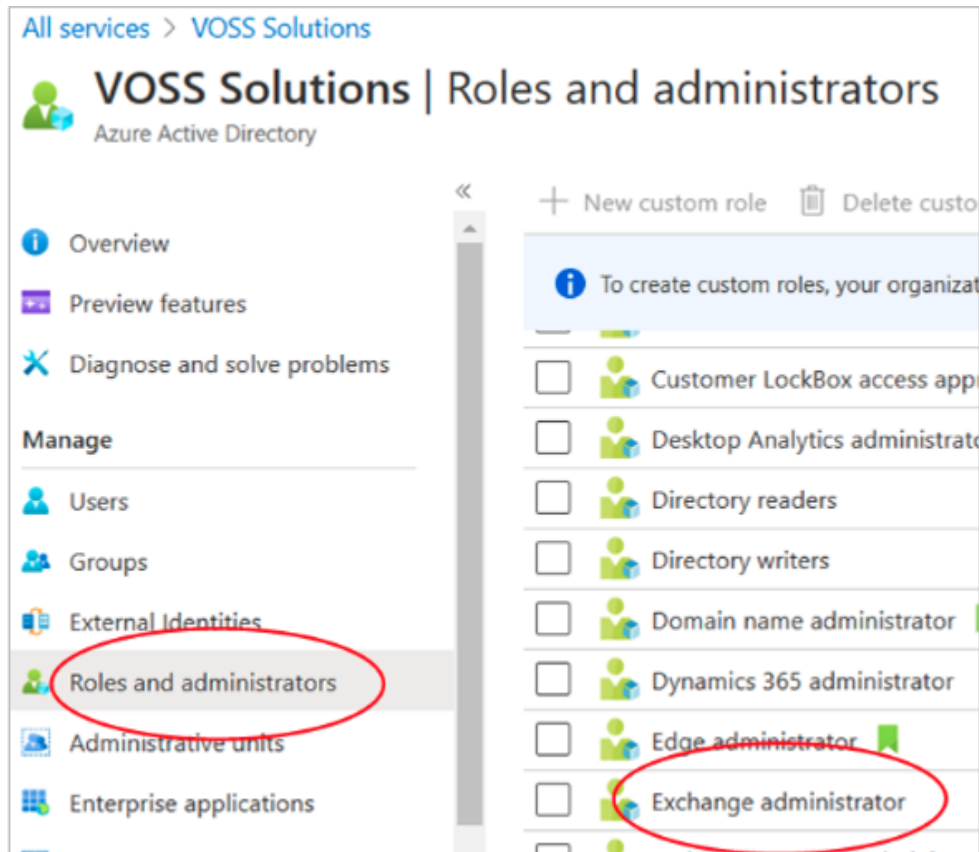
9.4.8. Step 7: (Optional - Exchange Online only) Upload certificate and add application to Exchange administrator role

This procedure uploads the certificate you exported previously, to Azure, and adds the VOSS Automate application to the Exchange administrator role.

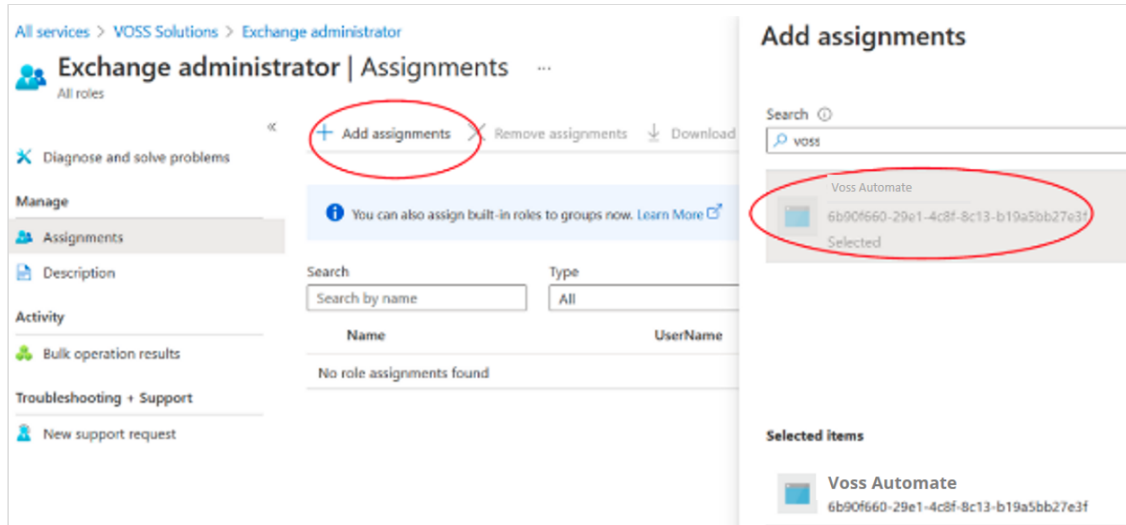
1. In Azure portal, ensure the the .cer file you created is accessible, then go to **Azure Active Directory > Manage**.
2. Select **Certificates & secrets > Certificates**.
3. Select **Upload certificate**.
4. On the **Upload certificate** page, navigate to your exported certificate.



5. Click **Add**.
6. Add your application (e.g. VOSS Automate) to the Exchange administrator role:
 - Go to **All services > Azure Active Directory** to open the **Overview** page.
 - Under **Manage**, select **Roles and administrators**.
 - From the list of roles, click on the **Exchange administrator** role name.



- On the **Assignments** page, select **Add assignments**.
- On the **Add assignments** page, locate and select your application.



- Click **Add**.

9.4.9. Step 8: (Optional - Exchange Online only) Test the connection from PowerShell server 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 VossSolutions0365.onmicrosoft.com
```

2. Use the following command, then confirm that you can see a user mailbox:

```
Get-EXOMailbox -ResultSize 1
```

9.5. PowerShell Proxy Setup

This procedure configures the PowerShell proxy servers and installs the Microsoft Teams PowerShell module.

Note:

- You must have local Administrator privileges on the PowerShell Proxy server to perform these steps.

You will need to perform the following tasks:

1. *Configure PowerShell Proxy for Redundancy*
2. *Configure the Outbound Internet Proxy*
3. *Configure WinRM*
4. *Install Software Management Components*
5. *Test the Tenant Connection*

9.5.1. Configure PowerShell Proxy for Redundancy

Important: This task is **only** required if you're deploying multiple PowerShell Proxy servers behind a load balancer. If you do not have any concerns around redundancy, you can skip this task.

This procedure adds a Fully Qualified Domain Name (FQDN) to the local hosts file on each PowerShell Proxy server you're deploying. Each PowerShell Proxy server must be able to address itself with the FQDN corresponding to the load balancer's virtual IP address.

Perform these steps:

1. On each of the PowerShell Proxy servers, open an elevated PowerShell window, and issue the following command:

```
PS C:\WINDOWS\system32> notepad C:\Windows\System32\drivers\etc\hosts
```

2. In the Notepad window uncomment the 127.0.0.1 line (delete the hash) and append the FQDN of the load balancer virtual IP:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
# localhost name resolution is handled within DNS itself.
127.0.0.1 localhost psproxy.domain.com
# ::1 localhost
```

9.5.2. Configure the Outbound Internet Proxy

This procedure configures a PowerShell Proxy server to use an outbound Internet proxy.

Important: This step is **only** required if your deployment is using an outbound Internet proxy to access the public Internet (including Microsoft tenants).

Prerequisites:

- If the outbound Internet proxy requires authentication, you will need to obtain those credentials and configure them in VOSS Automate (as described in the Core Feature Guide). The credentials are not configured directly on the PowerShell Proxy server.

Perform these steps:

1. Sign into the PowerShell Proxy server using the local service account that VOSS Automate will use to connect to the proxy.

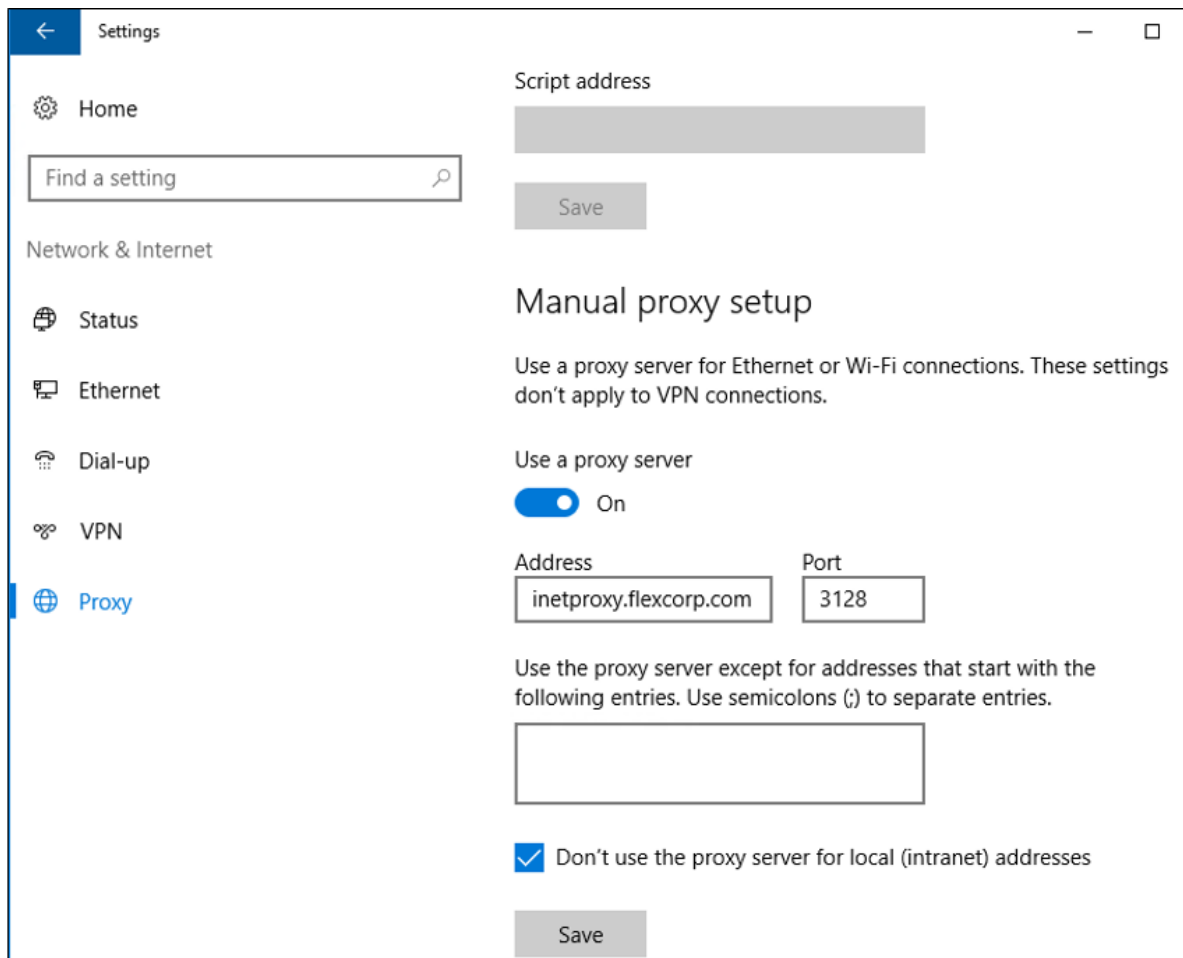
Note: VOSS Automate must use a server-local service account for accessing the PowerShell Proxy server. It must not be a domain account (should the server be domain-joined). The service account must have the following properties:

Account Type	Local Computer Account (not a domain account)
Local Group Membership	<ul style="list-style-type: none"> • Administrators • Remote Management Users

2. Open Windows Settings and go to **Network & Internet > Proxy**.
3. Under **Manual proxy setup** enable **Use a proxy server**.
4. In the **Address** field, fill out the IP address or FQDN of the outbound Internet proxy server.
5. In the **Port** field, fill out the port number required by the proxy.

Note: The port is typically 3128, but your organization may require a different port.

6. Select **Don't use the proxy server for local (intranet) addresses**.



7. Click **Save**.

Note: This is a per-user configuration, so ensure you sign in using the VOSS Automate service account.

8. To make this configuration the default setting for all HTTP clients, open an elevated PowerShell session, and issue the following command:

```
netsh winhttp import proxy source=ie
```

9.5.3. Configure WinRM

This procedure configures the Windows Remote Management (WinRM) service with the appropriate settings for VOSS Automate.

VOSS Automate uses the Web Services-Management protocol (WSMan) to create the PowerShell sessions that manage Microsoft UC applications.

On Windows computers, the Windows Remote Management (WinRM) service implements WSMan.

You will need to configure WinRM on a PowerShell Proxy running on Windows Server 2019.

Note: Any firewalls between VOSS Automate and the PowerShell Proxy, including Windows Firewall on the proxy, must permit the connections listed in the following table, which describes WinRM Firewall Settings.

These firewall exceptions are enabled by default in Windows Server 2019.

Service	Protocol	Port
WinRM 2.0 (HTTP)	TCP	5985
WinRM 2.0 (HTTPS)	TCP	5986

Perform these steps:

1. Open an elevated PowerShell session.
2. Issue the following commands:

```
Enable-WSManCredSSP -Role Server -Force
Enable-WSManCredSSP -Role Client -DelegateComputer \* -Force
Set-Item WSMan:\localhost\Service\AllowUnencrypted $true
Set-Item WSMan:\localhost\Service\Auth\Basic $true
Set-Item WSMan:\localhost\Client\AllowUnencrypted $true
Set-Item WSMan:\localhost\Client\Auth\Basic $true
Set-Item WSMan:\localhost\Client\TrustedHosts '{server identity}'
```

Note: When setting the **TrustedHosts** value, you'll need to provide the identity of the server on which you're executing these commands:

- If this is a standalone PowerShell Proxy (not behind a load balancer), provide the server's IP address and FQDN, with a comma between them.
- If this PowerShell Proxy is behind a load balancer, append the FQDN of the load balancer's virtual interface.

For example, assume the server's FQDN is `psproxy01.domain.com` and its IP address is `10.1.1.10`. If the server is not behind a load balancer, the value for **TrustedHosts** (including the quotes) will be:

```
'10.1.1.10,psproxy01.domain.com'
```

If the server is behind a load balancer, and the FQDN of the load balancer's virtual interface is `psproxy.domain.com`, then provide the following value for **TrustedHosts**, including the quotes:

```
'10.1.1.10,psproxy01.domain.com,psproxy.domain.com'
```

9.5.4. Install Software Management Components

This procedure installs the following software components on a new PowerShell Proxy server:

- *Step 1: Install .NET Framework 4.8*
- *Step 2: Install Microsoft Teams PowerShell Module*
- *Step 3: Install Microsoft ExchangeOnlineManagement Module*

Before you start

The `Install-Module` command used in *Step 2: Install Microsoft Teams PowerShell Module* and *Step 3: Install Microsoft ExchangeOnlineManagement Module* downloads the specified PowerShell module from the PowerShell Gallery (an online repository).

Since the PowerShell Gallery has deprecated the use of TLS versions earlier than TLS 1.2, you will need to force Windows PowerShell to use TLS 1.2, which will allow the `Install-Module` command to work correctly. TLS 1.2 is the default in Windows Server 2019 and later. If you're using an earlier release of Windows Server, use the following command to force PowerShell to use TLS 1.2:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

The command is relevant only for the current PowerShell session (its effect persists only until you close the PowerShell window and end the session). Errors such as the following when using the `Install-Module` command are likely the result of a TLS version mismatch: "Unable to resolve package source", "No match was found..."

Step 1: Install .NET Framework 4.8

1. Browse to <https://dotnet.microsoft.com>.
2. Navigate to the download for .NET Framework 4.8 Runtime, or do an Internet search for ".NET Framework 4.8 download".

Note: Ensure you only download from a URL ending in "microsoft.com". The authenticity of software downloaded from third-party websites cannot be guaranteed.

3. Download and run the .NET Framework 4.8 Runtime installer.

Note: Once the installation completes, you may need to reboot the server.

Step 2: Install Microsoft Teams PowerShell Module

To upgrade any PowerShell proxies that have already been deployed, perform these steps:

Starting with VOSS Automate version 21.3-PB1, the required MS Teams PowerShell module v4.3.0. If you're upgrading existing PowerShell proxy servers, perform the following steps (on each PowerShell proxy server) to use the supported version of the MS Teams module (v4.3.0).

1. Exit any existing PowerShell and PowerShell ISE windows.
2. From an elevated (run as Administrator) PowerShell window:

```
Stop-Service WinRM
Uninstall-Module MicrosoftTeams
Install-Module MicrosoftTeams -RequiredVersion 4.3.0 -AllowClobber
Start-Service WinRM
```

3. Verify

```
Get-Module -ListAvailable -Name MicrosoftTeams
```

The output should show version 4.3.0

```
$cred = Get-Credential
```

Enter MS Teams tenant admin credentials in the pop-up.

```
Connect-MicrosoftTeams -Credential $cred
Get-CsOnlineUser -ResultSize 1
```

The output should display the details for one random user.

To install MS Teams PowerShell module on a new PowerShell proxy, perform this step:

1. From an elevated PowerShell session issue the following command:

```
Install-Module MicrosoftTeams -RequiredVersion 4.3.0
```

Step 3: Install Microsoft ExchangeOnlineManagement Module

1. From an elevated PowerShell session issue the following command:

```
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 2.0.5
```

Note: Check with VOSS in case a newer version of the ExchangeOnlineManagement module is recommended.

9.5.5. Test the Tenant Connection

This procedure tests the connection to Microsoft Teams from a non-privileged PowerShell session.

Perform these steps:

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. Issue the following command to test the connection to Microsoft Teams and to perform a test query:

```
Connect-MicrosoftTeams -Credential (Get-Credential)
Get-CsOnlineUser -ResultSize 1 | Select DisplayName
```

When prompted, enter your Teams service account credentials.

Note: Perform step 1 first if your PowerShell Proxy is behind an outbound Internet proxy that requires authentication.

3. Verify that you have successfully connected to the tenant and retrieved one random user.

9.6. Configure Microsoft Tenant Connection Parameters

This procedure configures the following connections:

- From VOSS Automate to the PowerShell Proxy
- Between the PowerShell Proxy and the tenant
- The Graph API connection between VOSS Automate and the tenant

Prerequisites:

You will need:

- The FQDN or IP address of a single-node PowerShell Proxy, or the FQDN corresponding to your load balancer's virtual IP address. See [PowerShell Proxy Setup](#)
- The credentials for the local service account you created on the PowerShell Proxy
- Proxy authentication credentials (if the outbound Internet Proxy requires authentication)

- The credentials for the Microsoft Teams tenant service account. See [Create Microsoft Teams Service Account on Azure](#).
- The Client ID, Tenant ID, and, for authentication for MS Graph, the client secret and/or the certificate created when registering VOSS Automate as an application object with Azure Active Directory. See [VOSS Automate App Registration in Azure](#).
- If you're using VOSS Automate to manage Microsoft Exchange online, you will need the certificate authentication thumbprint you generated on the Azure portal for Microsoft Exchange. See [VOSS Automate App Registration in Azure](#).

To add and configure the Microsoft Tenant

1. Log in to the VOSS Automate 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. Add the Microsoft tenant:

1. Go to (default menus) **Apps Management > Microsoft Tenant**.
2. Click **Add**.
3. Choose the hierarchy level where you wish to add the tenant. Typically, this is at Customer level.
4. Enter a name and a description for the tenant.

The screenshot shows a web interface for adding a Microsoft tenant. At the top, there is a breadcrumb navigation: a home icon followed by "/ Microsoft Tenant / Vosslab". To the right of the breadcrumb are two icons: a floppy disk (save) and a trash can. Below the breadcrumb is a form titled "Tenant". The form contains two input fields. The first field is labeled "Name *" and contains the text "Vosslab". The second field is labeled "Description" and contains the text "vosslab.net Tenant".

3. Add the PowerShell Proxy connection parameters:

1. Locate the **Microsoft Teams Powershell** section.
2. In the **Host** field, enter the FQDN or IP address of a single-node PowerShell Proxy, or the FQDN corresponding to your load balancer's virtual IP address.

Note: For details around the local hosts file and the TrustedHosts WinRM configuration, see [PowerShell Proxy Setup](#).

3. In the **Username** field and **Password** field, enter the credentials for the local service account you created on the PowerShell Proxy.

Microsoft Teams Powershell

Host *	10.5.25.246
Username *	WSMan-svc
Password * <input type="checkbox"/> Show

4. Configure the outbound internet Proxy:

1. Locate the **Microsoft Teams HTTP Proxy** fields.
2. If you have an outbound Internet Proxy deployed between the PowerShell Proxy and the public Internet, select the **Use HTTP Proxy** checkbox.

Note: If there is no outbound Internet Proxy deployed between the PowerShell and the public internet, leave both checkboxes unchecked, and leave the **Username** and **Password** fields blank. Continue to the next step.

3. If the outbound Internet proxy requires authentication, select the **Use HTTP Proxy Authentication** checkbox, and enter the Proxy authentication credentials in the **Username** / **Password** fields.

Note: 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 [PowerShell Proxy Setup](#), and note the caveat regarding proxy authentication in [PowerShell Proxy Deployment Topologies](#).

Microsoft Teams HTTP Proxy

Use HTTP Proxy	<input checked="" type="checkbox"/>
Use HTTP Proxy Authentication	<input type="checkbox"/>
Username	_____
Password	_____ <input type="checkbox"/> Show

5. Add the Microsoft Teams Tenant service account credentials:

1. Locate the **Microsoft Teams** fields.
2. In the **Admin Username** and **Admin Password** fields, enter the credentials for the Microsoft Teams tenant service account.

Note: You created this account earlier. See [Create Microsoft Teams Service Account on Azure](#).

6. Configure the Azure Active Directory application registration parameters:

1. Locate the client secret value you stored previously.

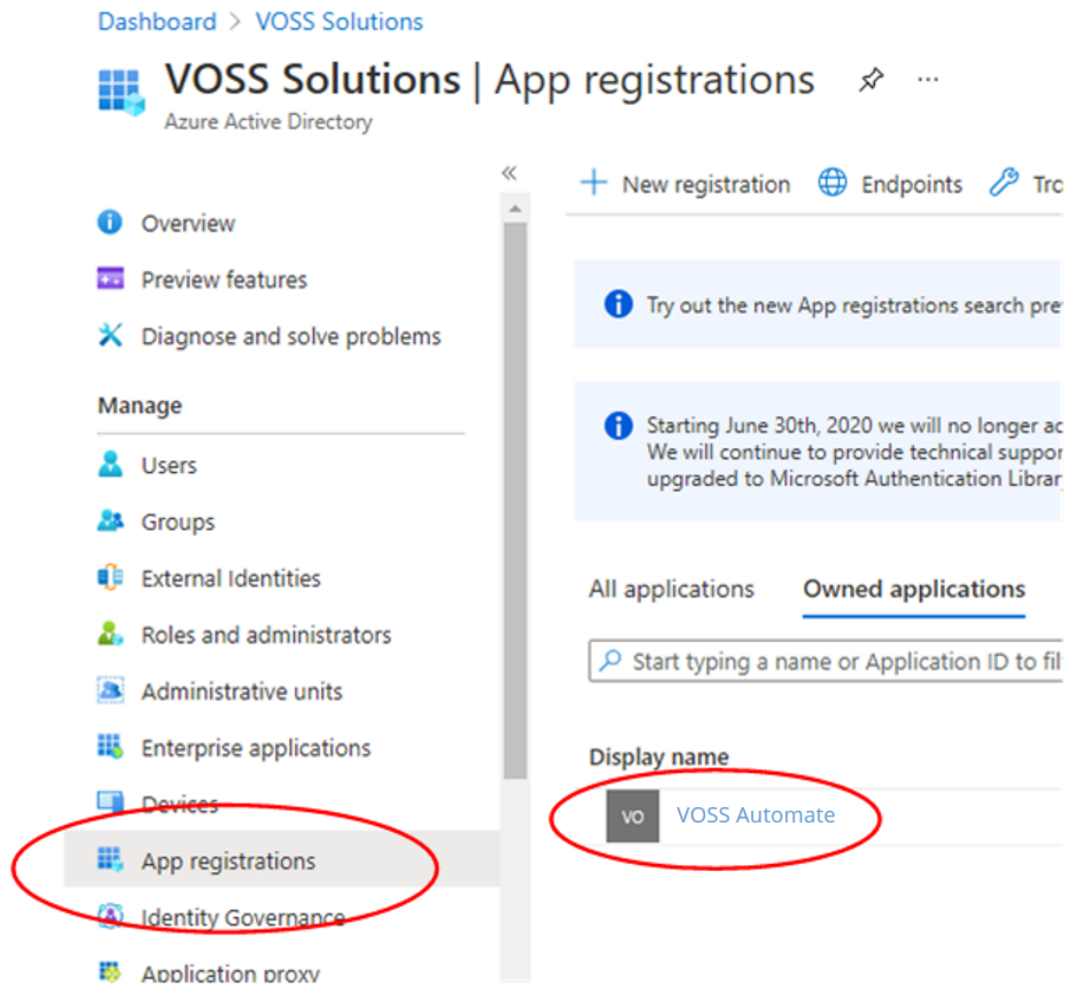
Note: You would have obtained and stored this client secret when registering your VOSS

Automate application. See [VOSS Automate App Registration in Azure](#).

2. Locate your Client ID and Tenant ID, which you specified in the Azure AD portal.

If you need to obtain the Client ID and Tenant ID from the Azure Portal now:

- Use your Global Administrator credentials to sign in to the [Azure portal](#).
- Go to **Azure Active Directory > Manage > App registrations**.
- Select your VOSS Automate application.



- Locate the **Client ID** and **Tenant ID** values under **Essentials**.

^ Essentials

Display name
VOSS Automate

Application (client) ID
a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6q7r8s9t0 ← **Client ID**

Object ID
12345678-9012-3456-7890-123456789012

Directory (tenant) ID
98765432-1098-7654-3210-987654321098 ← **Tenant ID**

Supported account types
My organization only

7. Add Microsoft 365 details to the Microsoft tenant:

1. Locate the **Microsoft 365** fields.
2. Enter the **Client ID** and **Tenant ID** values.
3. If you're using client secret authentication, copy the secret value into the **Secret** field.

Microsoft 365

Client ID *

Tenant ID *

Secret * Show

4. If you're using certificate authentication:

- Paste the certificate thumbprint obtained from Azure into the **Certificate Thumbprint** field.
- From the **Certificate** drop-down, choose the certificate previously created in the Admin Portal.

Note:

- You uploaded the public key for this locally stored certificate to Azure. The thumbprint added in the Microsoft 365 tenant parameter is generated in Azure when the public key file is uploaded to Azure.
- Certificate authentication only if a client secret is not provided.

8. If you're using VOSS Automate to manage Microsoft Exchange online, provision the Exchange Online application certificate thumbprint.

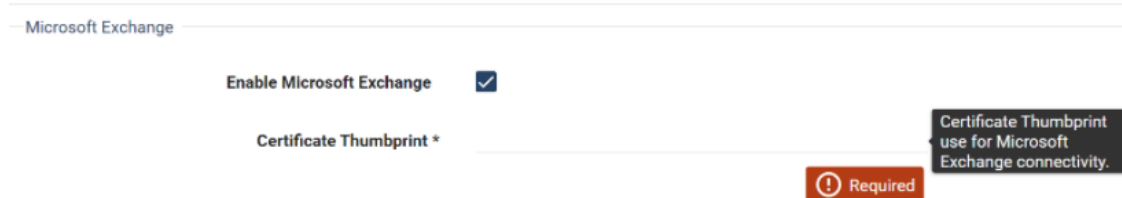
Note: The certificate authentication thumbprint is generated on the **Azure** portal for Microsoft Exchange. You would have installed this certificate on the PowerShell proxy server and configured it in the application registration.

The certificate thumbprint is the encrypted password required for an authenticated connection to the Microsoft Cloud Exchange portal. Connecting to Microsoft Exchange is required to sync in the Microsoft Exchange objects (mailboxes, shared mailboxes, rooms, and distribution lists).

1. Locate the **Microsoft Exchange** fields.
2. Select **Enable Microsoft Exchange**.
3. In the **Certificate Thumbprint** field, paste the certificate thumbprint you obtained earlier.

Note: You obtained the certificate thumbprint when logged into the PowerShell proxy to register the VOSS Automate application with Azure Active Directory. See [VOSS Automate App Registration in Azure](#).

The certificate thumbprint was created on the proxy and uploaded to the Azure portal. When generating PowerShell scripts to manage Microsoft Exchange Online, VOSS Automate includes this thumbprint so that the PowerShell proxy can use the corresponding certificate to authenticate with Microsoft Exchange Online.



Microsoft Exchange

Enable Microsoft Exchange

Certificate Thumbprint *

Required

Certificate Thumbprint use for Microsoft Exchange connectivity.

9. Click **Save**.
10. Test your Microsoft tenant connection. You will be prompted to confirm the test.

Note: In this step you will verify that VOSS Automate can connect to the Microsoft Teams tenant using PowerShell, and to Azure Active Directory using the Microsoft Graph API.

1. On the **Microsoft Tenant** page, choose the relevant tenant.
2. Click **Test Connection**.

Next Steps

- Verify that no changes are needed in user name mapping macros prior to sync. High level administrators with access to the data/MultivendorUsernameMappingMacros model instances should carry out this task.
- Perform a sync from the Microsoft tenant to import Microsoft users, tenant dial plan, licenses, and policies to the customer level. You will be prompted to confirm the syncs.
For Microsoft Exchange, ensure that instances for all 4 device models (User mailboxes, Shared Mailboxes, Room Mailboxes, and Distribution Mailboxes) are synced in at the level were the tenant exists.
- 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. See [Add a Network Device List \(NDL\)](#).
- Create sites.
- Run the overbuild. See: [Overbuild for Microsoft](#).
- Go to [VOSS Automate Configuration and Sync](#)

Related Topics

- [Microsoft Overview in the Core Feature Guide](#)

10. LDAP Management

10.1. LDAP Integration

10.1.1. Overview

The table describes two scenarios for LDAP integration in VOSS Automate:

LDAP sync and authentication	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• Users are added locally or are synced in from CUCM.• LDAP authenticates these users.• Not available for OpenLDAP.• Requires VOSS Automate version 10.6(3) or later.

Note:

- VOSS Automate provides LDAP server support for case-insensitive search base DN's. For example, on an LDAP server, the following search base DN's are equal:
 - CN=Users,DC=example,DC=com
 - cn=Users,dc=example,dc=com
-

10.1.2. LDAP Authentication

LDAP authentication works as follows:

1. User provides their credentials in the VOSS 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	<p>Matching username and password</p> <ul style="list-style-type: none"> • VOSS Automate username and password must match the username and password in the LDAP server (based on the LDAP field chosen for <i>username</i>). • Once authenticated, the LDAP username is mapped to VOSS Automate user to determine access, role, and so on.
Alternative authentication setup	<p>Non-matching username and password</p> <p>VOSS Automate supports authentication for mapping non-matching usernames. This is useful where the username in VOSS Automate and the UC apps is different to the username in LDAP. For example, if the LDAP username is bobsmith but the username in VOSS 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 VOSS 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.)</p>

Note: For LDAP authentication, the password rules of the VOSS 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 VOSS Automate.

10.1.3. LDAP Sync Scenarios (Top-Down and Bottom-Up)

VOSS Automate supports two LDAP user sync scenarios: Top-Down or Bottom-Up:

Note: While it is possible to 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 <i>directly</i> 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). It also provides the best scenario for the flow-through provisioning functionality.
Bottom-Up	Users are synced <i>indirectly</i> 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.

10.1.4. LDAP Sync Lists

The table describes, for LDAP sync, LDAP sync lists, arranged in override order:

1. <i>Always synced list</i>	Fields required to list LDAP Users on the GUI
2. <i>Drop Field List</i>	Fields never imported from LDAP
3. <i>Data Sync Blacklist</i>	A change in these fields does not trigger an update
4. <i>Model Type List</i>	From the LDAP data sync. Set up and used in scheduled syncs
5. <i>LDAP Sync List (manual or from CFT)</i>	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',
  'whenCreated',
  'uSNCreated',
  'badPasswordTime',
  'pwdLastSet',
  'lastLogon',
  'whenChanged',
  'badPwdCount',
  'accountExpires',
  'uSNChanged',
  'lastLogoff',
  'dSCorePropagationData'
]

```

Data Sync Blacklist

See Data Sync Blacklist in the Advanced Configuration Guide.

An LDAP Sync List won't override any of the Data Sync Blacklist attributes (default or custom) in data/Settings. That is, for fields that appear in both the LDAP Sync List and in the Data Sync Blacklist, 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 Model Type List](#)
- [Controlling a Data Sync with a Model Type List](#)

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.
- 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.

10.1.5. 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:

Ldap Sync List Microsoft Active Directory	Ldap Sync List Open Ldap
Model Type: device/ldap/user	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.

10.1.6. 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.

VOSS 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 DN's 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

10.2. LDAP Server

10.2.1. Add a LDAP Server

This procedure adds and configures a LDAP server for integration with VOSS Automate.

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 VOSS Automate.
3. Go to (default menus) **LDAP Management > LDAP Server**.
4. Click **Add**.
5. Fill out the fields on the **Base** tab.
6. Optionally, on the **Sync List** tab, 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](#)

7. Click **Save**.

8. 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.

10.2.2. LDAP Server Page Field Reference

This page contains the following tabs:

- Base tab
- Sync List tab

Base Tab

Fields	Description
Description	Defaults to the current hierarchy level.
Host Name *	Hostname or IP address of the LDAP server. This field is required.
Port	Port number for LDAP traffic. Defaults to 389.
User DN *	The User Distinguished Name of an administrative user who has access rights to the Base DN on the LDAP server. This field is required. Examples: <ul style="list-style-type: none"> Administrator@stb.com OU=LDAP0,DC=stb,DC=com
Admin Password *	Admin password associated with the user. This field is required.
Search Base DN *	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 or OU. As an example, to search within an Organizational Unit called CUS01 under a domain called GCLAB.COM, the Search Base DN would be OU=CUS01,DC=GCLAB,DC=COM. This field is required. 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 *	Choose between 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, VOSS Automate user management allows for the management of users on the LDAP server (add, modify, delete).

Fields	Description
CUCM LDAP Directory Name	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. This is an optional parameter but the following should be considered: For top down sync scenario, Users will be added to CUCM as Local Users if this parameter is not set. For bottom up sync scenario, Users will not be able to log on to VOSS Automate if this parameter is not set.
Encryption Method	Choose between No Encryption , Use SSL Encryption (ldaps://) , or Use StartTLS Extension . <ul style="list-style-type: none"> • 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 Cleared, 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	Select this check box 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.
Authentication Scope	Hierarchical scope this server applies to: Local authentication or Full tree authentication. ¹
User sync type	Type of users that can authenticate against this server: All users or Synced users only <ul style="list-style-type: none"> • 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	Indicate whether the server is available for authentication. Default value is True.

¹ For details around authentication scope, see [User Login Options by Authentication Method and Server Authentication Scope](#).

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**

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).

Note: A sync list improves performance, and limits sync attributes to those relevant to your scenario.

Important: A note on this tab warns that 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:

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). VOSS Automate provides default Sync List CFTs for the following: <ul style="list-style-type: none"> • Microsoft AD servers • Open LDAP 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 .

10.3. LDAP User Sync

10.3.1. Overview

You will need to set up an LDAP user sync to sync in users from a specified LDAP directory into VOSS 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 (via the User Management menu in VOSS Automate). For example, you may want to move users to other hierarchies, or to push users to CUCM.

During an LDAP sync:

- Some fields are always imported to VOSS Automate
- Some fields are not imported into VOSS Automate

For details, see [LDAP Integration](#)

10.3.2. Delete or Retain Associated Accounts at User Sync

You can configure (via **Customizations > Global Settings**) the LDAP user sync to delete or retain Cisco (CUCM) subscriber voicemail and Webex accounts when running syncs after deleting the 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](#)

10.3.3. Add an LDAP Sync

This procedure adds a LDAP sync to prepare for synchronizing users in from LDAP to VOSS Automate.

Warning: When configuring the LDAP sync, take care when setting the following options to **Automatic**, as this will delete all users from this LDAP server, in VOSS Automate as well as in the UC application users, phones, services, and so on:

- **User Purge Mode**
- **User Delete Mode**

Perform these steps:

1. Log in as Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node of the LDAP server you want to synchronize users from.
3. Go to (default menus) **LDAP Management > LDAP User Sync**.
4. Click **Add**.
5. Fill out details for the sync:

Field	Description
LDAP Server	Mandatory. The LDAP server you're syncing from.
LDAP Authentication Only	<p>This setting is available only in VOSS Automate, and is disabled by default.</p> <p>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.</p> <p>Select this checkbox (enable) to prevent user sync from the predefined LDAP directory. In this case:</p> <ul style="list-style-type: none"> • 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	<p>Defines the LDAP object (from the configured LDAP server), and is used to import and authenticate users.</p> <ul style="list-style-type: none"> • 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. <p>Contact the LDAP server administrator if you need to identify a non-default User Model Type to use.</p>
LDAP Authentication Attribute	The attribute used for creating an LDAP user. This value is used for LDAP authentication against LDAP when the LDAP Authentication Only is enabled.

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). This field is mandatory.
User Move Mode	Defines whether users are automatically moved to sites based on the filters and filter order defined in User Management > Manage Filters .
User Delete Mode	Defines whether users are automatically deleted from VOSS 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.
User Purge Mode	Defines whether users are automatically deleted from VOSS 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.

6. Inspect the default mappings and modify if required, see [User Field Mapping](#).

7. Click **Save**.

An LDAP sync is added, and is inactive by default. 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)

Related Topics

- Global Settings in the Core Feature Guide

10.4. LDAP Schedule

10.4.1. Overview

You can sync users in to VOSS Automate from LDAP by activating a scheduled sync, or by running a manual sync.

10.4.2. Activate a LDAP Scheduled Sync

This procedure activates a LDAP sync from a schedule.

Prerequisites

- LDAP server must be present

Perform these steps:

1. Go to (default menus) **LDAP Management > 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 VOSS 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, at (default menus) **User Management > Users**.

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 Integration](#).

10.5. Set up LDAP for Authentication Only

This procedure sets up LDAP for authentication-only, in VOSS Automate.

Note: Users can be added locally or synced from Cisco Unified CM (CUCM):

LDAP authenticated, by default	<ul style="list-style-type: none"> • Users that are LDAP synced in CUCM and then synced into VOSS Automate
By default, not LDAP authenticated	<ul style="list-style-type: none"> • Users that are manually configured in CUCM and then synced into VOSS Automate • Users who are manually configured in VOSS Automate

You can change the default behavior, as described in [View and Update LDAP Authentication Users](#).

LDAP for Authentication Only is available at hierarchy nodes that have an LDAP server; thus, it is not available for users created at the site level. When enabled, you must fill out the **CUCM LDAP Directory Name** for the LDAP server. If two or more LDAP server syncs have been created and you don't provide this detail, no LDAP users are created, and the transaction log displays a warning message.

To set up LDAP for authentication-only:

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where you have set up the LDAP server you want to use to authenticate users.
3. Choose **LDAP Management > LDAP User Sync**.
4. Click **Add**.
5. Fill out the relevant details:

Field	Description
LDAP Server	Choose the LDAP Server where you are authenticating users.
LDAP Authentication Only	<p>Disabled by default. When disabled, users are synced from the configured LDAP directory and their passwords are authenticated against the configured LDAP directory. When enabled, the LDAP server is used only to authenticate users.</p> <p>When selected:</p> <ul style="list-style-type: none"> • The CUCM LDAP Directory Name for the LDAP server must be filled in. When more than one LDAP server sync is created and this is not filled in, no LDAP users will be created and a warning message will be seen in the transaction log. • Users are not synced from the configured LDAP directory, but their passwords are authenticated against the LDAP directory. • You can manually add users from the GUI or API, bulk load them, or sync them from Unified CM.
User Model Type	Read-only. Identifies the LDAP object (defined in the configured LDAP server), used to authenticate users.
LDAP Authentication Attribute	<p>Choose the LDAP Attribute to be used to authenticate users. This field is mandatory. Options are:</p> <ul style="list-style-type: none"> • sAMAccountName - AD only, this is the default for AD. • uid - OpenLDAP only, this is the default for OpenLDAP. • mail • employeeNumber • telephoneNumber • userPrincipalName - AD or hybrid (with MS) <p>These are the same values Unified CM users for LDAP Attribute for User ID.</p> <p>AD (Active Directory) only: For the following types of users, do not select userPrincipalName, unless the userPrincipalName value was set as the Username when the user was created:</p> <ul style="list-style-type: none"> • 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 <p>For users synced from LDAP into Unified CM and then into VOSS Automate: Caveats (AD and OpenLDAP) For users synced from LDAP into Unified CM and then into VOSS Automate:</p> <ul style="list-style-type: none"> • 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. <p>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:</p> <ul style="list-style-type: none"> • 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

6. Click **Save**.

All users that have `SyncToHierarchy` set to the hierarchy of the LDAP server now use the LDAP server for authentication. The users are added to the LDAP Authentication Users list.

10.6. View and Update LDAP Authentication Users

All users that use LDAP for authentication are displayed on the **Users** form (default menu **User Management > Users**). This list 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.

Perform the following steps:

1. Log in as provider, reseller, or customer administrator.
2. Choose **User Management > Users**.
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.
6. To update LDAP authentication for a user, select the user, make the updates and click **Save**. You can update only the LDAP Username field. However, LDAP authentication fails if the corresponding change is not also done on LDAP.

10.7. LDAP Custom Role Mappings

10.7.1. 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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.

10.7.2. Add a LDAP Custom Role Mapping

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 (default menus) **LDAP Management > 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**.

10.8. Re-provision Synced LDAP Users

This procedure re-provisions users that were synchronized from an LDAP server, in particular, those users that have been updated on the LDAP server and for which these updates have not been propagated through VOSS Automate.

In particular, the re-sync will force an update of the selected users on all UC apps by executing an update Data Sync as well as its associated workflow.

Perform these steps:

1. Log in as a customer administrator or higher and select **User Management > Sync & Purge > LDAP Re-Provision Users**.
2. Choose the LDAP Server on which the users need to be re-synced.
3. From the LDAP Users control, add one or more users to re-sync.
4. Click **Save** to start the re-sync action.

10.9. CUCM LDAP Directory Sync

This procedure runs an on-demand CUCM LDAP directory sync to add new CUCM users into a Cisco Unified Communications Manager (CallManager/CUCM), from VOSS Automate.

Note: This sync uses VOSS Automate's generic driver to perform a doLdapSync AXL request.

For details around regular scheduled syncs, see [LDAP User Sync](#).

To perform a CUCM LDAP directory sync:

1. Log in to the Admin Portal as a Provider administrator or higher.
2. Go to (default menus) **LDAP Management > CUCM LDAP Directory Sync**.
3. From the **CUCM** drop-down, choose a CUCM 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 CUCM users into the CUCM LDAP directory.

11. Entitlement

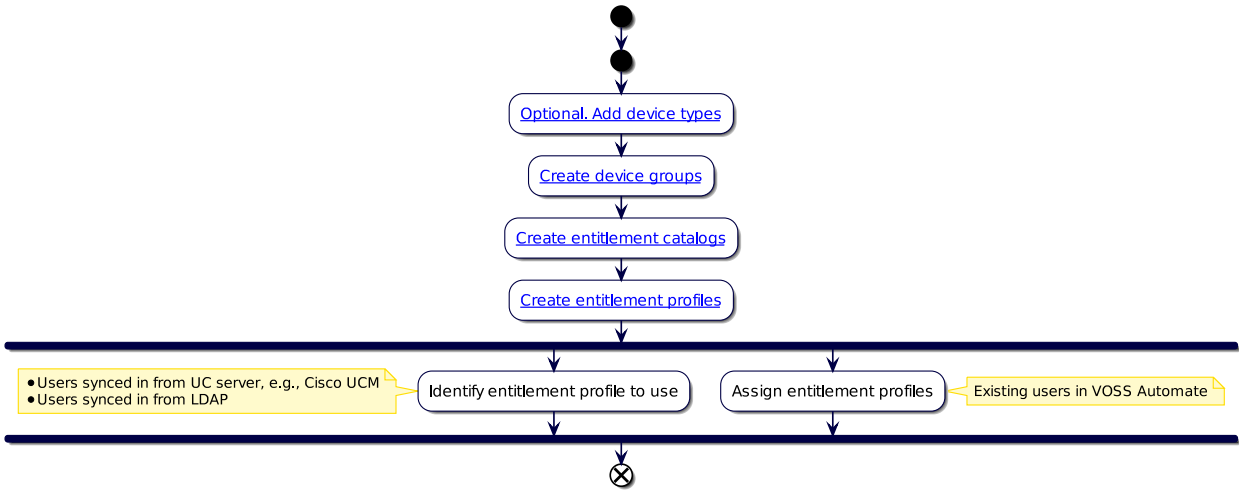
11.1. Introduction to Entitlement

Entitlement in VOSS 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 or subscriber, you can choose whether to assign an entitlement profile.

11.1.1. Setting up Entitlement

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: <ul style="list-style-type: none">• Voice service only• Maximum of two devices:<ul style="list-style-type: none">– 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: <ul style="list-style-type: none">• Voice service• Voicemail service• Maximum of ten devices (limited to SIP sets)

11.1.2. Entitlement Components

The table describes entitlement components. These are the the VOSS Automate models and the rules that define how entitlement works in the system:

Model	Description
Device types	<p>One or more physical devices, which may be grouped into device groups for entitlement purposes.</p> <p>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.</p> <p>Provider admins can add, update, or remove device types.</p>
Device groups	<p>A group of device types. The same device types may exist across different device groups</p> <p>Provider admins can add, update, or remove device groups.</p> <p>Reseller and customer admins can only view device groups.</p>
Entitlement catalogs	<p>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.</p> <p>Provider admins can add, update, and delete entitlement catalogs at their hierarchy level and below.</p> <p>Reseller and customer admins can only view entitlement catalogs.</p>
Entitlement profiles	<p>Defines a set of services, device groups, and device limits to which an end user may be subscribed.</p> <ul style="list-style-type: none"> • 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. <p>Provider admins can add, update, and delete entitlement profiles at their hierarchy level and below.</p> <p>Reseller and customer admins can only view entitlement profiles.</p>
Entitlement defaults	<p>Default entitlement profiles can be set up and assigned in VOSS Automate, but in some cases, the default is based on settings outside of VOSS Automate, depending on how users are added to VOSS Automate. See Default Entitlement Profiles</p>

11.1.3. Default Entitlement Profile

Entitlement defaults work differently depending on how a user is added to VOSS 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 Subscriber	This assigns the entitlement profile selected on the portal/loader by the administrator who adds the subscriber. When using QAS 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/Subscriber Management Add. 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** check box 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** check box selected (set to true), in the User's hierarchy tree, then the User will inherit this Entitlement Profile.
- If the **Default Profile** check box 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.

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

11.2. Entitlement Enforcement

11.2.1. Device Groups

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 Subscriber Management fails if the added Phone is not in a device group assigned to the entitlement profile applied to the user.

11.2.2. 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 Subscriber Management fails if the total number of devices limit or the total number of devices in a device group limit is exceeded.

11.2.3. Transaction Log

The transaction log messages contain detailed information that can be used to determine what entitlement profile limitation caused an action to fail.

11.2.4. 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.

Service disabled	Result
	When this check box is selected, this entitlement
Default Profile	profile will be the default entitlement profile displayed in the Quick Add Subscriber Entitlement Profile drop-down.
Voice	Adding a phone to a user in Subscriber Management fails. For an existing user with a phone with this profile (where voice is disabled), the update of the user from "Subscriber Management" fails, unless the existing phones for the user are dissociated.
Voicemail	Adding Voicemail to a user in Subscriber Management fails. For an existing user with Voicemail, updates in Subscriber 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 Subscriber Management fails. For an existing user with Cisco Unified Communications Manager IM and Presence Service enabled, updates in Subscriber Management fail after an entitlement profile with Presence disabled is applied to the user.
Extension Mobility	Adding Extension Mobility to a user in Subscriber Management fails. For an existing user with Extension Mobility, updates in Subscriber 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 Subscriber 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 subscriber fails if this field is enabled. For an existing subscriber 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 subscriber if this field is disabled. If Contact Center is enabled for an existing subscriber, and an entitlement profile with Contact Center disabled is applied, the update operation fails.

11.3. Add a Device Type

VOSS Automate is prepopulated with a list of current product types. However, the provider administrator may add additional device types as needed.

To add a new device type:

1. Log in as provider administrator.
2. Choose **Entitlement > Device Types** (default).
3. Click **Add**.
4. Enter the new device type.
5. Click **Save**.

The new device type is added to the list of available device types that can be assigned to a device group.

11.4. Create Device Group

Device groups are used in entitlement catalogs and entitlement profiles to limit entitlement to a defined subset of available device types.

To create a device group:

1. Log in as provider administrator.
2. Choose **Entitlement > 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.

11.5. Create an Entitlement Catalog

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.

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 (default menus) **Entitlement > 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.

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: [Create an Entitlement Profile](#)).

11.6. Create an Entitlement Profile

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 VOSS Automate from LDAP.
- Syncing users into VOSS Automate from a UC server, such as Cisco Unified Communications Manager (CUCM).

- Adding or updating a user VOSS Automate, using Subscriber Management or User Management.

Prerequisites:

- Add an entitlement catalog at or above the hierarchy node where you're adding the entitlement profile. See [Create an Entitlement Catalog](#)

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.

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 (default menus) **Entitlement > Profiles**.
4. Click **Add** to open the **Profiles** screen.
5. Fill out field values. Ensure you provide all 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 be 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: <ul style="list-style-type: none"> • 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.

Related Topics

- [Contact Center](#)

12. User Management

Important: When upgrading from 19.X or earlier, please refer to the *VOSS-4-UC 21.1 Release Changes and Impact* document for details on model and workflow changes. Customizations related to these changes may be affected.

When upgrading from 19.X or earlier, please refer to the *VOSS-4-UC 21.1 Release Changes and Impact* PDF on the Documentation Portal.

12.1. Users

12.1.1. Introduction to User Management

Overview

VOSS Automate supports two types of users:

Administrators	<ul style="list-style-type: none">• These users access the system to perform admin tasks• Can be assigned to any hierarchy: Provider, Customer, or Site
End users	<ul style="list-style-type: none">• These users are set up with services in the system• Can be created at any level of the hierarchy, but can only become subscribers (and be assigned services) at the Site level.

Important: When upgrading from 19.X or earlier, please refer to the *VOSS-4-UC 21.1 Release Changes and Impact* PDF document on the Documentation Portal for details on model and workflow changes in 21.1 / 21.2. Customizations related to these changes may be affected.

How Users are Added to the System

Users may be added to VOSS Automate from these sources:

- Synched in from LDAP, and promoted to a user (including flow through provisioning)
- Synched from CUCM (Cisco Unified Communications Manager)
- Synched from Azure (Microsoft users)
- Bulk loaded, via a Bulk loader template
- Manually created

Note: Conflicts between users synched from different sources are handled according to the strategy described in [Managing 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 synchronized 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 CUCM that appears in the network device list (NDL) assigned to that site. When a Cisco user is added to CUCM, it becomes a subscriber, and can be provisioned with various collaboration services.

For details around how Microsoft users are synched in from Azure and then moved to the sites as subscribers, see [Microsoft Subscribers](#)

User Authentication

Authentication (auth) methods define how a user is authenticated when logging in to VOSS 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 VOSS Automate to provide single sign-on (SSO) support for users created or synched at that hierarchy node.

Note: Typically, Microsoft users will not need to log in to VOSS Automate. Their default auth method is Automatic. When the default auth method is set to LDAP, VOSS Automate checks with the LDAP server to verify the user's credentials. Once verified, the user is logged in to VOSS Automate.

Related Topics

- [User Authentication Methods](#)
- [View Users](#)
- [Add an Admin User](#)
- [Update a User](#)
- [User Management Scenarios](#)
- [User Sync Source](#)
- [User Field Mapping](#)

- *Localization Language*

12.1.2. Users and Subscribers

Overview

Users become subscribers in VOSS Automate when they're provisioned with services.

The concept of a VOSS Automate user allows you to stage users into VOSS Automate before assigning a site and UC applications. As part of the process of assigning users with phones and/or services and configuring these in the downstream UC App, the system creates a subscriber entry for the user. For example, once a VOSS Automate user is sent to the Cisco Unified CM, a corresponding subscriber is created in the system.

The table describes the main differences between user and subscribers:

VOSS Automate User	<ul style="list-style-type: none"> • Exists only on VOSS Automate. • Represents VOSS Automate local data associated with a user. • Includes the user's details. • Can exist on different hierarchy levels. • Can be created independently of a user (can exist on its own). • Can be created on VOSS Automate directly or imported from an external source, such as LDAP. • Becomes a subscriber when it is assigned with phones and/or services. • Managed via the Users page (default menu: User Management > Users).
Subscriber	<ul style="list-style-type: none"> • Exists on the UC applications (such as Cisco Unified Communications Manager, Cisco Unity Connection, Microsoft, Avaya, WebEx). • Represents UC application data associated with a user. • Is always associated with a user since it is created once the corresponding VOSS Automate user is sent to a downstream UC app. • Exists only at site level on VOSS Automate. Therefore, before a user is provisioned with phones and/or services, it must be placed in the relevant site. • Managed via the Subscribers page (default menu: Subscriber Management > Subscribers).

Users, Subscribers, and the User Provisioning Workflow

Both users and subscribers are impacted during user provisioning operations, such as LDAP sync, Cisco Unified Communications Manager (Cisco Unified CM) sync, or user bulk loading.

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

1. Sync user from LDAP into VOSS Automate. A VOSS Automate user is created.
2. Move the VOSS Automate user to a site (default menu: **User Management > Move Users**)
3. Push the user to the UC applications. The corresponding subscriber can be created from either of the following:
 - **Subscribers** page (default menu: **Subscriber Management > Subscribers**)
 - **Quick Add Subscriber** page (default menu: **Subscriber Management > Quick Add Subscriber**).

Note: You do not need to send all VOSS Automate users to a UC application, such as Cisco Unified CM, and have a corresponding subscriber created; this is the administrator’s decision, based on criteria associated with each user. We recommend that you filter out any users from LDAP that are not eligible for UC services. It is possible that some ineligible users cannot be filtered due to missing attributes and thus get synced into VOSS Automate. These users remain as VOSS Automate users (a corresponding subscriber is not created).

Additional Functionality of VOSS Automate User

VOSS 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, Cisco Unified CM, manual configuration), and the hierarchy the user was originally added to.
Moving users	Between hierarchy nodes.

VOSS Automate User and Corresponding Subscriber

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

You can create a subscriber directly, via:

- The Admin portal
- Bulk load
- Cisco Unified CM sync

A VOSS Automate user instance is created automatically. If staging is not required (such as when configuring a subscriber directly on a site, using bulk loading), the administrator does not need to add a VOSS Automate user explicitly (as a separate step).

Subscribers 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 Unified CM users
- Phones
- Lines
- Extension Mobility profiles
- Remote destinations
- Voicemail
- WebEx users

A subscriber is simply a representation of data in the UC applications. Each subscriber “comes into existence” 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 Unified CM directly or from VOSS Automate). The subscriber 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 Unified CM end user), the subscriber is available to view in the list view. When the UC application data is deleted (such as the Cisco Unified CM end user), the subscriber disappears.

Unlike VOSS Automate users, there is no local data in VOSS Automate that defines the subscriber; it is all based on data in the UC applications themselves.

In the **Subscribers** list view (default menu: **Subscriber Management > Subscribers**), any user that has a UC applications end user instance appears in the list, regardless of whether there is any other data associated with the user (such as phone or line).

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

Since subscribers are a representation of the data in the UC applications, they may be updated either in VOSS Automate or in the UC applications directly.

- When updating a subscriber on the **Subscribers** page (default menu: **Subscriber Management > Subscribers**), the data on the UC application is updated immediately.
- When updating a subscriber directly in the UC applications, the changes are visible in VOSS Automate the next time you view the subscriber.

Related Topics

- User Provisioning Use Cases in the Core Feature Guide
- Multi-vendor Subscribers in the Core Feature Guide

12.1.3. View Users

From the default menu **User Management > Users** list view, users are shown at or below the current hierarchy node. The users can be created in the system in various ways, depending on your specific setup:

- Synced in from LDAP and promoted to a user
- Synced in from applications (for example: Voicemail, Conferencing, and so on - see: [User Sync Source](#))
- Added to VOSS Automate when creating an end user
- Added to VOSS Automate when creating an administrator user

User creation can also vary across different hierarchies in the system.

Note the following user details:

Sync Source	The source application of user data, for example: LOCAL indicates that the user has been manually created in VOSS Automate and has not been synced from LDAP or from Cisco Unified CM. CUCM indicates that the user exists on both VOSS Automate and Cisco Unified CM, and is not synced from LDAP. The user may have been created first on VOSS Automate (top-down) or created on Cisco Unified CM and synced into VOSS Automate (bottom-up). See: User Sync Source ¹
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 CUCM-LDAP or or top-down LDAP). Example values: <ul style="list-style-type: none"> • CUCM-Local: if the sync source is CUCM and user is synced from CUCM • CUCM-LDAP: if the sync source is CUCM 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) ²
Auth Method	See: User Authentication Methods ³

- Click any user to see additional information about the user. See also: [View a User's Provisioning Status](#).
- Click **Add** to add a user manually.

12.1.4. Add an Admin User

This procedure adds an admin (administrator) user, using VOSS Automate.

To manually create an Admin user:

Important: If the user is to be a multi-role admin user, the user should first reside at site level and then be assigned a self-service **Role** by the administrator, as well as 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.

See: Additional Role Access Profile Validation in the Advanced Configuration Guide.

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.

Note: Fill out at least the mandatory details on the form. Note that the read-only User Type field can have the values:

- “Admin”. This value is defined by the admin role.
 - “End User + Admin”. This value is defined by a data/AuthorizedAdminHierarchy instance associated to the user as well as a self-service role.
-

1. Log in at the hierarchy node where you want to create the Admin user.
 2. Go to (default menu) **User Management > Users** to open the **Users** form.
 3. Click **Add**.
 4. On the tabbed pages of the Users form, fill out field values.
 5. Click **Save**. The new admin user is added.
-

Important: Users are typically added or updated on VOSS Automate from the sync source, such as LDAP, CUCM, or CUC. See [User Sync Source](#) for more details.

Sync source precedence may override user input. When updating a user on VOSS Automate and the following conditions exist, field values are updated from the sync source and not from data input to VOSS Automate (in this case, the fields are read-only in the Admin Portal):

¹ **Sync Source:** see: [User Sync Source](#).

² **User Type:** see: [Add an Admin User](#).

³ **Auth Method:** see: [User Authentication Methods](#).

- Exists on a sync source
 - Has mapped fields
 - Has a higher precedence than LOCAL (VOSS Automate) data
-

Related Topics

- *User Field Mapping*
- *Authorized Admin Hierarchy*
- *User Login Options by Authentication Method and Server Authentication Scope*
- *Update a User*
- *Hybrid Cisco-Microsoft Management*

User Details Tab

Fields	Description
User Name*	Sign-in username. This field is mandatory.
Role*	Choose the user's role. This field is mandatory.
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 VOSS Automate Phone Services ⁻¹
Sync Source	Identifies the application from which the user (and user data) was synced, i.e. LOCAL (VOSS Automate), CUCM or MS-LDAP. This field is read only.
User Type	Read-only. Determined by the role interface. ("Admin", "End User" or "End User + Admin") ⁻²
Auth Method	Identifies the authentication method for the user ⁻³ This section is <i>applicable to End Users only</i> . <ul style="list-style-type: none"> • Local - VOSS Automate User • Automatic - If LDAP or SSO set at hierarchy or above, use this • LDAP ⁻⁴ • SSO ⁻⁵
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 VOSS Automate username.
Authorized Admin Hierarchy	Selected for users with multiple user roles to enable administrative capabilities for end users. ⁶

¹ See [Phone Services Feature Setup](#)

² See Authorized Admin Hierarchies and Roles under [Role-based Access](#)

³ See [User Authentication Methods](#)

⁴ See [View and Update LDAP Authentication Users](#)

⁵ See [Single Sign On \(SSO\) Overview](#)

⁶ See [Authorized Admin Hierarchy](#)

Account Information Tab

This tab 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 Tab

This tab is relevant only to end users.

Defines contact information for the user, such as employee number, employee type, country, state, street, department, manager, Fax number, directory URL, Jabber ID, telephone number, mobile, and IP phone.

Hybrid Status Tab

This tab 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.

Assigned Lines Tab

This tab 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 Tab

This tab is relevant only to end users.

Provides a view showing the composition of the user, this typically includes:

- CUCM
- CUC
- VOSS User Hierarchy
- CUCM User Hierarchy
- CUC User Hierarchy
- CUCM 1 to N

Select the **Provisioned** check box to view additional CUCM'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 Tab

This tab is relevant only to end users, and provides direct links to the associated user apps, including: CUCM User, CUC User Voicemails, Webex App user, Pexip, UCCX Agent, MS 365 user, MS Teams user, and MS Exchange user. For example, clicking on the link for MS Exchange user opens the user's User Mailboxes settings page.

Custom Tab

This tab is relevant only to end users. User defined customized strings and booleans.

LDAP Tab

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 **User Account Control** dropdown supports the following values: **Normal Account**, **Enabled**, **Password Not Required** and **Enabled, Password Doesn't Expire**.

Important:

- User management on the LDAP server from this tab 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 **Action > 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 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. Open the **SSO User** form (default menu **Single Sign On > SSO User**), click **Add**, and choose the IdP that can authenticate the user.
-

12.1.5. Update a User

Users are typically added or updated on VOSS Automate from the sync source, e.g. LDAP, CUCM, CUC, etc. See [User Sync Source](#) for more details.

Important: Sync Source precedence may override user input. If you update a user on VOSS Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (VOSS Automate) data

Only the mapped fields will be updated from the sync source. The data of these fields will be updated from the sync source and not the user input added in VOSS Automate. The Admin Portal would typically render these fields read-only.

For user authentication method (Auth Method) changes upon updates, see [Authentication Method Setting Rules](#).

Sync Source Scenarios

- [Add User Sync Scenarios](#)
- [Update User Sync Scenarios](#)
- [LDAP Add Sync Scenarios](#)
- [LDAP Update and Delete Sync Scenarios](#)

See also [User Field Mapping](#).

Additional Info

Note: Updating an Admin user who has become a subscriber 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**.

If the Admin user password is *updated*, user passwords on Unified CM, Unity 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.

If the user was added as a Microsoft Active Directory LDAP user (see: [Add an 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 VOSS Automate once the user is again synced in VOSS-4UC from the **Sync & Purge** menu.

On the button bar on the associated **Users** form, there are additional actions available to manage a user:

- **Align Hierarchy to Sync Source**

For example, if the user's sync source is 'CUCM', and the data/User is at Customer level and the CUCM user is at Site level, then the data/User instance will be moved from Customer level to the CUCM's hierarchy, i.e. Site level

- **Align Hierarchy to User**

All other related instances of the User (e.g. CUCM, device/cucm/User, device/cuc/user, etc.) will be moved to the hierarchy of the data/User instance.

- **Delete From Ldap**

If the user was also added to a Microsoft Active Directory LDAP server, (see: [Add an Admin User](#)), then the user can also be removed from the server using this menu. The user's **User Details** tab will then reset the **Sync Source** and **Sync Type** of the user according to the Sync Source precedence.

If this menu option is used for users on LDAP servers that are not Microsoft Active Directory LDAP servers on port 636 and with **Enable Write Operations** checked, the delete transaction will fail.

- **Push To Ldap**

This menu must be used when adding user details on the **LDAP** form tab for the *first time* and first adding the LDAP user - see: [Add an Admin User](#). Thereafter, the **Save** button will also update 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.

- If this menu option is used for users on LDAP servers that are not Microsoft Active Directory LDAP servers on port 636 and with **Enable Write Operations** checked, the transaction will fail with a message "Write Operations not enabled on LDAP server".
- For VOSS Automate LDAP synced users, the **LDAP** tab will show a message that Push to LDAP is not allowed.

See [Add an Admin User](#)

12.2. Provisioning

12.2.1. Prerequisites

End-user provisioning with VOSS Automate depends on the completion of the following customer onboarding tasks:

- Devices defined (Cisco Unified Communications Manager, UC applications, 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
- Directory Number Inventory configured
- Voice Mail service defined and associated with a customer

12.2.2. Sample End-user Provisioning Workflow

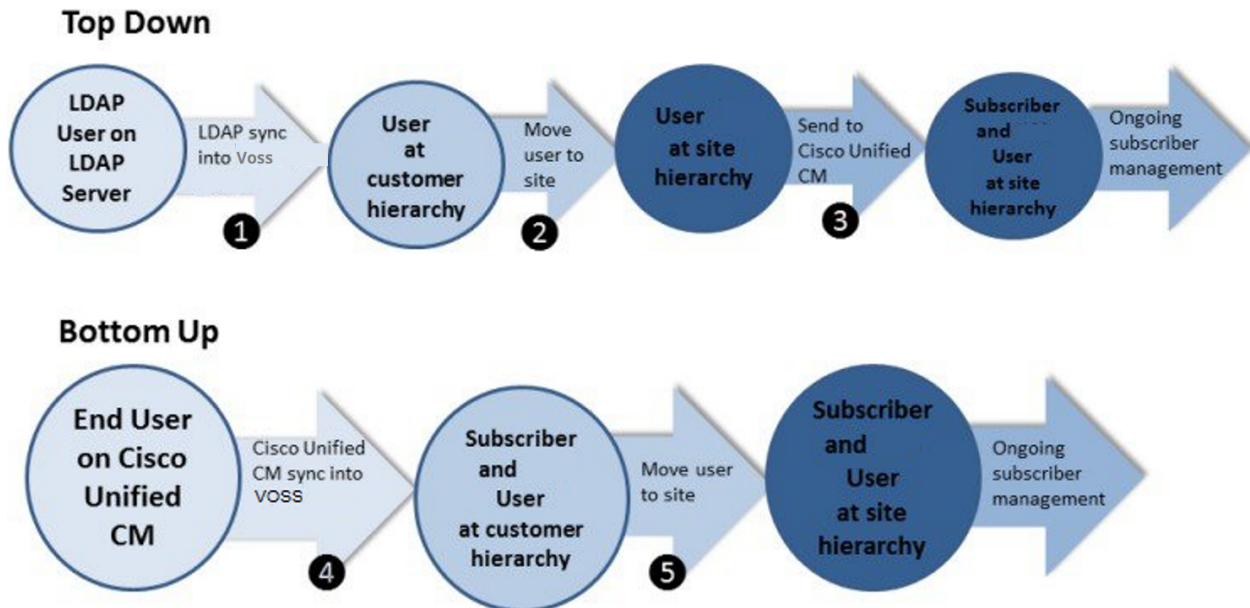
The following is a sample end-user provisioning workflow. Not all steps apply for all customers. Some steps can be performed in alternate order.

1. Synchronize users from the LDAP server:
 - Set up LDAP for User Synchronization
 - Synchronize Users from LDAP
2. If LDAP synchronization is not used and users are provisioned on Cisco Unified Communications Manager (Unified CM), you can synchronize users from Unified CM. For more information, see [Sync Users, Lines, and Phones from CUCM](#).
3. In addition to synchronizing users, you can manually create users. For more information, see [Add an 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. For more information, see [Create a Filter to Move Users](#).
 - b. Enable automatic user moves for synchronization. For more information, see [Automatically Move Users Synchronized from Cisco Unified CM](#).
 - c. Manually move users. For more information, see [Move Users](#).
6. Push manually created and LDAP-synchronized users to Unified CM. For more information, see [Manual User Add to CUCM](#).
7. Manage subscribers (see under [Add a Subscriber](#)):
 - a. Configure a Phone with a Line.
 - b. Associate a Phone to a Subscriber.

8. (Optional) Associate voice mail to a subscriber (see under *Add a Subscriber*):
 - a. Associate the Voice Mail Service to a Subscriber.
 - 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 subscriber (see under: *Add a Subscriber*):
 - a. Add Login/Logout Service on Unified CM.
 - b. Import UC Services and Service Profiles.
 - c. Subscribe the Login/Logout Service to a Phone.
 - d. Associate the Extension Mobility Service to a Subscriber.
10. (Optional) Configure conferencing (see *Introduction to Conferencing* and *Add a Subscriber*).
11. Configure Single Number Reach for a Subscriber (see under: *Add a Subscriber*).
12. Associate a Service Profile to a Subscriber and Enable IM and Presence.

12.2.3. User Provisioning Use Cases

The following are two typical user provisioning use cases:



Use the following menus in VOSS Automate to perform the operations shown in the preceding figure:

1. **User Management > Sync & Purge > LDAP Users**
2. **User Management > Move Users**
3. Performed by any of the following:
 - **User Management > Users**
 - **Subscriber Management > Subscribers**

- **Subscriber Management > Quick Add Subscriber**

4. **User Management > Sync & Purge > CUCM Users, Lines, Phones**

5. **User Management > Move Users**

In each diagram, the user starts on an external server, either an LDAP (for example, Open LDAP or Active Directory), or on Cisco Unified CM. When the user is synced into VOSS Automate, either a VOSS Automate User is created, or both a VOSS Automate User and Subscriber 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 Subscriber and a VOSS Automate User exist. From that point, the user is primarily managed from Subscriber Management.

12.2.4. View a User's Provisioning Status

To view a user's current provisioning status.

1. Log in as provider, reseller, or customer administrator.
2. Go to (default menu) **User Management > Users** to open the Users list.
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** check box is selected by default so that *only provisioned data* is shown. You can clear the check box to show all unprovisioned 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.

12.3. Authentication

12.3.1. User Login Options by Authentication Method and Server Authentication Scope

This section describes whether users can log in on VOSS Automate (Y or N), based on:

- a. User's authentication method (Auth Method), either Local, LDAP, SSO, or Automatic
- b. User's type, either all users, or LDAP synced
- c. Server's authentication scope, either of the following:
 - Current and below
 - Current only

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

User Auth Method	<ul style="list-style-type: none"> • Scope: Current and below • User Type: All 	<ul style="list-style-type: none"> • Scope: Current and below • User Type: synced users 	<ul style="list-style-type: none"> • Scope: Current only • User Type: All 	<ul style="list-style-type: none"> • Scope: Current only • User Type: 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 (If user at server node)	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)

No IDP(SSO) - LDAP Configured and Enabled for Authentication

User Auth Method	<ul style="list-style-type: none"> • Scope: Current and below • User Type: All 	<ul style="list-style-type: none"> • Scope: Current and below • User Type: synced users 	<ul style="list-style-type: none"> • Scope: Current only • User Type: All 	<ul style="list-style-type: none"> • Scope: Current only • User Type: 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)

12.3.2. 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

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.
Subscribers	System users that have, or are linked to, user accounts in one or more UC applications. Subscriber 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:

Auth Method	Description
Automatic	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Authentication is performed in order of preference, in the user's hierarchy, or above:</p> <ol style="list-style-type: none"> 1. Local user <i>only if</i> no LDAP, SSO IdP, in this hierarchy or above 2. LDAP server 3. SSO identity provider (IdP)
Local	<p>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.</p>
LDAP	<p>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.</p>
SSO	<p>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 VOSS-4UC. 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 <i>within</i> 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).</p>

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 Add Subscriber add user	Apply setting from Global Settings.
Quick Add Subscriber modify user	Leave setting as is.

12.3.3. 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 allowing access to the system. Additionally, administrators can configure settings for events such as failed sign-in attempts and lockout duration.

Note: The number of questions in the Password Reset Question Pool must be equal to (or more than) the number set in the Number of Questions Asked During Password Reset field.

As at 21.2, only the legacy Admin GUI provides access to the password reset questions (click your profile name at the top right of the screen). This feature is reserved for future development in the Admin Portal and the Business Admin Portal.

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.

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.

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.

12.3.4. 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`

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](#)
- [Customize Login Page Theme and Text in the Legacy Admin Portal](#) (if a theme is applied to the login screen)

12.3.5. 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.
 - 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.
-

12.3.6. 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 Login 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.

These URLs are specific to the admin role, also pointing to the IdP for SSO authentication, and redirect the user to the relevant administrator interface:

- Admin Portal: `{{"https://{host name}/admin/sso/{Login URI}/login}}"`
- Business Admin Portal: `{{"https://{host name}/business-admin/sso/{Login URI}/login}}"`

IdP(SSO) Credentials

Log in using the relevant SSO identity provider (IdP) credentials.

12.4. Sync and Purge

12.4.1. Introduction to User and Subscriber Syncs

Overview

Users pushed to Cisco Unified Communications Manager (CUCM) are synced between the user management and subscriber management functions of VOSS Automate. Adding, updating, or deleting a user in one place is automatically reflected in the other.

Subscribers and Default Entitlement Profiles

New users added to VOSS Automate using Subscriber Management 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.

12.4.2. 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 VOSS 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 VOSS 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 precedence - 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 VOSS Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (VOSS Automate) data

the data of these fields will be updated from the sync source and not the user input added in VOSS Automate. The Admin Portal would typically render these fields read-only.

The detailed scenarios for the operation: *adding 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	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 hierar- chy	Create data/User Update data/User based on sync source Move App user to data/User hierarchy	APP SOURCE
	Y	Y	below APP user hierar- chy	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 hierar- chy	Error: Create User Log entry with message	APP SOURCE
	Y	Y	above APP user hierar- chy	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 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

Field sync takes place according to:

- Sync Source precedence - 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 VOSS Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (VOSS Automate) data

the data of these fields will be updated from the sync source and not the user input added in VOSS 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 ex- ists	device/ ldap/ User exists	device/ <APP>/ User exists	Hierarchy	Action	User Sync Source
Y			same as user	Update data/User	LO- CAL
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 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 VOSS Automate or any application that is a sync source

Field sync takes place according to:

- Sync Source precedence - 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 VOSS Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (VOSS Automate) data

the data of these fields will be updated from the sync source and not the user input added in VOSS 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:

data/ User exists	device/ ldap/ User exists	device/ <APP>/ User exists	Hierar- chy	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

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 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 VOSS Automate or any application that is a sync source

Field sync takes place according to:

- Sync Source precedence - 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 VOSS Automate:

- that exists on a sync source
- has mapped fields
- has a higher precedence than LOCAL (VOSS Automate) data

the data of these fields will be updated from the sync source and not the user input added in VOSS 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 CUCM 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:

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

12.4.3. User Sync Source

VOSS Automate provides a precedence hierarchy of applications from which to sync user data.

For example:

If CCX data is synced, it will not overwrite user data synced from CUCM or CUC.

Note: Data overwrite will take place according to the relevant mapping table that exists between VOSS Automate data application data.

Default precedence order:

Application	Precedence
MS_LDAP	1
OPEN_LDAP	1
LDAP	1
CUCM	2
CUC	3
AVAYA_SYSTEM_MANAGER	3
BROADWORKS	10
HCMF	10
MICROSOFT	10
MS_365	10
PEXIP	10
UCCX	10
WEBEX_TEAMS	10
ZOOM	10
MS_TEAMS	11
LOCAL	99

Choose **User Sync Source** to see the default application precedence. The **Precedence** column shows the priority of data per application.

Related Topics

- [Add User Sync Scenarios](#)
- [Update User Sync Scenarios](#)
- [LDAP Add Sync Scenarios](#)
- [LDAP Update and Delete Sync Scenarios](#)

12.4.4. User Field Mapping

Overview

User field mapping shows the list of field mappings, at the hierarchy you're working with.

VOSS Automate provides a set of default field mappings (named `default`) between applications and VOSS Automate user data at the `sys` level hierarchy. The system uses these field mappings to align data when syncing.

Whenever an application is added at a hierarchy, the default application mapping is cloned to this hierarchy level and provided with an application name (e.g. IP address for Unified CM, business key for LDAP server). The cloned mapping displays on the **User Field Mapping** page (default menus: **User Management > Advanced > User Field Mapping**), and applies to user management at this hierarchy.

The mapping that applies at the sync hierarchy (for an application that is the sync source) is used when values are written to VOSS Automate user data. Mapping for the following applications is stored in the `data/UserFieldMapping` model:

UC Source	Model Type	Application Name
CUCM	device/cucm/User	CUCM
MS_LDAP	device/ldap/user	LDAP
OPEN_LDAP	device/ldap/InetOrgPerson	LDAP

Example - The default CUCM mapping contains the following mapping:

VOSS Automate	CUCM
User Name	userid

When syncing user data from a CUCM source, where this default CUCM field mapping applies at the hierarchy, the sync updates the VOSS Automate user. You can view the sync source for these users in the **Sync Source** column in the list view of the **Users** page, via (default menus) **User Management > Users**. In this case, the sync source is CUCM.

Important: If application users related to a custom field mapping exist in VOSS Automate, existing mapped fields are read-only and can't be updated.

Additionally, 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 booleansCustom Boolean

After a sync, custom values display on the **Custom** tab of an entry on the **Users/username** page. To view these values, go to (default menus) **User Management > Users**, click on a username in the list to open the **Users/username** page, and select the **Custom** tab

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)

View User Field Mappings

To view the list of mappings:

1. Log in to the Admin Portal.
2. Choose a hierarchy.
3. Go to (default menus) **User Management > Advanced > User Field Mapping** to open the **User Field Mapping** page.
4. View the list of mappings at the hierarchy.
5. Click on a user field mapping to view its details.

Important: While several fields in the hierarchy-specific field mapping can be edited, any changes you make only apply to *new* users (field mapping changes won't apply to existing user data at this hierarchy).

12.4.5. Users Synced from LDAP to VOSS Automate

When users are synced top-down from LDAP into VOSS Automate, LDAP authentication is enabled by default in VOSS Automate for these users.

When LDAP users are pushed to Unified CM (CUCM) and Cisco Unity Connection (CUC), authentication is either LDAP or local authentication, 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.

12.4.6. User Synced from LDAP to VOSS Automate (SSO Enabled)

Passwords are defined and enforced at the Identity Provider (IdP) when the user is synced from LDAP to VOSS Automate with SSO enabled.

12.4.7. Users Synced from LDAP to CUCM

When a user is synced from LDAP to Cisco Unified Communications Manager (CUCM), the password is not synced like other user information that is pulled from LDAP.

If 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. However, if LDAP Authentication is not enabled, the default password is whatever was configured in CUCM as the default. If no default password is defined, then configure a password manually.

12.4.8. Users Synced to VOSS Automate

Passwords are not transferred when users are synced from Cisco Unified Communications Manager (CUCM) to VOSS Automate. An administrator must configure the passwords before the accounts can be used.

The following CUCM users are affected: users that were manually added to CUCM and users synced from LDAP.

12.4.9. Sync or Purge LDAP Users

This procedure syncs or deletes (purges) users that were synced from an LDAP server.

1. Set the hierarchy path to the hierarchy node where the LDAP server is.
2. Go to (default menu) **User Management > Sync & Purge > LDAP Users**.
3. Complete the following fields:

Field	Description
Remove Log Messages	Select the check box if you want to remove user management logs before synchronizing or purging.
Remove Log Direction	Choose Local to remove logs at the hierarchy of the LDAP server. Choose Down to remove logs at and below the hierarchy of the LDAP server. This field appears only if the Remove Log Messages check box is selected.
LDAP Server *	Choose the Organization Unit of the LDAP Server from which you need to sync or purge the users. This is mandatory field.
LDAP Action *	Choose synchronize or purge. This field is mandatory.

4. Click **Save** to start the action you selected.

12.4.10. Sync Users, Lines, and Phones from CUCM

This procedure syncs users, lines, and phones from Cisco Unified Communications Manager (CUCM).

Note: Syncing lines and phones is meant only for self-provisioning and is not intended for a full migration scenario. Only Jabber and desk phones are supported for syncing from CUCM. Single Number Reach (SNR) and Extension Mobility are not supported in terms of adding to CUCM first and then syncing into VOSS Automate.

Use MIF filter to detect the un-synced users, and purge them from the affected site. After the users are purged, import the CUCM once again.

1. Set the hierarchy path to the hierarchy node where the CUCM server is.
2. Go to (default menu) **User Management > Sync & Purge > CUCM Users, Lines, and Phones**.
3. Complete the following fields.

Field	Description
Remove Log Messages	Select this check box if you want to remove user management logs before synchronizing.
Remove Log Direction	Choose Local to remove logs at the hierarchy of the selected Unified CM. Select Down to remove logs at and below the hierarchy of the selected Unified CM. This field appears only if the Remove Log Messages check box is selected.
Action	Choose synchronize. This field is mandatory.
Cisco Unified CM	Choose the Unified CM server. Data is synchronized from the selected Unified CM. This field is mandatory.

4. Click **Save** to start synchronizing.

12.4.11. 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.

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.
2. Go to (default menus) **Apps Management > Advanced > 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.

12.4.12. Purge a CUCM User from VOSS Automate Only

This procedure purges a single CUCM user from the VOSS Automate database only, while leaving it on the associated CUCM.

Note: If the same user is synced from multiple CUCMs, it results in a duplicate user on VOSS 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 (default menu) **User Management > Sync & Purge > Local-Purge CUCM User**.
4. Complete the following fields.

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 VOSS Automate.

5. Click **Save** to purge the selected user from VOSS Automate.

Note: The user remains on the associated CUCM.

12.5. Manage Filters

12.5.1. 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.

To define the filter:

1. Go to (default menu) **User Management > Manage Filters > 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.
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** form (default menu **User Management > Move Users**).

12.6. Move Users

12.6.1. Pushing Users to CUCM

Overview

When managing users in VOSS Automate, you perform several steps to process the new users introduced into the system from the following sources:

- Synced from the LDAP directory
- Synced from CUCM (Cisco Unified Communications Manager)
- Manual configuration in VOSS Automate

One step is to push the user to the CUCM assigned to the customer and site where the user was added. You can push the user to CUCM from VOSS Automate in two ways:

- Automatic Push - Enabled or disabled using the **Auto Push to CUCM** check box from **Site Management > Sites**
- Manual Push - Performed for the same user from **User Management > Users** and for example **Subscriber Management > Quick Add Subscriber**.

There are various options available in VOSS Automate for configuring users with phones, lines, and features. Depending on the option you choose, you can automatically push users to CUCM.

To determine whether to automatically push users to CUCM, consider the following guidelines:

- When users are synced into VOSS Automate from an LDAP server, or the users are configured locally on VOSS Automate, and then the **Subscriber Management > Subscribers** menu is used to provision phones, lines, and features for those users, we recommend an automatic user push to CUCM. It does

not matter whether you perform the Subscribers configuration through the Admin Portal, bulk loaders, or API. We recommend automatic user push to CUCM in all cases.

- When users are configured locally on CUCM and synced into VOSS Automate, the users are already on CUCM, so automatic push to CUCM is not required.

Automatic User Push to CUCM

You can enable Automatic User Push to Cisco Unified Communications Manager (CUCM) by selecting the **Auto Push Users to CUCM** check box on the **Site Management > Sites > Site Details** page. Automatic User Push is cleared (disabled) by default.

Users are automatically pushed to a CUCM in the following situations:

- When users are moved to a site (either by filters, username, or usernames):
 - If a Network Device List (NDL) is configured on that site and contains a CUCM, then users are pushed to the CUCM.
 - If an NDL is configured on that site with no CUCM, nothing happens.
 - If an NDL is not configured on that site, nothing happens.
- When an NDL is added to a site after the site was created:
 - If the NDL is configured with a CUCM, the users at the associated site are pushed.
 - If the NDL is not configured with a CUCM, nothing happens.
- When a CUCM is added to an NDL:

If the NDL is associated with a site, the users on that site are pushed to the new CUCM.
- When a new user is created at the site level:
 - If an NDL is configured on that site and contains a CUCM, the user is pushed to the CUCM.
 - If an NDL is configured on that site with no CUCM, nothing happens.
 - If an NDL is not configured on that site, nothing happens.

Manual User Add to CUCM

You can manually add users to CUCM from hierarchy nodes between Customer and Site, inclusive.

To verify that users are available as subscribers, with assigned phones, lines, and features, go to (default menus) **Subscriber Management > Subscriber**.

Related Topics

- [Quick Add Subscriber for CUCM Users.](#)

12.6.2. Automatically Move Users Synced from CUCM

This procedure automatically moves users that were synced from Cisco Unified Communications Manager (CUCM), using previously defined move filters.

1. Choose **Apps Management > CUCM > Servers**.
2. Click the CUCM 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.

12.6.3. Move Users

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.

Note: To move users, go to (default menus) **User Management > Move Users**.

Related Topics

- Create a Filter to Move Users in the Core Feature Guide
- Automatically Move Users Synced from CUCM in the Core Feature Guide

Move User Restrictions

The table describes restrictions that apply when moving users:

Scenario	Description
Moving users pushed to CUCM	<ul style="list-style-type: none"> • CUCM users can only be moved down the hierarchy. For example, from Customer to Site. • A Network Device List (NDL) containing the same CUCM the users were pushed to must be referenced at or below the target hierarchy node.
Moving users between sites	<ul style="list-style-type: none"> • (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: <ul style="list-style-type: none"> – 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.

Move Options

The table describes three options for moving users:

Option	Description
Move users by filters	Move users based on one or more user attributes, for example, City or Street.
Move users by usernames	Move multiple users at once, by their username (bulk move).
Move user by username	Move a single user, by their username.

Move Users 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 (default menus) **User Management > Move Users**.

Note: Alternative step: Go to (default menus) **Overbuild > Move Users**.

2. Choose the hierarchy where you're moving users from, for example, a customer.

3. Go to (default menus) **User Management > Move Users** (or **Overbuild > Move Users**).
4. In the **Action** drop-down, choose an option for moving the user/s:

Action	Description
Move users by filters	<ol style="list-style-type: none"> a. From the Move From Hierarchy drop-down, choose the hierarchy node from which you are moving the user. b. From the Available list, choose one or more Move Filters and click Select to move them to the Selected list. You can choose filters in a different order to change the order in which they are applied.
Move users by usernames	<ol style="list-style-type: none"> a. From the Move From Hierarchy drop-down, 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	<ol style="list-style-type: none"> a. From the User drop-down, choose the user to move. 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 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.

5. Click **Save** to move users.
6. To verify that moved users are moved to the target hierarchy, go to (default menus) **User Management > Users**, and check that the user has been moved as required.

Related Topics

- For more details around moving one or more users by username, see [LDAP Custom Role Mappings](#)

Move Users from Site to Site

Note: This procedure is relevant on Provider deployments only.

As an administrator, you can move users from one site to another with their assigned devices and services intact. 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 plans.

Non-SLC Dial Plans

When moving a user with their devices and services between sites with a non-SLC dial plan configured, VOSS Automate checks the following conditions:

- The sites are not configured with an SLC dial plan.
- Both sites 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 needed default settings (that is, they are not empty nor null).
- The role is valid at the move-to site.

Non-SLC, Site to Site Move - Models and Relations Moved

When a user is moved from one site to another, the following models and relations move with them:

- `relation/User`
- `relation/Voicemail`
- `relation/Subscriber`
- `relation/SparkUser`
- `relation/LineRelation`
- `relation/HcsCucmCcTagREL`
- `data/InternalNumberInventory`

Fields Updated by Destination Site's Defaults

Various fields from the destination site's defaults update the models that are moved, such as (but not limited to):

- Voicemail Pilot Numbers
- Unified CM Device Pool
- Unified CM Location
- Unified CM Region, and others

For the device/cucm/Line model, these fields are updated:

- Calling Search Space Name
- Route Partition Name
- Share Line Appearance Css Name

Within relation/Subscriber, three models are updated:

- 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.

In addition, 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

Updating these values is also necessary if you want to use the Overbuild feature with your existing Unified CM data in the future.

The following models trigger a warning message when you attempt to move them from one site to another. While VOSS Automate does not prevent you from moving these models, it displays a message to notify you of the possible implications of moving them:

- E.164 associations
- Call pickup groups
- Hunt lists

Note: If you use an API for a version prior to VOSS Automate 11.5.1, the Move Users function has the previous behavior. Devices and services do not move with a user.

Moving Users 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 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.

SLC Dial Plans

When you move a user between sites with an 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 user are moved from a dial plan site to a non-dial plan site the users are set to a default CSS.

SLC Site to SLC Site Move - Models and Relations Moved

When you move a user from one SLC site to another, the models and relations moved are the same as with non-SLC dial plans, with these exceptions:

- When moving relation/Subscriber -> Lines:
 - Lines are disassociated from all phones and the relation.
 - Removing the line from **Subscriber Management > 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 VOSS Automate does not prevent you from moving these models, it displays a message to notify you of the possible implications of moving them:

- Agent line associations
- Lines associated to a subscriber's phones, device profile, or RDP
- Voicemail

Moving Microsoft Users

When the user being moved manually (via **User Management > Move User**) is a Microsoft user, the following models are also moved:

device/msgraph/MsolUser device/msteamsonline/CsOnlineUser device/msexchangeonline/UserMailbox

These models are moved regardless of the hierarchies the users are moved to/from.

12.6.4. 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.
- 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.

12.6.5. Convert User Type CUCM-LDAP to CUCM Local

This tool is used to convert 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”.

Converting a user from CUCM-LDAP to CUCM Local is typically required when the user has been deleted from the LDAP Server, the Unified CM has synced with the LDAP Server, and the user has been set to “Inactive”. In this scenario, the user would be deleted when the Garbage Collection process runs on the Unified CM.

Converting the user to a CUCM Local user prevents the user from being automatically deleted.

- Only users with CUCM-LDAP type are shown by default in the **User to Convert** drop-down.
- If the **Show Inactive LDAP Users Only** check box is selected, the list of users is filtered to only show the “CUCM-LDAP” users with a status of “Inactive”, i.e. status value = 2.

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 will be deleted from CUCM when the Garbage Collector next runs on CUCM.

- Password. The password entered here will be used to set the password for the user on CUCM and CUCxn.

Informational fields show:

- Current User Hierarchy
- LDAP Directory Name
- Current User Status:
 - Active (1): the user is still in LDAP since the last sync

- Inactive (2): the user is not in LDAP since the last sync

12.6.6. Managing Duplicate Usernames

Important: The username must be unique within the hierarchy both upwards and downwards. User email must be unique system-wide.

Users are created in a synchronization with LDAP or Cisco Unified CM, or they are created manually in the VOSS Automate. All users are created according to these duplicate username guidelines:

- The username of a user cannot 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.
- A user cannot be added if another user that is above, or was originally above before being moved, in the current hierarchy has the same username.
- A user cannot be manually added if another user that is at the same level or below in the current hierarchy has the same username.
- You cannot convert a user to a Subscriber / Unified CM user if another user at the same level or below the Unified CM in the current hierarchy has the same username.
- A user may or may not be synchronized from LDAP or Unified CM 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 as shown in these tables:

Note: The restriction on unique usernames in a hierarchy also applies to administrator users.

Users Created in an LDAP Synchronization

Original source of the existing user	Action
LDAP	Simple user update, if the user is coming from the same LDAP server
Cisco Unified CM	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 Unified CM Synchronization

Original source of the existing user	Action
LDAP	User is not synchronized
Cisco Unified CM	Simple user update, if the user is coming from the same Cisco Unified CM server
Manually created	Update user, update provisioning status and SyncTo info with Unified CM server

The table below refers to Subscribers created in VOSS Automate using:

- Subscriber Management > Subscribers
- Subscriber Management > Quick Add Subscriber
- Auto Push feature on Site

Quick Add Subscriber and Subscriber Management create Subscribers and users, while Manage Users and the Auto Push feature convert existing users into Subscribers.

Users Created in VOSS Automate and Pushed to Cisco Unified CM

Original source of the existing user	Action
LDAP	Update user, update provisioning status with Unified CM server (keep SyncTo info the same)
Cisco Unified CM	No action or updates are necessary
Manually created	Update user, update provisioning status with Unified CM server and update SyncTo to the Cisco Unified CM hierarchy if the current SyncTo is below it

Note:

- If a user cannot be created or updated during an LDAP or Unified CM synchronization, a log is created in User Management > Log Messages and the synchronization succeeds. If a user cannot 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 Subscriber.
- 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.
- An update is blocked if two duplicate users are from the same source but originate from different servers.

12.7. Admins

12.7.1. Manage Local Administrators and Operators

This procedure adds administrators for intermediate nodes, and adds or edits local administrators or operators.

Note: Default local VOSS 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 (default menu) **User Management > Admins** to open the **Admins** list.
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 (*):

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. <ul style="list-style-type: none"> 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.
Password	Set the 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 VOSS Automate.
User Type	Cannot be edited - determined by the Role interface (administration / selfservice).

5. Click **Save**.

12.8. Session Timeouts

12.8.1. 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, VOSS 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](#).

12.8.2. 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 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.

12.9. User Accounts and Passwords

12.9.1. Manage Passwords

The following sections describe the various ways passwords are set by default and can be configured between LDAP, VOSS Automate, and other systems, such as Cisco Unified Communications Manager.

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 VOSS 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, Voicemail, and WebEx passwords.

12.9.2. Passwords and Manually Added Users

User Added Manually Through Subscriber Management

A user added through Subscriber Management has the same password that was configured in VOSS Automate when the subscriber was provisioned.

User Added Manually Through 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

Create a Default Password with Unified CM

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.

12.9.3. Force User Password Change

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. Choose **User Management > Users**.
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.

12.9.4. Force Administrator Password Change

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. Choose **User Management > Admins**.
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** check box is cleared.

12.9.5. 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 VOSS Automate.
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the **Change Password** option from the drop-down menu. The **Change Password** screen is displayed.
4. Enter your existing password in the **Old Password** field.
5. Enter your new password in the **New Password** field. Refer to **Minimum Password Length** and **Enable Password Complexity Validation** fields under *Customized Credential Policy* if required.
6. Confirm your new password by re-entering it in the **Repeat New Password** field.
7. Click **Change Password** in the button bar. Your password is changed.

12.9.6. Unlock a Locked Out User

This procedure unlocks a user's account, where the user is locked out on account of a credential policy violation.

Perform these steps:

1. Log in as provider, reseller, or customer admin.
2. Choose **User Management > Users**.
3. Click the user whose account you want to unlock.
4. On the **Account Information** tab, clear the **Locked** checkbox.
5. Click **Save**.

12.9.7. Unlock a Locked Out Administrator

This procedure unlocks an administrator's account, where the administrator is locked out on account of 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.

Perform these steps:

1. Log in as provider, reseller, or customer admin, depending on the location of the locked out administrator.
2. Go to **User Management > Admins**.
3. Click the administrator whose account you want to unlock.
4. On the **Account Information** tab, clear the **Locked** checkbox.
5. Click **Save**.

12.9.8. Manually Disable a User Account

This procedure manually disables a user account. Usually, 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.

Perform these steps:

1. Log in as provider, reseller, or customer admin.
2. Go to **User Management > Users**.

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**.

12.9.9. Manually Disable Administrator Account

Usually, 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.

1. Log in as provider, reseller, or customer admin.
2. Choose **User Management > Admins**.
3. Click the administrator whose account you want to disable.
4. Click the **Account Information** tab.
5. Select the **Disabled** check box.
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**.

12.10. Access Profiles

12.10.1. Introduction to Access Profiles

Overview

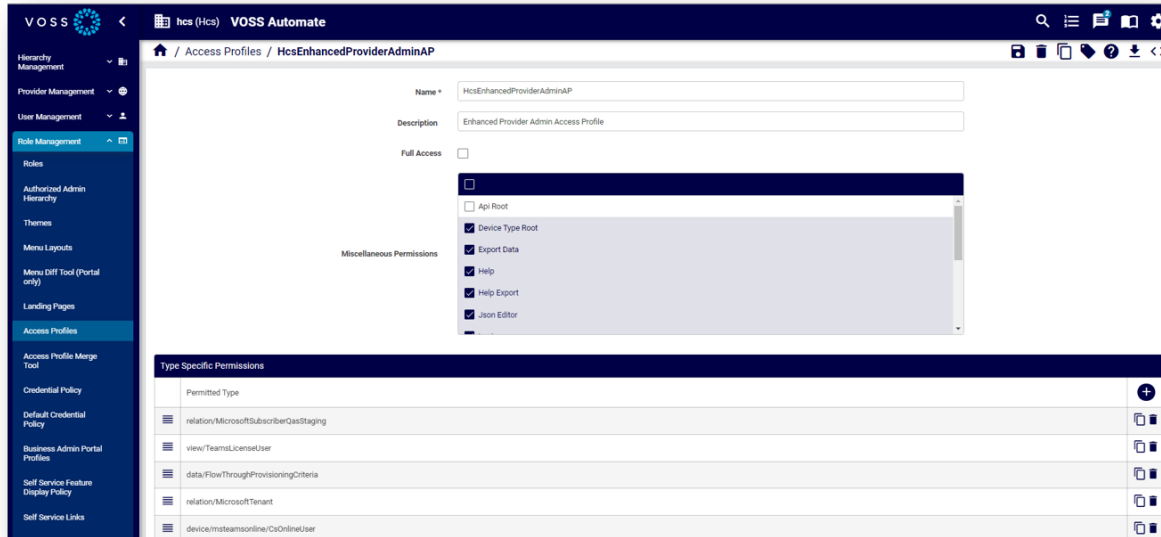
Access profiles define the model types that a user is allowed to access, and are assigned to users via Roles (default menus: **Role Management > Roles**).

Note: 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.
Cloned access profiles	A cloned access profile has equal or less permissions than the access profile of the admin user who creates the clone.

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
- Menu Layout and Access Profiles in the Core Feature Guide

Manage Access Profiles

Admins at a higher level than Provider admins can view, add, edit, and delete access profiles via (default menus) **Role Management > Access Profiles**.

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:

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.

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.
Permitted Operations	operations	The operations that are permitted by this Access Profile for the given type.

12.10.2. Access Profile Permissions and Operations

Administrators *above* Provider level can maintain access profiles as a part of role management. For example, `hcsadmin`.

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.

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)

The lists below provide details on the types of settings.

- **Miscellaneous Permissions**

Many of these are general permissions that can be overridden per model as **Type Specific Permissions**.

The explanations below show the affect of enabling the permission.

- **Api Root:** Access to API root endpoint is permitted.
- **Device Type Root:** Access to API device type model root endpoint is permitted.
- **Export Data:** General permission to export data.
- **Help:** On-line help button is shown.
- **Help Export:** Help data can be exported.
- **Json Editor:** Access to JSON Editor for the editing of model instances. A **JSON Edit** button is available on the GUI form.
- **Login:** Login is allowed.
- **Meta Schema:** Meta schema is accessible.
- **Model Type Choices:** Access to API choices endpoint of model types is permitted.
- **Model Type Root:** Access to API model root endpoint is permitted.
- **Operations:** Operations on models are permitted.
- **Tag:** Models can be tagged.
- **Tool Root:** Access to API tool root endpoint is permitted.
- **Upload:** Uploads are allowed.

- **Type Specific Permissions**

These are typically available on the GUI when listing or showing the type.

Note:

- The 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.
-

Typical operations are listed below:

- **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.
- For system level administrators above provider level: **Purge** for device models. From a list or instance view, remove the local database instance but retain it on the device.

Note: This operation is only applicable in cases where the UC server is still online and available in the VOSS Automate system.

- For designers: **Migration:** a migration template can be obtained.
- For designers: **Tag** and **Tag Version:** a model instance can be tagged and a version provided.

Related Topics

- Introduction to Access Profiles in the Core Feature Guide

12.11. Self Service

12.11.1. 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.
- By default when synced from Cisco Unified Communications Manager.
- Manually assigned by an administrator using **User Management > Users**.

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](#).
- 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.

12.11.2. Self-service and User Configuration

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 Self-service Interface

Task or Item	Description
User access	<p>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.</p> <p>You can grant a user access to Self-service by creating a user with a <i>selfservice</i> 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.</p> <p>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.</p>
User Authentication	<p>Self-service authentication is controlled by the administration interface using the same three authentication methods: Automatic, LDAP, and SSO.</p>
GUI Themes and Branding	<p>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:</p> <p><a href="https://<host>/selfservice/#/login?theme=mytheme">https://<host>/selfservice/#/login?theme=mytheme</p>
Personal Phones (Remote Destinations)	<p>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) check box on the Personal Phones tab under Customizations > Self-service Feature Display Policy.</p> <p>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.</p>

For more information, see:

- [Add a Subscriber](#)
- [Add an Admin User](#)
- [User Authentication](#)
- [Download and Update a Theme on the Legacy Admin Portal](#)
- [Create a Custom Self-service Role](#)

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 Customizations > 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 Customizations > Self-service Feature Display Policy 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 Customizations > Self-service Feature Display Policy 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 VOSS 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 Customizations > Self-service Feature Display Policy to change this setting.

For more information, see:

- [Phones](#)
- [Voicemail](#)
- [Create a Custom Self-service Role](#)

12.11.3. Create a Self-Service Link

1. Navigate to the required hierarchy.
2. Click **Add** and enter a Name for the set of links.
3. Enter one or more Description and Link. The Description will display on the Self-Service GUI. The Link is in the format of a URL, for example: `http://...`

13. Role Management

13.1. Roles

13.1.1. Role-based Access

The system implements role-based access control through:

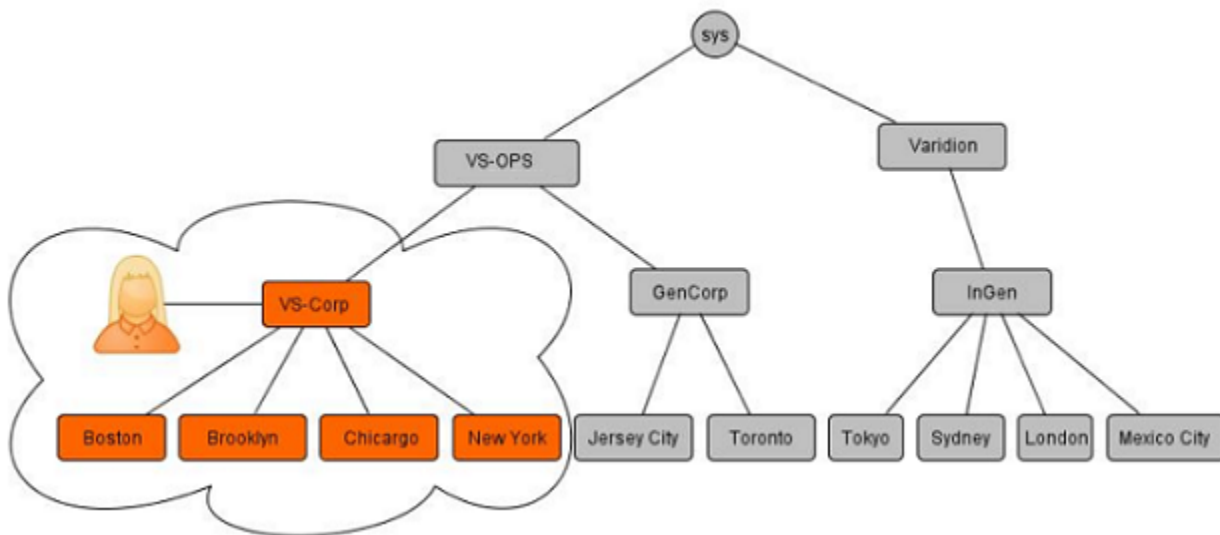
- Hierarchies and user roles
- Authorized Admin Hierarchies, Authorized Admin Hierarchy roles and roles

Hierarchies

Users are added to the system at a specific hierarchy level and can then only view system resources available to users at that hierarchy.

On the interface, this means that the user has no visibility of nodes outside of the sub-tree starting at the parent hierarchy. The user may change to a level of the hierarchy below the parent hierarchy.

The diagram shows that a user at VS-Corp has no visibility of GenCorp and InGen.



For users at site level and with a self-service role, an **Authorized Admin Hierarchy** instance can be assigned that in turn contains an admin role. Such a user is then a multi-role user. For details, see: [Authorized Admin Hierarchy](#).

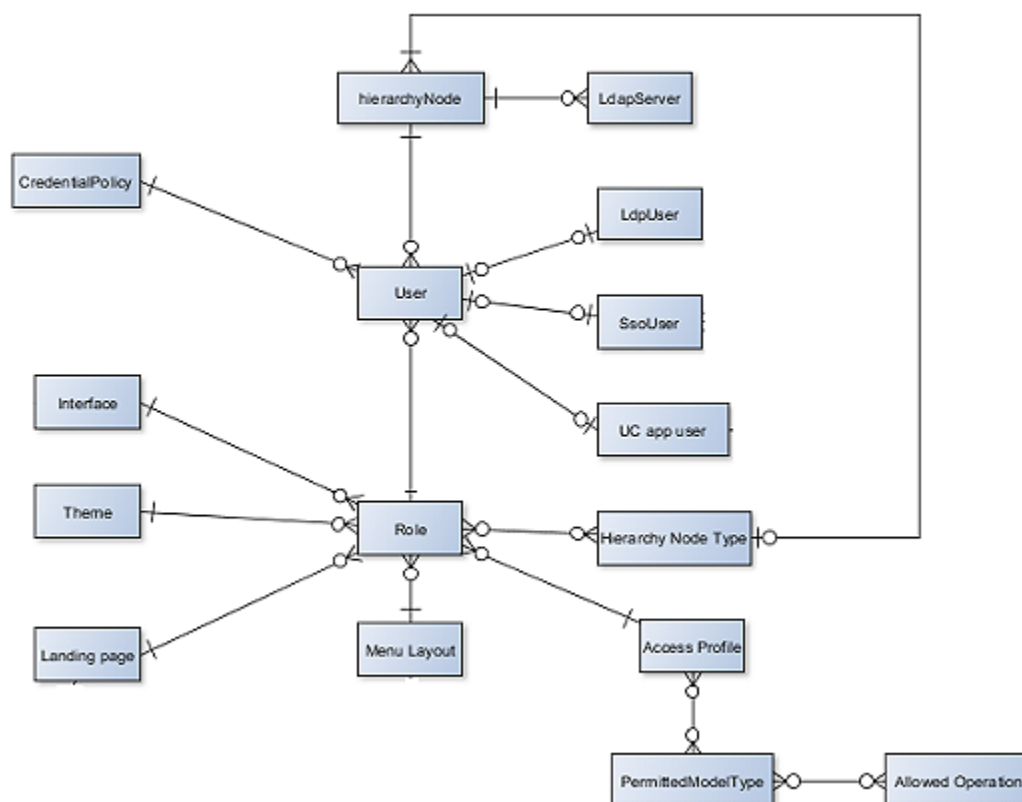
User Roles

From the context of the hierarchy level that a user was created at, role-based access is implemented. When users are added to the system at a hierarchy level, a user role can be assigned to them directly.

Note: The created roles can also be selected and added to an Authorized Admin Hierarchy.

A user role is a combination of:

- Rules applying to the role, specifically, the hierarchy types applying to the role. A role is only available to a user at a hierarchy level that belongs to a hierarchy type associated with the role. For example, a Site Administrator role may have a rule that associates it with Site and Building hierarchy types, but not Customer hierarchy types. In this way a Site Administrator role cannot be associated with a user created at a Customer hierarchy level. A hierarchy rule is therefore enforced by the role.
- System permissions to resources from that hierarchy.
- Access Profiles associated with a User Role that determine access specific operations supported by different models and/or on miscellaneous permissions.
- The visibility of resource attributes.
- The look and feel of the interface.
- Default values of resource attributes.



Related Topics

- Role-based Access for Multi-vendor Subscriber in the Core Feature Guide
- User Roles in the Core Feature Guide

13.1.2. Authorized Admin Hierarchy

Overview

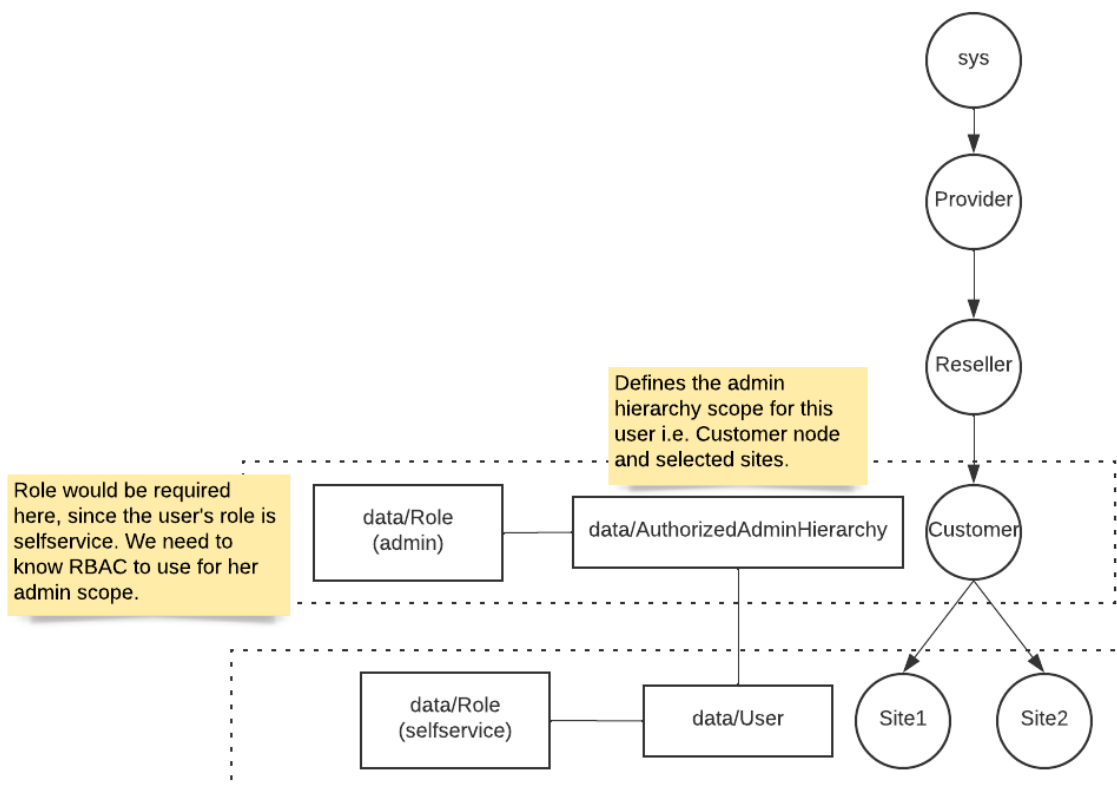
VOSS Automate allows a single user account to be configured as both an End User (with services) and as an Administrator, and supports the following:

- 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

An Authorized Admin Hierarchy 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 instance. See: [User Roles](#).

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.

Users with multiple user roles then have a **User Type** of “End User + Admin”. See: [Add an Admin User](#).



Upon user login, the VOSS Automate system then assigns the appropriate role to the user in accordance with the requested portal:

Portal	Role
Automate Self-service	selfservice
Automate Classic Admin	administration
Automate Admin	administration
Automate Business 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 Single Sign-On for VOSS Automate](#).
- 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.

Manage Authorized Admin Hierarchy

Configuring Authorized Admin Hierarchy involves these high-level tasks:

- Create an instance of Authorized Admin Hierarchy at the relevant hierarchy level.
- Provision the end user as usual.
- Associate the end user with an Authorized Admin Hierarchy instance.

To create an instance of an Authorized Admin Hierarchy:

1. Log in as Customer or Provider administrator and choose **Role Management > Authorized Admin Hierarchy**.
2. To add or modify an Authorized Admin Hierarchy instance, either add or modify the instance **Name** and select the **Role**.
3. Click **Save**

Related Topics

- [Add an Admin User](#)
- [Introduction to Self-service](#)
- [Configure Single Sign-On for VOSS Automate](#)
- For API details, see the REQUEST-PORTAL API request header in: the API Request Headers section in the API Guide.

13.1.3. User Roles

VOSS Automate ships with a powerful role-based access framework that ties a user role to menu layouts, access profiles, landing pages, and themes.

Note: The system comes with a default set of roles, menu layouts, access profiles, landing pages, and themes.

Default roles:

- HCS Admin
- Provider
- Reseller
- Customer
- Site
- User
- MicrosoftOnlyRole (for a Microsoft-only scenario)
- MvsEnhancedCustomerAdministrator and MvsEnhancedProviderAdministrator (for multi-vendor scenarios)

A user role in the system combines the look and feel of the system interface with a number of default permissions and values.

Each user role is a combination of:

Component	Description
Landing page	The content of the first page you see when logging in, including links on the page.
Menu layout	The menu layout associated with a user role defines the available menu, and where relevant, may also include the configuration templates and the field display policies (FDP) that apply to the resources that the menu links to.
Theme	The appearance of the user interface can be associated with a role.
Access profile	Permissions for resources are defined in Access Profiles. An Access Profile can be associated with a user role.
Interface	Defines the application interface the role definition applies to. Roles support the Administration interface and the Self Service interface.

When creating or updating a user, you can select their role. The user will then have a landing page, menu, theme, and interface defined for their user role. For example, the Configuration Template defaults and settings as well as Field Display Policy views of the menu associated with the role apply.

A user role may be assigned to more than one users. The user hierarchy and role serve as components of role-based access control in the system.

A number of default user roles are provided. Each user role has a predefined landing page, menu layout and access profile. Each of these elements, including theme, can be customized.

Note: Users cannot modify their own user role or the associated Access Profile, Menu Layout, Landing Page or any of the Configuration Templates or Field Display Policies associated with the role.

A role may be associated with a specific hierarchy. For example, the Site Admin role can only be assigned to a user at the Site hierarchy level.

Related Topics

- Add and Edit Roles in the Core Feature Guide
- Role-based Access in the Core Feature Guide
- [Role-based Access for Multi Vendor Subscribers](#) and [Multi Vendor Subscribers](#)

13.1.4. Add and Edit Roles

Overview

Provider administrators can manage the roles that are available for administrators, operators, and users at lower levels in the hierarchy.

Note: References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

Edit a Role

To edit an existing role:

1. Log in as provider administrator.
2. Go to **Role Management > Roles**.
3. Locate the role you want to change; then, click on the role to open it.
4. Update the role settings, as required.
5. Save your changes.

Add a Role

To add a new role:

1. Log in as provider administrator.
2. Choose **Role Management > Roles**.
3. Click **Add**.
4. Define role settings:

Setting	Description
Name*	Name of the role. This field is mandatory.
Hcs Component Access*	Controls which HCM-F components (FF or SA) that users with this role have access to. Used with Hierarchy Type and Service Assurance Role Type when mapping roles to HCM-F. This field is mandatory.
Service Assurance Role Type*	Controls read/write access to HCM-F components. Used with Hierarchy Type and Hcs Component Access when mapping roles to HCM-F. This field is mandatory.
Hierarchy Type*	The type of hierarchy nodes applicable at the selected hierarchy level. For example, at Provider level, the following values are allowed: Provider, Reseller, Customer, and Site. While at the Reseller level, the following values are allowed: Reseller, Customer, Site. Controls which roles are available at which levels in the hierarchy. Also used with Hcs Component Access and Service Assurance Role Type when mapping roles to HCM-F. This field is mandatory.
Description	Description of the role.
Access Profile*	Permissions for resources are defined in Access Profiles. This field is mandatory.
Menu Layout	The menu layout assigned to the role. Controls the menu options available to users assigned to the role.
Landing Page	The home page assigned with the role. Controls what the home page looks like for users assigned to the role.
Theme*	The name of the theme assigned to the role. The theme controls the overall look and feel of the Admin Portal. This field is mandatory.
Self Service Feature Display Policy	The selected Self Service Feature Display Policy that is associated to the role.
Self Service Links	Provide useful links to Self Service end users.
Custom Interfaces	Add Interface Types and Names for the role. The available custom Interface Type is InterfaceBusinessAdminPortal, which provides access to the Business Portal Admin Portal.

5. Click **Save** to save the role.

Microsoft-only Role

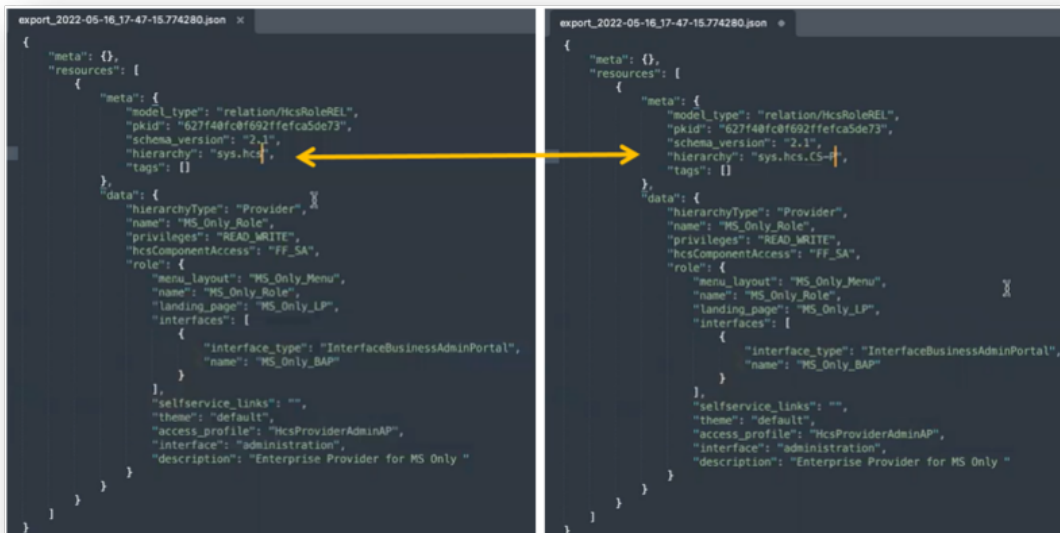
Starting with version 21.3-PB1, VOSS Automate ships with a Microsoft-only role (`MicrosoftOnlyRole`) and accompanying role-based access control elements, which are predefined for a Microsoft-only user interface experience. These elements include predefined field display policies, landing pages (`MicrosoftOnlyLP`), and menus (`MicrosoftOnlyMenu`), and a MS-only Business Admin Portal profile. Installing these templates provides the baseline for a Microsoft-only version of VOSS Automate, and hides non-Microsoft GUI elements, such as the FDPs, menus, and landing pages reflecting functionality used for managing Cisco devices.

To use the `MicrosoftOnlyRole` in VOSS Automate:

1. Log in to VOSS Automate as `hscadmin`.
2. Go to (default menus) **Role Management > Roles**.
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, landing page, and Business Admin profile.

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 (default menus) **Administration Tools > Import**.
8. Browse to the location you saved the JSON file, then click **Import**.
9. Go to (default menus) **Role Management > Roles** 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 (default menus) **User Management > Admins**. 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.

13.1.5. Clone a Role

Use this procedure to clone an existing role for a specific hierarchy node (provider, reseller, customer, or site).

Procedure

1. Log in as entadmin or provider administrator.

Note:

Administrators can clone roles associated with, or below, their level in the navigation hierarchy.

2. Choose **Role Management > Roles**.
3. Click the role that you want to clone.
4. Choose **Action > Clone**.
5. Enter a unique name for the role in the **Role** field. Make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).
6. (Optional) Add a description for the role in the **Description** field.
7. Click **Save** to save the role to the hierarchy that appears in the breadcrumb.

13.1.6. Create a Service Assurance Only Role

To restrict an administrator to performing only service assurance tasks, you need to create the appropriate service assurance only role.

Procedure

1. Log in as entadmin or provider administrator.
2. Choose **Role Management > Roles**.
3. Click **Add**.
4. Enter a name, and optionally a description, for the role.
5. Select the hierarchy type for the role.
Controls the hierarchy level that the role is available at.
6. From the **Hcs Component Access** drop-down, choose **Service Assurance Only**. The privileges, menu layout, and landing page values are automatically set to the appropriate values for a service assurance only role and cannot be overridden.
7. Optionally, select a theme for the role.
8. Click **Save**.

13.1.7. Create a Fulfillment Only Role

To restrict an administrator to performing only fulfillment tasks, you need to create the appropriate fulfillment only role.

Procedure

1. Log in as entadmin or provider administrator.
2. Choose **Role Management > Roles**.
3. Click **Add**.
4. Enter a name, and optionally a description, for the role.
5. Choose the hierarchy type for the role.
Controls the hierarchy level that the role is available at.
6. From the **Hcs Component Access** drop-down, choose **Fulfillment Only**.
7. Choose the privileges for the role.
8. Optionally, select a menu layout, landing page, and theme for the role.
9. Click **Save**.

13.1.8. Create a Custom Self-service Role

This procedure modifies the default Self-service feature display policy (FDP), creates a custom Self-service role (*selfservice*), and assigns the custom Self-service role to users.

VOSS Automate provides a default Self-service feature display policy. When providers, resellers, customers, and sites are added in VOSS Automate, the default Self-service feature display policy is assigned automatically to the *selfservice* role at each level of the hierarchy. The default Self-service feature display policy allows you to perform the following tasks in the Self-service interface:

- Add Voicemail
- Enable Remote Destination Profile (RDP)
- Manage phones and phone lines (but adding smart devices is not allowed)
- Assign configuration templates for phones, RDP, and voicemail
- Link to Launch Webex from Self-service interface

Most options are set to **Show**, rather than **Hide** to indicate that the Self-service user can view and edit the item in the Self-service interface. For example, My Availability, Speed Dials, Call Forward Basic, Advanced Call Forwarding, Ring Schedules, Advanced Timer options, Password, and PIN are all set to **Show**.

Perform these steps:

1. Log in as Provider administrator or higher.
2. Clone the default feature display policy:
 - a. Go to (default menus) **Customizations > Self Service Feature Display Policy**.
 - b. In the list view, click on the Default Self-service feature display policy. The Self Service Feature Display Policy (Default) screen opens.

- c. To create a copy (clone) of this Default FDP, click the **Clone** icon. The copy (clone) you created opens in the editing screen.
- d. On the **Details** tab, type a new name for the Self-service feature display policy in the **Name** field.
- e. Configure options for the clone on the tabs of this screen: **Details, Phones, Personal Phones, My Information, Voicemail, Call Forward**:

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 labeled **User can enable Voicemail (Add a Voicemail Account)** and the second check box is labeled **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 **Subscriber Management > Subscribers** page, 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 check box is no longer applicable.

Similarly, select the appropriate check boxes on the **Phones** and **Personal Phones** tabs.

To	Do
Allow users to add their own smart devices	On the Phones tab, click User can add own smart devices .
Add more phones or devices from Cisco Unified Communications Manager	On the Phones tab, complete information to add the phones or devices to the Device Configuration Templates for User area of the screen.
Change the Default RDP configuration template	On the Personal Phones tab, choose a different template from the Device Configuration Template for End-User Remote Destination Profile Add drop-down menu.
Change the Default Voicemail configuration templates	On the Voicemail tab, choose different templates from the drop-down menus.
Show/hide individual Voicemail options such as Voicemail Basic, Voicemail Devices, Phone Notification Device, Voicemail Alternative Extensions	On the Voicemail tab, choose Show from the specific drop-down menus.
Show WebEx link in the Self-Service interface	On the My Information tab, select Show from the Link to Webex self service portal drop-down menu. Note: The WebEx link (Protocol, Address, Port, and Site Name) must be defined in Device Management > WebEx > Servers and the subscriber must have access to WebEx on the WebEx tab (Subscriber Management > Subscribers). Ensure that when you expand the WebEx user form, the Enable CET and Enable PMR check boxes under Privilege are selected.
Hide Self-Service options from users	Choose Hide from the appropriate drop-down menus.

- f. Click **Save**. The custom Self-service feature display policy appears in the list and can be assigned to Self-service roles.
3. Assign the custom Self-service feature display policy to one or more Self-service roles.
 - a. Go to (default menus) **Role Management > Roles**.
 - b. Choose a Provider, Reseller, Customer, or site level Self-service role.
 - c. From the **Self Service Feature Display Policy** drop-down menu, choose the custom Self-service feature display policy you created in step 2.
 - d. Click **Save**.
 - e. If desired, repeat sub-steps b to d for other Self-service roles.
4. If a Cisco Unified Communications Manager sync or LDAP sync is not performed, manually assign the custom Self-service role to one or more existing users.

Note: You do not need to perform this step for new users who are added to the system in the future. New users are automatically assigned the Self-service role that you specify for the reseller, customer, or site when it is added to the network.

- a. Log in as Provider, Reseller, or Customer administrator.
- b. Go to (default menus) **User Management > Users**.
- c. Choose the user for whom you want to assign the custom Self-service role.
- d. From the **User Details** tab, at the **Role** drop-down, choose the custom Self-service role.
- e. Click **Save**.

13.1.9. Business Admin Portal Custom Interface

A role custom interface is available to assign to an administrator user so that the administrator can access the Business Admin Portal. Refer to the “Business Admin Portal” online help or documentation for details on this interface.

1. Log in as a provider administrator.
2. Choose **Role Management > Roles** and either choose an existing role to modify or create a new role (refer to “Clone a Role”).
3. Click + next to **Custom Interfaces**, and add an entry to the Custom Interfaces group:
 - a. From the **Interface Type** drop-down, choose **InterfaceBusinessAdminPortal**.
 - b. From the **Name** drop-down, choose the required interface name.
4. Click **Save**.

An administrator with this user role will be able to log in on the Business Admin Portal when appending the following endpoint to the login URL:

`https://<VOSS Automate IP>/business-admin/`

13.2. Themes

13.2.1. Introduction to Themes

Overview

Themes allow you to control 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. VOSS 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
- Manage Themes in the Legacy Admin Portal in the Core Feature Guide
- Create a Theme in the Admin and Business 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 <i>Less Files and Customizing Themes</i> in the Advanced Configuration Guide.
Custom branding options	Configured directly within the GUI

Note: File-based themes are not used for the Business Admin Portal.

To access theme management functionality in VOSS Automate . . .

- Legacy (classic) Admin Portal: Go to (default menus) **Role Management > Themes**.

Themes [default]

Base Theme Customisation Login Page Details

Theme Name* default

Navbar Text VOSS Automate Provider

Description VOSS Automate

Use this Theme to style Login page

Hide from Lower Hierarchies

Site Title VOSS Automate

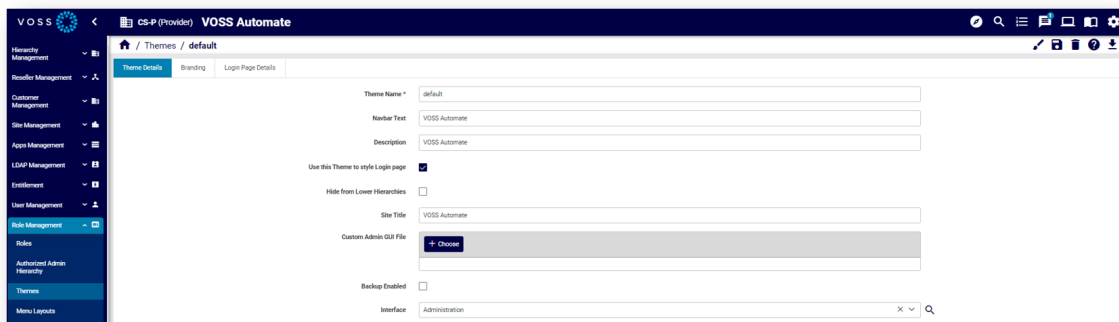
Import File

Browse

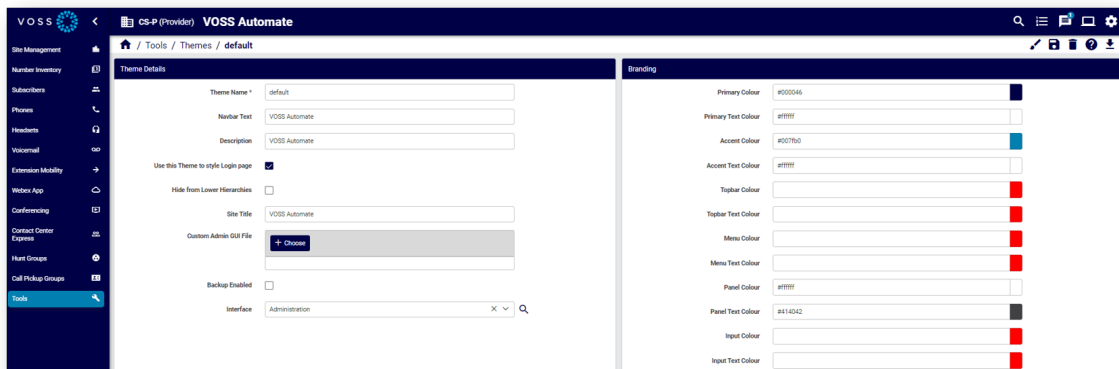
Backup Enabled

Interface Administration

- Admin Portal (introduced at v21.2): Go to (default menus) **Role Management > Themes**.



- Business Admin Portal: Go to (default menus) **Tools > Themes**.



Securing Themes

When importing a file-based theme to VOSS 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. See [Customize Login Page Theme and Text in the Legacy Admin Portal](#). See [Customize Login Page Theme and Text in the Legacy Admin Portal](#).

13.2.2. Manage Themes (Legacy Admin Portal)

This section describes how to manage themes in the VOSS Automate legacy Admin portal.

Add a Theme in the Legacy Admin Portal

This procedure adds a theme on the legacy Admin GUI, and involves two steps:

1. Prepare the theme file.
2. Import the file to add the theme to the system.

Prepare a Theme File for Import

It is recommended that you use an export of an existing theme as a baseline, and update it with a new name, images, and colours, as required.

Prerequisites:

- [Download and Update a Theme on the Legacy Admin Portal](#)

To prepare the theme file:

1. Create a folder with the same name as the theme you want to create, and unzip the exported theme to this folder.

Note:

- Ensure you maintain the directory structure.
 - For the name of the folder, only alphanumeric characters or underscores are allowed. Do not use spaces or special characters.
-

2. Add any CSS overrides to the file.

Note: You can only modify the definitions as shown in the export of a provided CSS file (`skin.css`).

3. Add required image files to the folder (if any).

For image filenames, you can use the following characters and character types:

ALPHA / DIGIT / "-" / "." / "_" / "~" / "#"

Important: If customization is done on MS Windows, check that no `desktop.ini` files reside in the directory tree of the theme before compressing it.

4. Create a .zip archive file with the same filename as the folder.

Import a Theme File

This procedure imports a prepared file to add a theme in the legacy Admin Portal.

Pre-requisites:

- Prepare a theme file.
- You must be a Provider admin or higher to add a theme.

To add a theme file to the Admin GUI:

1. Log into the VOSS Automate Admin GUI (legacy).
2. Choose the hierarchy level at which the theme will be created.
3. Go to (default menu) **Role Management > Themes**.
4. On the **Themes** list view, click **Add** to open the **Themes** page.
5. On the **Base** tab:
 - a. Add the theme name, which must be the same as the theme file name.
 - b. Enter the navigation bar (navbar) text, if required. This text displays on the navigation bar next to the logo.
 - c. Optionally, add a description.
 - d. To apply the theme to the Login page, select **Use this Theme to style Login page**.

Note: Applies to the relevant Login page, either Self-service or Admin Portal. To change the banner text for the Login page, see [Customize Login Page Theme and Text in the Legacy Admin Portal](#).

- e. To prevent admins at lower levels of the hierarchy viewing this theme in the list view, select **Hide from Lower Hierarchies**.
 - f. Add a site title, if required. The site title displays in the browser tab.
 - g. Browse to the location of the theme zip file. Wait for the file to display in the **Import File** field.
 - h. Optionally, select **Backup Enabled** to create a backup of the current theme on the server (if an existing theme file exists).
 - i. Choose the interface where this theme will apply, either Administration (default) or Self-service.
6. To customize the theme, update fields on the **Theme Customization** tab. See *Manage Themes (Admin Portal and Business Admin Portal)*.

Note: All fields on this tab become mandatory once you enter any details on this tab.

7. To customize the Login page, update fields on the **Login Page Details** tab. See *Customize Login Page Theme and Text in the Legacy Admin Portal*
- a. Add a title for the top of the Login page.
 - b. Add banner text.
8. Click **Save**.

Important: Do not leave the screen until the theme processing completes and the theme list refreshes. This can take a few minutes, depending on the complexity of the theme you're uploading.

Download and Update a Theme on the Legacy Admin Portal

This procedure downloads an existing theme, edits it, and re-uploads it to the legacy Admin Portal.

Pre-requisites:

- You must be a Provider admin or higher to customize a theme.

To download and update a theme:

1. Log in to the legacy Admin Portal.
2. Choose the hierarchy level at which the theme will be applied.
3. Go to (default menu) **Role Management > Themes**.
4. On the **Themes** list view, click on the theme you wish to download.
5. Click **Action > Download**. The file is downloaded as a .zip archive with the name of the theme, and contains a folder with the theme name, and the following files:
 - skin.css
 - skin.less
6. Edit the files.
7. When editing is complete, ensure the directory folder name is the same as your theme name, then compress the folder and save the file with the theme name and a .zip file extension.

Note:

- An error message displays if the file does not have a valid file extension.
- Any files or folders inside the zip file archive that start with a '.' character are silently discarded when unzipping the theme. For example, if the zip archive contains any files named `._.DS_Store` or `.directory`, these are ignored.

Important: If customization is done on MS Windows, check that no `desktop.ini` files reside in the directory tree of the theme before compressing it.

8. Import the updated theme:

Note: No file upload is required if the theme update does not require an updated CSS in a zip file but only updates the text of the theme.

- Go to (default menu) **Role Management > Themes**
- On the **Themes** list view, click on the theme you're updating.
- On the **Base** tab, click **Browse** at the **Import File** field, and open a theme with the same name.
- Optionally, select **Backup Enabled** to create a backup of the current theme on the server.
- Click **Save** to complete the import process.

Customize Login Page Theme and Text in the Legacy Admin Portal

This procedure applies a theme and updates the text of the Login page, in the legacy Admin Portal.

- Log in to the legacy Admin Portal.
- Choose the hierarchy where the theme was created, or where it belongs.
- Go to (default menu) **Role Management > Themes**.
- On the **Themes** list view, click on the theme you want to use for the Login page.
- Update the **Base** tab:
 - Select the **Use this Theme to style Login page**.

Note: When selecting this checkbox and a theme with the same Interface already has the Login page checkbox selected, this option is disabled on the existing theme as there can only be one Interface-Login page combination on the system.

Any new themes, or updates to existing themes, may modify other themes on the system with the same Interface by disabling their Login page attributes.

If no Interface is specified, the interface of the new Login theme defaults to *Administration*.

6. Update the **Login Page Details** tab:

- Add title text, which is used for the top of the Login page.
- Add banner text (limited to 2048 characters), which is used at the bottom of the Login page.

Add references to the cookie policy and privacy policy in the Banner Text field. These are added as placeholders:

- `{{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.

- c. Optional. In the **Cookie Policy** field and the **Privacy Policy** field, add link text captions and a URL for each policy.

Note: Although the cookie and privacy policy references are optional, the captions and URLs are mandatory if they're used, and the placeholder references are then also required in the **Banner Text** field.

For suggested input on the use of cookies by VOSS Automate in the cookie policy text, see [VOSS Automate Cookie Policy](#).

Browsers with blockers installed that prevent new tabs from opening will affect the functionality of links in the login banner.

Privacy policy links can also be added to user menus. See [Privacy Policy Menu Items](#) and [Manage Privacy Policy Menu Items](#).

To customize the banner text style, see "Theme Banner Customization" in the Advanced Configuration Guide.

7. Click **Save**.

Apply a Login Page Theme When Logging In

The Login page theme can also be applied to the login page during the log in process. To do 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
 - `https://instance/portal/#/login?targetAppMode=admin&theme=ABC` - Login page will show use ABC theme
- Business Admin Portal:
 - `https://instance/portal/#/business-admin` - Login page will show use XYZ theme

`https://instance/portal/#/login?targetAppMode=business-admin&theme=ABC` - Login page will show use ABC theme

13.2.3. Theme Element Color Reference for the Legacy Admin Portal

Note: Color selection is optional: where no colors are selected, defaults apply.

The Legacy Admin Portal GUI Element variable below is a descriptive name of the Admin Portal and Business Admin Portal GUI element that will be affected by the Color variable, which corresponds with the color name on the Theme design form.

Element	Color	Theme GUI Branding tab
\$sidebarLogoBgColor	\$primaryColor	Primary Color
\$sidebarBgColor	\$primaryColor	Primary Color
\$topbarTextColor	\$primaryLightestColor	Very Light Primary Colour
\$topbarIconColor	\$primaryLightestColor	Very Light Primary Colour
\$submenuBgColor	\$primaryColor	Primary Color
\$darkSubmenuBgColor	\$primaryDarkColor	Dark Primary Colour
\$horizontalSubmenuBgColor	\$primaryColor	Primary Color
\$horizontalSubmenuItemHoverBgColor	\$primaryColor	Primary Color
\$horizontalSubmenuItemDarkHoverBgColor	\$primaryColor	Primary Color
\$menuItemActiveBgColor	\$accentColor	Accent Color
\$subMenuItemActiveTextColor	\$accentLightColor	Light Accent Color
\$subMenuItemActiveIconTextColor	\$accentLightColor	Light Accent Color
\$darkMenuItemActiveBgColor	\$accentColor	Accent Color
\$darksubMenuItemActiveTextColor	\$accentLightColor	Light Accent Color
\$darksubMenuItemActiveIconTextColor	\$accentLightColor	Light Accent Color

13.2.4. Customize the Self-service Theme

This section provides steps to customize and add a Self-Service theme from within the legacy Admin Portal.

Customize an Existing Self-service Theme

To customize an existing Self-service theme:

1. Log in to the legacy Admin Portal.
2. Choose the hierarchy level at which the theme will be applied.

Note: Themes can only be customized by a Provider Administrator (or higher).

3. Go to (default menus) **Role Management > Themes** to open the **Themes** list view.

4. Click the Self-service theme you wish to download.
5. Click **Action > Download**. The file is exported in a .zip archive.

Note: The file is exported with the name of the theme. The archive contains a folder and a .css file with the theme name in it, for example voss_selfservice.zip contains voss_selfservice/voss_selfservice.css.

6. Modify the .css file, for example voss_selfservice.css. Use your browser to inspect the elements of the theme on the GUI that you wish to customize.
7. When editing is complete, ensure the directory folder name is the same as your theme name. Compress the folder and save the file with the theme name and a .zip file extension.

Note: An error message will display on the user interface if the file does not have a valid file extension.

8. Upload the edited file:
 - a. Go to **Role Management > Themes** and click on the theme to open it's editing screen.
 - b. If this file theme contains an update, browse to locate the file.

Note: If a theme update does not require an updated CSS in a zip file but only updates the text of the theme, then no file upload is required. See also [Add a Theme in the Legacy Admin Portal](#).

- c. Optionally, select **Backup Enabled** to create a backup of the current theme on the server.
- d. From the **Interface** drop-down, choose **Self Service**.
- e. Click **Save**. The file is imported.

Add a Self-service Theme

The preferred method to add a new Self-service theme is to downloading an existing theme to maintain directory structure and file naming conventions.

To add a new Self-service theme to the system:

1. Log in to the legacy Admin Portal.
2. Choose the hierarchy level at which the theme will be created.
3. Go to **Role Management > Themes** to open the **Themes** list view.
4. Click **Add** to open the **Themes** page.

Note: Themes can only be customized by a Provider Administrator (or higher).

5. Enter the **Theme Name** (same as the file name created above).
6. Enter an appropriate **Site Title** if required. The site title entered here is the title displayed in the browser tab.
7. Browse to locate the theme zip file you wish to import. Wait until the system displays the file in the **Import File** field.

8. If the theme must also apply to the login page, select **Use this Theme to style Login page**.
9. To set login banner text and notices on the login page, refer to [Customize Login Page Theme and Text in the Legacy Admin Portal](#).

Note: The **Use this Theme to style Login page** check box does not have to be enabled for banner text to show.

10. From the **Interface** drop-down, select **Self Service**.
11. Click **Save**.

Customize the Self-service Banner Style

To customize the Self-service banner style, find the element `.banner-text` in the CSS file and customize it, for example:

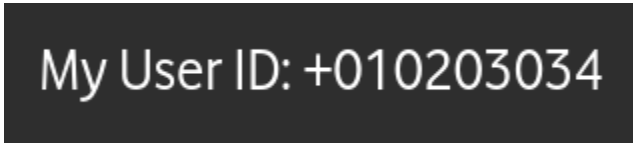
```
.banner-text {
  background-color: #515150;
  color: #FFFFFF;
}
```

Customize Self-service Theme for Minimal Mode

This section describes the options for customizing the Self-service theme to support minimal mode.

Important: If your theme uses a dark colors, the minimal theme may need to be modified to provide a contrasting text and background display.

Examples of minimal mode image snippets and theme settings



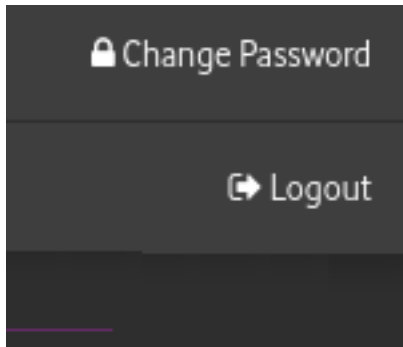
```
.minimal-mode-container {color: white;}
.minimal-mode-container .overlay {background-color: #2e2e2e!important;}
```

- resized logo (<number> variable)
- resized tagline (<number> variable)



```
.logo-holder-header {padding: <number>px <number>px;}
.ss-tagline {height: <number>px; width: <number>px;}
```

- contrasting drop-down menu items and text



```
.minimal-mode-menu ul {background: #3e3e3e;}
.minimal-mode-menu ul li {border-bottom: 1px solid #2e2e2e;}
.minimal-mode-menu ul li > a {color: white;}
```

13.2.5. Manage Themes (Admin Portal and Business Admin Portal)

Overview

The **Themes** page in the Admin Portal and in the Business Admin Portal can be used to create a theme that applies to the Business Admin Portal as well as to the VOSS Automate Admin Portal.

Note:

- To access the Themes page in the Admin Portal, go to (default menus) **Role Management > Themes**.
- To access the Themes page in the Business Admin Portal, go to (default menus) **Tools > Themes**.

You can select the following tabs on the **Themes** page in the Admin Portal:

- Theme Details
- Branding
- Login Page Details

Custom Themes

You can create a custom theme to change the following properties of the Business Admin Portal:

- Primary and accent colors
- Logo image
- Login screen background image

If the background image also contains logos, we recommend that these be placed on the bottom of the image.

- Background image for menu
- Browser tab title

Note: Two themes are compiled when you add a new theme in the Business Admin Portal. For this reason, it takes longer to compile themes on the Business Admin Portal than on the Admin Portal.

Themes created in the Admin Portal (or in the Business Admin Portal):

- Can't be exported in full
 - Require the use of the legacy Admin Portal to include Login page text and if you need to create a non-admin interface (Self-service).
-


Custom Theme File

If you're configuring a theme for the Admin Portal (via the Business Admin Portal or the Admin Portal), you will need to upload a custom Admin Portal theme file.

When using a theme file, the theme will apply to the Legacy Admin Portal. If you customize the theme via the **Branding** tab settings, the updates apply only to the Admin Portal and the Business Admin Portal. You can overwrite these updates in the legacy Admin Portal.

If you don't add a theme file, making changes to the theme via the **Branding** tab will apply to the legacy Admin Portal, the (new) Admin Portal, and to the Business Admin Portal. In this case you won't be able to upload a file theme to update the theme.

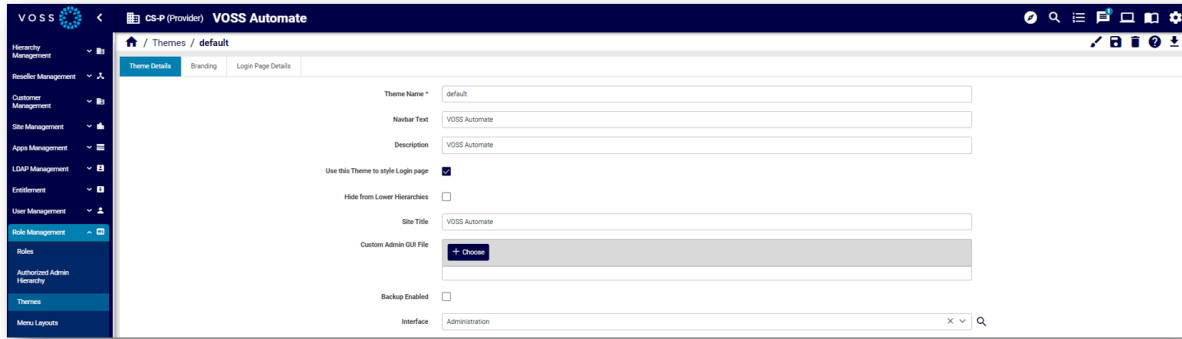
Preview a Theme

When creating a theme, you can use the toolbar **Preview** icon  to see what your theme looks like before assigning it to a user role. Once you assign a theme to a user role it is applied to the GUI.

Theme Details Tab

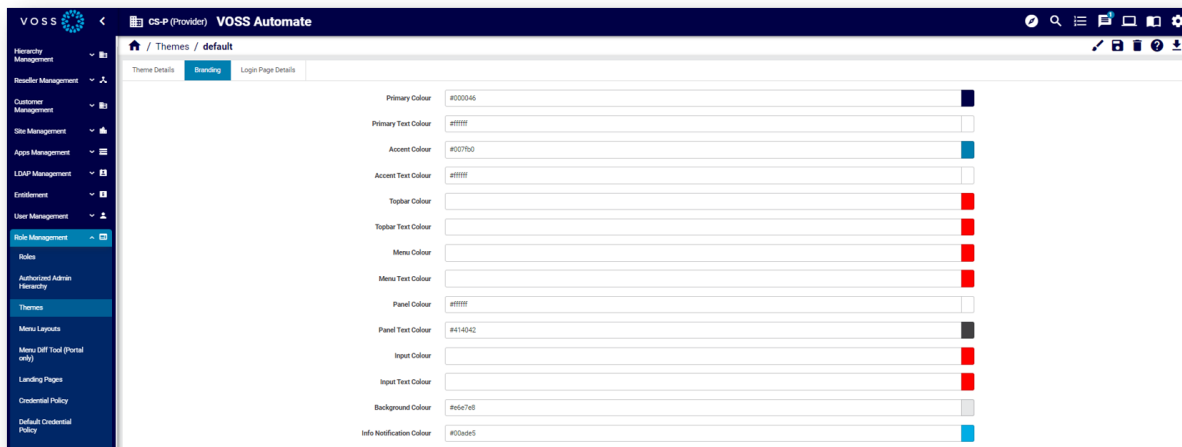
On the Theme Details tab of the Themes page you specify theme details:

- Provide a theme name and a description
- Specify navigation bar text
- Define whether to use the theme to style the Login page
- Define whether to hide the theme from lower hierarchies
- Specify the site title
- Upload a custom theme file, if applicable
- Enable or disable backups
- Define the GUI where the theme is applied



Branding Tab

On the **Branding** tab (in the Admin Portal or Business Admin Portal), 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.



When uploading images for the theme:

- Note the 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.
- The image for Menu Background does not apply to the VOSS Automate Admin Portal.
- For image filenames, you can use the following characters and character types:

ALPHA / DIGIT / "-" / "." / "_" / "~" / "#"

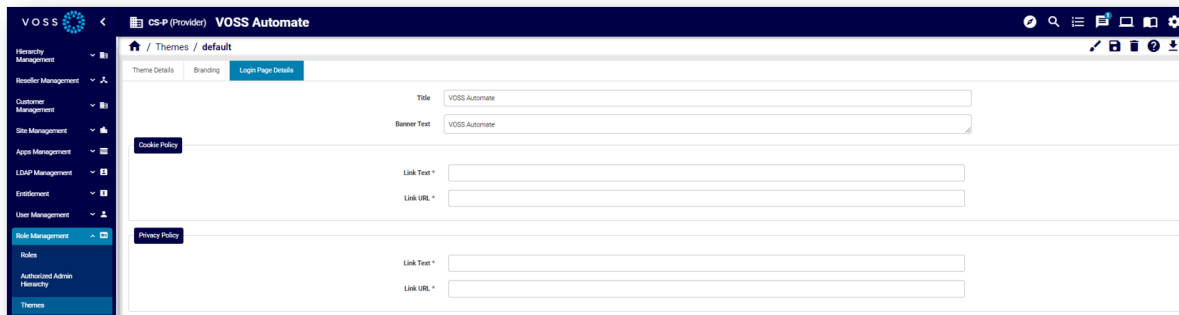
Image details:

- **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.



13.2.6. Theme Element Color References for the Administration Portal

Note:

- Color selection on the **Branding** tab of a theme *always* affects the Admin and Business Admin Portal.
- Color selection on the **Branding** tab of a theme *only* affects the Legacy Admin Portal *if no theme file* is attached to the theme.

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 #.

Administration 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	#ffffff	The color used for all the panels in the app.

Title	Field Name	Default Value (Hex)	Notes
Panel Text Color	panel_text_colour	#414042	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_colour	#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_colour	#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:

Primary Colour	#0a660c	
Primary Text Colour	#080808	
Accent Colour	#fff700	
Accent Text Colour	#7340db	
Topbar Colour	#77ff00	
Topbar Text Colour	#f20c0c	
Menu Colour	#a6f5d7	
Menu Text Colour	#121010	
Panel Colour	#00ddff	

Panel Text Colour	#121111	
Background Colour	#008cff	
Info Notification Colour	#004dff	
Info Notification Text Colour	#ede8e8	
Success Notification Colour	#ffd000	
Success Notification Text Colour	#0f0e0e	
Warning Notification Colour	#e86666	
Warning Notification Text Colour	#121111	
Error Notification Colour	#6e0b0b	
Error Notification Text Colour	#ede6e6	

Favicon		+ Choose
Logo	coverimageb.png 	+ Choose
Login Logo		+ Choose
Login Background		+ Choose
Menu Background		+ Choose

Note:

- For details on images and logos, see: *Manage Themes (Admin Portal and Business Admin Portal)*.
- If a color value appears blank, default values apply.
- Sub-menu and sub-sub-menu backgrounds are rendered as percentages of the Menu Colour.

Admin Portal

The dashboard features a left-hand navigation menu with the following items: Apps Management, LDAP Management, Entitlement, User Management, Role Management (highlighted), Roles, Themes, Menu Layouts, Menu Diff Tool (Portal only), and Landing Pages. The main content area includes a header with 'CS-P (Provider) VOSS Automate Provider', a search bar, and notification icons. Below the header, there is a 'This is the Header Text' section followed by 'This is the Line Text'. Two large green widgets display 'Land 9' and 'Hierarchy 36'. The bottom section is divided into 'General Administration' (with 'List Transactions' and 'Bulk Load' buttons) and 'Configure Devices' (with buttons for 'Configure CUCMs', 'Configure CUCs', 'Configure CUPs', 'Configure CERs', 'Configure WebEx', and 'Configure IOS').

The 'Field Display Policies' page shows a table with 480 rows. The table has columns for 'Name' and 'Description'. The 'Name' column includes a search filter. The table lists several policies, with 'AdminUser' and 'BundleFDP' highlighted in blue. Other policies include 'AddCustomerAdmin_FDP', 'AzureAD_MsolUser_FDP', 'BasicDataSync', 'BasicDataSyncSchedule', 'BusinessAdmin_Assoc_1_To_N_FDP', 'BusinessAdmin_Assoc_N_To_N_FDP', and 'BusinessAdminCallPickupGroupFDP'. The 'BusinessAdmin_Assoc_1_To_N_FDP' and 'BusinessAdmin_Assoc_N_To_N_FDP' policies have descriptions: 'Default 1 to N number association Display Policy for the f' and 'Default N to N number association Display Policy for the l' respectively. The table also shows 'Updated - 13Oct2021' for the 'AzureAD_MsolUser_FDP' policy.

The screenshot displays the VOSS Admin console interface. On the left is a navigation sidebar with categories like 'Apps Management', 'LDAP Management', 'Entitlement', 'User Management', 'Role Management', 'Customizations', 'Global Settings', 'Subscriber Profiles', 'Model Filter Criteria', 'Flow Through Provisioning Criteria', 'Field Display Policies', 'Configuration Templates', 'Business Admin Portal Profiles', and 'Self Service Feature Display Policies'. The 'Field Display Policies' section is currently active.

The main content area shows the configuration for a specific Field Display Policy:

- Name ***: BusinessAdmin_Assoc_1_To_N_FDP
- Description**: Default 1 to N number association Display Policy
- Target Model Type ***: relation/HcsDNMultiE164AssociateREL

Below the policy details is a 'Groups' section with a dropdown menu set to 'External'. Underneath, there are configuration options for the group:

- Title ***: External
- Display as Fieldset**:
- Number of Columns**: 0

At the bottom, there is a 'Fields' section with two columns: 'Available' and 'Selected'. The 'Available' column contains a search bar and two items: 'dn_number' and 'members.e164_number'. The 'Selected' column contains a search bar and one item: 'members'.

Business Admin Portal

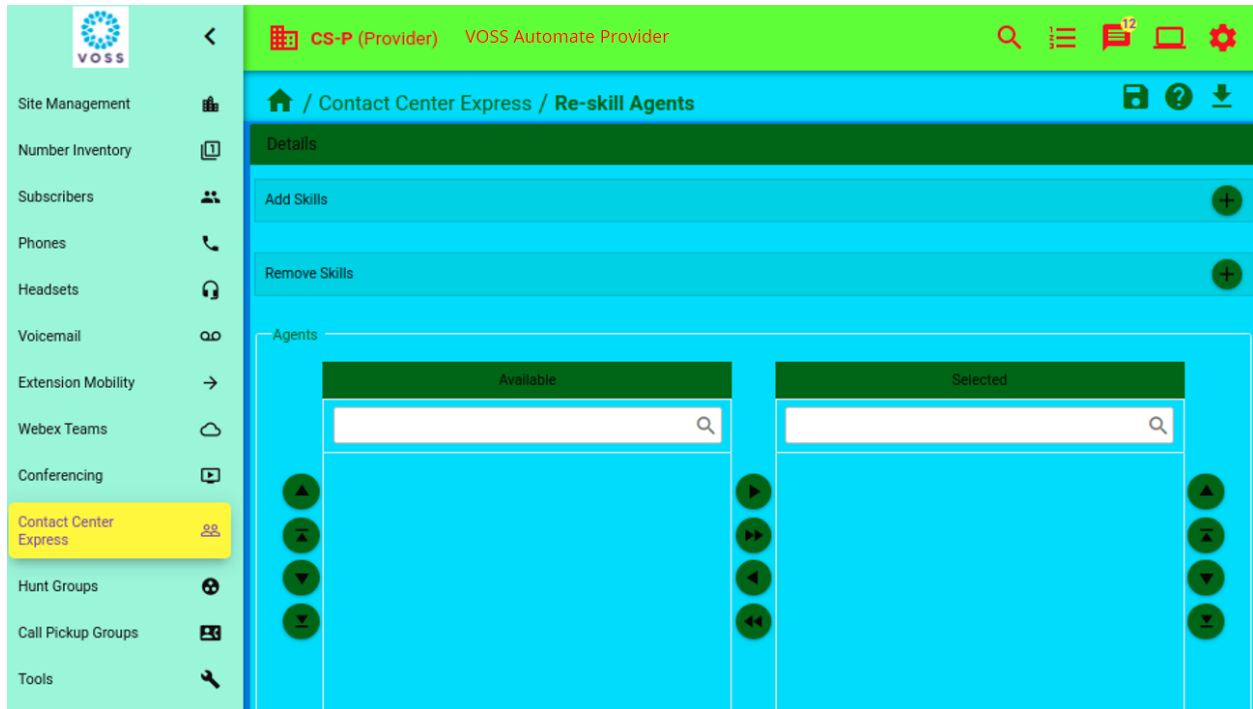
The screenshot displays the Business Admin Portal interface. On the left is a sidebar menu with the following items: Site Management, Number Inventory, Subscribers, Phones, Headsets, Voicemail, Extension Mobility, Webex Teams, Conferencing, Contact Center Express, Hunt Groups, Call Pickup Groups, and Tools. The top navigation bar shows 'CS-P (Provider)' and 'VOSS Automate Provider' with search, list, notification (12), and settings icons. The main content area features a home icon, a home button, and three statistics cards: Sites (27), Subscribers (277), and Phones (271). Below these are sections for Saved Searches (with a search query 'Subscribers: User Id contains 'john'' and a refresh icon) and Quick Actions (with buttons for View Subscribers, Add Subscriber, View Phones, Add Phone, Reset Pin / Password, Login User / Phone, and Logout Phone).

CS-P (Provider) VOSS Automate Provider

Home / Tools / Transaction Log

Id	Action	Username	Status	
54146	Create User Saved Search	CS-PAdmin	Success	Subscribers:
54136	Update Hcs Analog Gateway Rel	CS-PAdmin	Success	SKIGW12341
54132	Addendpoints Hcs Analog Gateway Rel	CS-PAdmin	Success	SKIGW12341
54123	Update Hcs Analog Gateway Rel	CS-PAdmin	Success	SKIGW12341
54122	Create Theme	system	Success	test
54115	Update Hcs Analog Gateway Rel	CS-PAdmin	Success	SKIGWEE123
54112	Execute Event	system	Success	GS_FMCv2_I
54104	Execute Event	system	Success	GS_FMCv2_I
54101	Execute Event	system	Success	GS_FMCv2_I
54061	Execute Event	system	Success	GS_FMCv2_I
54053	Execute Event	system	Success	GS_FMCv2_I
54050	Execute Event	system	Success	GS_FMCv2_I
53958	Execute Event	system	Success	GS_FMCv2_I
53938	Execute Event	system	Success	GS_FMCv2_I
53913	Execute Event	system	Success	GS_FMCv2_I
53908	Execute Event	system	Success	GS_FMCv2_I
53905	Execute Event	system	Success	GS_FMCv2_I
53897	Execute Event	system	Success	GS_FMCv2_I
53892	Execute Event	system	Success	GS_FMCv2_I
53889	Execute Event	system	Success	GS_FMCv2_I
53779	Update Hcs Analog Gateway Rel	CS-PAdmin	Fail	SKIGWEE123

1 < > 2 3 4 5 >
200



13.2.7. Login 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 - see *Customize Login Page Theme and Text in the Legacy Admin Portal*.

13.3. Menu Layouts and Landing Pages

13.3.1. Menu Layouts

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.

VOSS Automate allows an administrator (with appropriate permissions) to customize menu layouts for different user roles and hierarchy levels. 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.

Note: This topic describes functionality as displayed in the Admin Portal. The look and feel of landing page and menu layout configuration options may differ in the legacy Admin GUI.

The screenshot shows the VOSS Automate Admin Portal interface. The sidebar on the left contains navigation options: Hierarchy Management, Reseller Management, Customer Management, Site Management, Apps Management, LDAP Management, Entitlement, User Management, Role Management (highlighted), Roles, Themes, Menu Layouts, and Menu Diff Tool (Portal only). The main content area is titled 'Menu Layouts / HcsProviderMenu'. It features a form with 'Name *' set to 'HcsProviderMenu' and an empty 'Description' field. Below the form is a table titled 'Menu Items' with the following data:

		Menu Items	Filters	Icon	Title	Description	Condition	Type	Href
☰	+ 🗑️	+	Y	🗑️	Hierarchy Management				
☰	+ 🗑️	+	Y	👤	Reseller Management				
☰	+ 🗑️	+	Y	🗑️	Customer Management				
☰	+ 🗑️	+	Y	🏠	Site Management				
☰	+ 🗑️	+	Y	📱	Apps Management				
☰	+ 🗑️	+	Y	👤	LDAP Management				
☰	+ 🗑️	+	Y	📄	Entitlement		{{ macro.is_cisco_cucm_enabled }}		

Related Topics

- Navigation - Menu and Landing Pages in the Best Practices Guide
- Advanced Configuration Guide
- Fixed and Configurable Filters in Menus and Landing Pages in the Core Feature Guide
- Macros in VOSS Automate in the Core Feature Guide
- Custom Icon Names Reference in the Core Feature Guide
- Landing Pages in the Core Feature Guide
- Custom Components 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.

Home / Menu Layouts / HcsProviderMenu

Name *

Description

Menu Items											
		Menu Items	Filters	Icon	Title	Description	Condition	Type	Href	Field Display Policy	Configuration Template
					Hierarchy Management						<input type="text"/>
					Reseller Management						<input type="text"/>
					Customer Management						<input type="text"/>
					Site Management						<input type="text"/>

Filter (contains)

- ucprep_DateTimeGroup-Reference-YMD
- ucprep_DateTimeGroup-Reference-MDY
- HcsVossCER_Cluster_VirtualCFT

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 and Landing Pages](#)

Fixed Filters

⌵ +

▼ No value set

Filter By

Filter Type

Filter String

Ignore Case

Configurable Filters

⌵ +

▼ No value set

Filter By

Filter Type

Filter String

Ignore Case

Default Menu Layouts

VOSS 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 menu, 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 VOSS Automate documentation is based on the default, predefined menu layouts that ship with the system.

To work with menu layouts in the Admin Portal (via the default menus):

- Go to **Role Management > Menu Layouts** to view and edit menu layouts.
 - Go to **Role Management > 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, VOSS Automate provides best practice menus for Provider and Customer administrators, including the associated access profiles and landing pages.

The best practice menus are more business-oriented, and include additional options based on best practice adaptations that may also be included in VOSS Automate.

The table describes the key features of the best practice menus:

Feature	Description
Structure mapped to business use case	<p>A menu order, nesting and naming convention based on common business use.</p> <p>Menus are ordered 'top-down, following the logical order of tasks and the system hierarchies that perform these tasks.</p> <p>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.</p> <p>In a similar way, the Cisco Subscriber Services menu has sub menus for all the functionality associated with Cisco subscribers in VOSS Automate.</p>
Naming convention	<p>First word capitalized for menu names where the menu is for a <i>form view</i> (input or edit). For example ADD Internal Number Inventory</p> <p>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.</p>
Menus for URLs	<p>Included in the structure are menus that provide links to other VOSS Automate portals, allowing you to launch a another portal directly from a menu.</p> <p>For this to work, you must update these URLs to match your configuration.</p>

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 or Edit a Field Display Policy](#).
- 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 mense, see [Access Profile Permissions and Operations](#).
- Note the landing pages available for the best practices menus. See the list under the **Landing Pages** menu.

Menu Items Requiring Adaptations

The table lists the menus for specific adaptations:

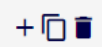
Note: Not all adaptations may be available on your system. If you wish to use any of these menus, please contact the VOSS team.

Menu	Sub Menu	3rd level menu	Adaptation
VOSS Phone Server Management	VOSS Phone Server VOSS Phone Adaptive Dial Plan		VOSS Phone Server
Customer Management	Contact Centre Services	<ul style="list-style-type: none"> • CC Users • CC User Preferences • CC User CFTs (with GS_CCUser filter) 	ContactCentre-VoiceRecording User
HCS Dial Plan Management	HCS Dialplan Additions HCS Group CLI	<ul style="list-style-type: none"> • Dialplan Additions • Dialplan Addition Templates • Dialplan Additions CFTs (GS_DialplanAdditions filter) • Dialplan Additions CFTs (ENT_Filter) • CustSCode-PT Translation Patterns • External Group CLI Inventory • External Group CLI Association • Internal Group CLI Inventory • Internal Group CLI Association • ExternalGroupCLI-PT Calling Party Transforms 	Dialplan Additions Group CLI
Site Management	Advanced Site Functions	SameDialplanOB 8XData	Overbuild Same Dialplan AddSite
Number Management	(N to 1) DN to E164 Associations with Update		N to 1 E164 Association Update Support
Number Management	ADD Multi-step Number Inventory		Number Inventory Mgmt - Multi-Step
Cisco Subscriber Services	Add Lines to Pickup Group		Pickup Group Membership
Cisco Subscriber Services	<ul style="list-style-type: none"> • Change Line • Change Line Profiles • Change Line Instance Profiles 		Change Line
Cisco Subscriber Services	Line Recording		Line Recording

Menu	Sub Menu	3rd level menu	Adaptation
Cisco MACD Functions	<ul style="list-style-type: none"> • FAC Code Management • Sync FAC Codes Across Clusters 		Enhanced ForceAuthenticationCode Support
Multi- Vendor Services	VOSS Phones		VOSS Phone Server
Audit Tools	VOSS Day 2 Customer Audit Tool		Audit Tool
Overbuild Tools	RUN EM-User Overbuild		Audit Tool
Overbuild Tools	E164 TPs AND TRANSFORM Move Tool		DN Overbuild

Add or Edit a Menu Layout

This procedure adds new menus and updates 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 (default menus) **Role Management > Menu Layouts**.
4. Choose an option:
 - To create a new menu layout based on settings in an existing menu layout (recommended), click on a menu layout you want 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 the settings for the clone to create the new custom menu layout.
 - To 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.
 - To edit an existing menu layout, click on the menu layout you wish to edit, make your changes, and save. Updates display only once you've logged out and logged in again.
5. At **Name** and **Description**, fill out a name and description for the new menu layout.
6. At **Menu Items**, configure the main menus and sub menus. You can make the following changes:
 - Re-order menus
 - Add, clone, or delete rows for main menus and nested sub menus.
 - Add, clone, or delete sub menus (click the Plus icon in the **Menu Items** column to display nested sub menus)

Menu Items								
		Menu Items	Filters	Icon	Title	Description	Condition	Type
☰	+ 📄 🗑️	∨	🔍	📊	Hierarchy Management			

Menu Items							
		Menu Items	Filters	Title	Description	Condition	Type
☰	+ 📄 🗑️	+	🔍	Hierarchy			relation/HcsHierarchyNodeREL
☰	+ 📄 🗑️	+	🔍	Delete Intermediate Node			view/HcsDeleteIntermediateNodeVIEW
☰	+ 📄 🗑️	+	🔍	Localization Language			data/LanguageDefault

- Configure fixed and configurable filters
- Choose a menu icon (for main menus only)

Menu Items					
		Menu Items	Filters	Icon	Title
☰	+ 📄 🗑️	∨	🔍	📊 Business	Hierarchy Management

Filter (contains) 🔍

- 🐛 Bug Report
- 🔧 Build
- 📊 Burst Mode
- 📊 Business

- Add or edit a menu title
- Provide a menu description
- Specify a condition that defines when the menu displays
- Choose a model type
- Create internal or external href links
- Choose a FDP (field display policy) and/or a CFT (configuration template)
- Choose a custom component
- Choose the landing page to associate with the menu item
- Choose how a menu or sub menu displays, for example, list, form, or landing page

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 details around each of these configuration options, see [Menu Layouts Field Reference](#).

7. Click **Save** to add the new menu layout.
8. Assign the menu layout to the appropriate roles.

Menu Layouts Field Reference

This section describes menu layout configuration options:

Note: You can view, add, and edit menu layouts in the Admin Portal via (default menus) **Role Management > Menu Layouts**. 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:

Column	Description
Reorder	Click on the reorder icon 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.
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: <ul style="list-style-type: none"> • 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 to associate with the menu item. <hr/> Note: The model type defines the available custom components. <hr/>

Column	Description
Href	<p>Click in the cell to specify a path as a direct reference to a model type used for the menu item.</p> <p>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: <i>api/relation/SubscriberPhone/add</i></p> <p>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.</p> <p>It is recommended that you do not use hrefs to reference <i>view/</i> type models.</p>
Field Display Policy	<p>Click in the cell to choose a FDP (field display policy) to associate with the menu.</p> <hr/> <p>Note: FDPs cannot be used with custom components.</p> <hr/>
Configuration Template	<p>Click in the cell to choose a CFT (configuration template) to associate with the menu.</p>
Custom Components	<p>Click in the cell to choose an Admin Portal custom components. Options in the drop-down depend on the model you choose in the Type field. For example, when choosing model type <i>view/AddPhone</i>, the custom component available for selection is Add Phone. The custom components allow you to display GUI content (such as landing pages, lists, and forms) in the same layout as they appear in the Business Admin Portal.</p> <p>Custom components are also available for multi vendor environments and for Microsoft-only environments. This feature is only available in the new VOSS Automate Admin Portal.</p>

Column	Description
Landing Page	Click in the cell to choose a landing page to display, when the Display As option for the menu item is set to Landing Page . This option is only available in the new VOSS Automate Admin Portal. Note that sub menus cannot be selected as landing pages, and landing pages do not have context-sensitive help.
Display As	<p>Click in the cell to choose how the menu item should display. The default is <i>List</i>.</p> <p>Options are: List, Landing Page, Form, External Link, Tree</p> <ul style="list-style-type: none"> • List (default) <ul style="list-style-type: none"> 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 • Landing Page <ul style="list-style-type: none"> Allows you to choose an existing landing page, which will display when this menu item is chosen. This option is <i>only</i> available in the VOSS Admin Portal GUI. • Form (for a single instance) <ul style="list-style-type: none"> 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 view/ model types always open the <i>Add</i> form; thus, if used, the value should not have the /add/ endpoint, for example, as in this JSON: <pre data-bbox="639 1182 1097 1335"> { "type": "view/QuickSubscriber", "display": "form", "title": "Quick Add Subscriber" } </pre> • External Link <ul style="list-style-type: none"> Recommended for use with href, where 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) <ul style="list-style-type: none"> Choosing a Tree display shows a tree view of the resource. When using href with Tree display, the href provides the tree path.

Related Topics

- [Fixed and Configurable Filters in Menus and Landing Pages](#)
- [Landing Pages](#)
- [Add or Edit a Landing Page](#)
- [Custom Components](#)

13.3.2. Menu Diff Tool

Note: This feature is available only in the VOSS Automate Admin Portal. It is not available in the Legacy Admin Portal.

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 that is copied contains sub-menus, these are included.

Click **Save** to save changes in the target menu.

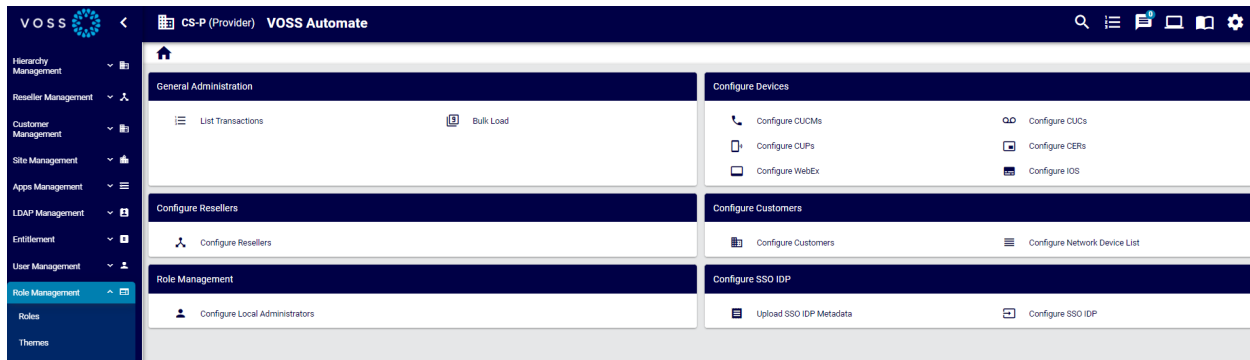
13.3.3. Landing Pages

Overview

A landing page is the page you see when you log in, or when clicking the **Home** button from anywhere in the system, or when choosing a menu item that has been defined as a landing page.

A default landing page ships with the system, and is associated with pre-defined roles in the hierarchy, for example Provider, Customer, and Site administrators.

Note: This topic describes functionality as displayed in the Admin Portal. The look and feel of landing page and menu layout configuration options may differ in the classic Admin GUI.



Customized Landing Pages

Landing pages may be customized for different user roles, and have several configuration options:

- Add shortcut links to frequently used functionality
- Enhance the look and feel on the user's Admin Portal
- Add images and links in vertical or horizontal patterns with unlimited boxes and shortcuts

Editable landing pages provide a way to set up direct links to areas in the system, which can be used as short-cuts by the administrators in line with their role.

Existing images can be used or new images can be added in line with branded look and feel.

You may clone (copy) existing landing pages and then create a new landing page based on pre-populated settings, or the landing page can be exported, edited externally, and then re-imported. Designers with access to the tag function can use tag versions to uniquely identify different landing pages, and to track and control changes.

The CSS of the Theme can be used to control the layout of the landing page.



Related Topics

- Menu Layouts in the Core Feature Guide
- Advanced Configuration Guide
- Macros in VOSS Automate in the Core Feature Guide
- Fixed and Configurable Filters in Menus and Landing Pages in the Core Feature Guide
- Custom Icon Names Reference in the Core Feature Guide
- Custom Components for Menu Layouts and Landing Pages in the Core Feature Guide

Add or Edit a Landing Page

This procedure adds a new landing page or edits an existing landing page.

1. Log in to the Admin Portal as a Provider administrator, or higher.
2. Choose the hierarchy level for the landing page, for example, Customer.
3. Go to (default menu) **Role Management > Landing Pages**.
4. Choose an option:
 - To create a new landing page based on settings in an existing landing page (recommended), click on the relevant landing page to open its editing screen, then click **Clone**. Now modify the settings of the cloned landing page and save it as a new landing page.
 - To edit an existing landing page, click on the landing page in the list view to open its editing screen, update its settings, and save your changes.
5. On the **Details** tab, configure the following options for the landing page:

Note:

- For configuration details, see [Landing Pages Field Reference](#)
 - Rows with nested 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.
-

- Add a name
- Configure meta tasks (button text, model type, Href, FDP, CFT, display format, filters)
- Configure counters (filters, icon, title, model type, FDP, CFT).
- Configure sections, and links in sections.

6. On the **Welcome Header**, configure the following options:

Note:

- Header text
 - Line text
-

7. Save the landing page.

8. Assign the landing page to the relevant roles.

Landing Pages Field Reference

This section describes landing page configuration options:

Note: You can view, add, and edit landing pages in the Admin Portal via (default menus) **Role Management > Landing Pages**. See [Add or Edit a Landing Page](#)

You can select the following tabs on the Landing Pages add/edit screen:

- Details tab
- Welcome Header tab

Details Tab

The Details tab defines the following options for the landing page:

Column	Description
Name	The name of the landing page.
Meta Tasks	These rows display the shortcut buttons (one or more) at the top of the home page screen (directly below the line text, if configured). Click in the row to edit an existing shortcut button, or click the Plus icon (+) to add a new shortcut button.
Counters	These rows display the model-type instance counts (one or more) that display on the landing page. Click in a row to edit an existing counter, or click the Plus icon (+) to add a new counter.
Sections	These rows display the sections (one or more) that display as blocks on the landing page. Click on an item to edit it, or click the Plus (+) icon to add a new section. Use the hamburger icon to re-order the sections.
Links	Configures links in sections on landing pages.

Common functionality

The table describes edit functionality typically available for landing page elements:

Column	Description
Reorder	Click on the reorder icon in the relevant row to change the location of a landing page element.
Add, clone, or delete row	Click an icon to either add a row, clone (copy) a row, or to delete the row.
Type	The model type to associate with the landing page element. Blank when href field is populated. The model type shows the related FDPs (field display policies) and CFTs (configuration templates) that can be applied.
Href	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, (example API URL for a list of items of type relation/SubscriberPhone) the Add Phone page would have the following href (API URL): api/relation/SubscriberPhone/add In this case, you'll need to use JSON-format landing page import, or bulk load, to add any associated field display policies (FDPs) and configuration templates for the menu item. The recommendation is not to use Hrefs to reference view/ type models. Href is a direct reference to a model type (the path), if applicable. If used, the Type field is empty.
Field Display Policy	The field display policy associated with the landing page element.
Configuration Template	The configuration template associated with the landing page element.

Meta Tasks

The table describes Meta Tasks configuration options:

Column	Description
Button Text	Text for the button.

Counters

The table describes configuration options for Counters:

Column	Description
Icon	The icon to be used for this counter.
Title	Mandatory. The title to be displayed for this counter, for example, <i>Phones, Users</i> .

Sections

The table describes configuration options for Sections:

Column	Description
Links	Displays a Links table where you can configure links in the section.
Title	Mandatory. The section title as it will show on the Landing page.
Image URL	Optional URL image to be displayed as section image. For example, let's say a theme is uploaded with landing page images, and the theme folder has a subfolder with the following file: <i>mytheme/img/landingpage/landing1.png</i> In this case, the URL would be: <i>/www/themes/mytheme/img/landingpage/landing1.png</i>
Condition	Click in the cell to add or edit a macro that allows you to display/hide the section, based on a condition specified in a macro. If the macro evaluates to true, the section displays, else, when false, the section is hidden. The default is true (sections you add display by default). See the Advanced Configuration Guide for more information about using macros.

Links

The table describes configuration options for Links in sections on a landing page:

Column	Description
Filters	Click the filter icon in the relevant row to display a dialog where you can choose fixed and configurable filters for the link. Fixed filters cannot be removed. The following options are available for configurable filters for links: <ul style="list-style-type: none"> • Columns (Displays only when <i>Display As</i> option is <i>Inline List</i>, and the value for <i>Display Multiple Columns</i> is set to <i>Yes</i>) • Filter By • Filter Type • Filter String
Icon	The icon to use for the link. Click in the cell to choose an icon. Icons display in the drop-down with a descriptive name.
Display Multiple Columns	Available only when Display As option is <i>Inline List</i> . Defines whether the link displays as multiple columns. When set to <i>Yes</i> (select the checkbox in the field), you can set column values in the filters for this link. When set to <i>No</i> , the filters do not have an option to specify columns.
Link Text	Mandatory. Text for the link.

Column	Description
Condition	Optional. Specify a macro as a condition to define whether the link displays on the landing page. If the macro evaluates to True (default), the link displays. See the Advanced Configuration Guide for more information about using macros as conditional criteria.
Href	If a direct reference to a model type is used for the menu item, the specified path.
Custom Component	Click in the cell to choose an Admin Portal custom components. Options in the drop-down depend on the model you choose in the Type field. For example, when choosing model type <i>view/AddPhone</i> , the custom component available for selection is Add Phone . The custom components allow you to display GUI content (such as landing pages, lists, and forms) in the same layout as they appear in the Business Admin Portal. Custom components are also available for multi vendor environments and for Microsoft-only environments. This feature is only available in the new VOSS Automate Admin Portal.

Column	Description
Display As	<p>Click in the cell to choose how the menu item should display. The default is <i>List</i>.</p> <p>Options are: List, Landing Page, Form, External Link, Tree</p> <ul style="list-style-type: none"> • List (default) <ul style="list-style-type: none"> 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 • Inline List <ul style="list-style-type: none"> The link points to the first five list of items. When choosing this option, you can choose Yes or No for option Display as Multiple Columns. When set to Yes, you can define columns in the filters for this link. • Landing Page <ul style="list-style-type: none"> Allows you to choose an existing landing page, which will display when this menu item is chosen. This option is <i>only</i> available in the VOSS Admin Portal GUI. • Form (for a single instance) <ul style="list-style-type: none"> Displays an input form (for an Href resource value other than view/models, a resource ends with /add/). 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 view/ model types always open the <i>Add</i> form; thus, if used, the value should not have the /add/ endpoint, for example, as in this JSON: <pre data-bbox="639 1266 1097 1419"> { "type": "view/QuickSubscriber", "display": "form", "title": "Quick Add Subscriber" } </pre> • External Link <ul style="list-style-type: none"> Recommended for use with href, where 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) <ul style="list-style-type: none"> Choosing a Tree display shows a tree view of the resource. When using href with Tree display, the href provides the tree path.

Related Topics

- [Fixed and Configurable Filters in Menus and Landing Pages](#)
- [Landing Pages](#)
- [Add or Edit a Landing Page](#)
- [Custom Components](#)

Welcome Header Tab

The table describes the fields on the Welcome Header tab for landing page configuration:

Field	Description
Header Text	A single line static welcome message displayed at the top of the landing page.
Line Text	Text for the welcome line displayed under the header. Use [user-role] as a placeholder to insert the current user's role, to serve as the header. For example: /www/img/landingPageIcons/User.png

13.3.4. Custom Components

Overview

Custom components allow you to display GUI content (such as landing pages, lists, and forms) in the same layout as they appear in the Business Admin Portal.

Custom components are used to generate menu items and landing pages with the look and feel and functionality of the Business Admin Portal. This allows you to view content in the Admin Portal in what may be termed, 'Business Admin Portal mode'. However, some functionality, such as forms that open when clicking a link to lines for example, display in standard, 'Admin Portal mode'. Thus, depending on the type of resource you're viewing, the system may switch between 'Business Admin Portal mode' and 'Admin Portal mode'.

Important:

- Custom components are only available in the VOSS Automate Admin Portal (not in the legacy Admin Portal).
- At the time of writing (21.3), for menus or landing pages generated via custom components, it is not possible to assign a field display policy (FDP) to show or hide fields on the page that displays. By default, all fields display on pages associated with custom-component generated menu items or landing pages. The ability to assign FDPs for custom components is reserved for future development.

Related Topics

- [Add or Edit a Menu Layout](#)
- [Add or Edit a Landing Page](#)

Model Types and Associated Custom Components

The table describes the custom components available for menu layouts and landing pages:

Note:

- On forms where you select a custom component, the **Type** field refers to the model type. A model type may be associated with one or more custom components. Once you choose the model type, the **Custom Component** drop-down displays the custom components available for that model type. Leave the **Type** field blank if you wish to use a dashboard custom component.
 - You can use the value in the **Route** column (in the following table) to inspect the component appearance. Refer to the URL endpoints of Business Admin Portal menu items that match the **Route** value.
-

Important: At the time of writing (21.3), all custom components for *edit* functionality are reserved for future development. This includes all custom components where the custom component name or route includes the text, *edit*. For example, Add/Edit Extension Mobility (custom component) and /extension-mobility/edit-extension-mobility (route).

Type	Custom Component	Route
view/AddPhone	Add Phone	/phone/add-phone
view/AddSubscriberFromProfile	Add Subscriber	/subscribers/add-subscriber
relation/PexipConference	Add/Edit Conferencing	/conferencing/form-conferencing Edit is reserved for future development.
relation/SubscriberDeviceProfile	Add/Edit Extension Mobility	/extension-mobility/edit-extension-mobility Edit is reserved for future development.
relation/HuntGroupRelation	Add/Edit Hunt Group	/hunt-group/edit-hunt-group Edit is reserved for future development.
relation/Voicemail	Add/Edit Voicemail	/voicemail/edit-voicemail Edit is reserved for future development.
relation/SparkUser	Add/Edit Webex App	/webex-teams/form-webex-teams Edit is reserved for future development.
view/BulkAddUser	Bulk Add Subscribers	/subscribers/bulk-add-subscribers
	Call Pickup Group Dashboard	/call-pickup-group
	Conferencing Dashboard	/conferencing
	Contact Center Express Dashboard	/contact-center

Type	Custom Component	Route
relation/LineRelation	Edit Line	/number-management/edit-line Edit is reserved for future development.
relation/SubscriberPhone	Edit Phone	/phone/edit-phone Edit is reserved for future development.
relation/HcsSiteREL	Edit Site	/site/edit-site Edit is reserved for future development.
relation/Subscriber	Edit Subscriber	/subscribers/edit-subscriber Edit is reserved for future development.
	Extension Mobility Dashboard	/extension-mobility
	Headset Dashboard	/headsets
	Hunt Group Dashboard	/hunt-group
view/UserPhoneMoveUsers_VIEW	Move Subscriber	/subscribers/move-subscriber
relation/MultiVendorSubscribers	Multi-Vendor Subscribers List	/subscribers/list-mv-subscribers
	Number Inventory Dashboard	/number-management
	Phone Dashboard	/phone
	Site Management Dashboard	/site
	Subscriber Dashboard	/subscribers

Type	Custom Component	Route
relation/Subscriber	Subscribers List	/subscribers/list-subscribers
	Tools Dashboard	/tools
	Voicemail Dashboard	/voicemail
	Webex App Dashboard	/webex-teams

Custom Component Example

This section displays the output for a custom component used for the following scenario:

- Model type: relation/Subscriber
- Custom component name: Subscribers List
- Menu title: List Subscriber

Menu item added via custom component

The image displays an example of a new menu item titled *List Subscriber*, which uses model type *relation/Subscriber* and custom component *Subscribers List*.

In this case, although you're viewing a Subscriber list in the Admin Portal, notice the Business Admin Portal style graphic icons that display in the **Phones** column and in the **Services** column.

Username	First Name	Last Name	Email	User Type	Entitlement Profile	Primary Extension	Phones	Services
acarstel01	Andy	Carstel	acarstel01@ab-group.com	End User	AB_Group-Standard-EP			
adervers01	Andy	Dervers	adervers01@ab-group.com	End User	AB_Group-Standard-EP			
fgertrand01	Frances	Gertrand	fgertrand01@ab-group.com	End User	AB_Group-Standard-EP			
fgourand01	Freya	Gourand	fgourand01@ab-group.com	End User	AB_Group-Standard-EP			
jbrown	Jim	Brown	jbrown@ab_berlin.com	End User	AB_Group-Standard-EP			
jpeters01	James	Peters	jpeters01@ab-group.com	End User	AB_Group-Standard-EP			
kbrown	Kevin	Brown	kbrown@ab_berlin.com	End User	AB_Group-Standard-EP			
kfurmer01	Kris	Furmer	kfurmer01@ab-group.com	End User	AB_Group-Standard-EP			
mvalder01	Mable	Valder	mvalder01@ab-group.com	End User	AB_Group-Standard-EP			
nfervier01	Neal	Fervier	nfervier01@ab-group.com	End User	AB_Group-Standard-EP			

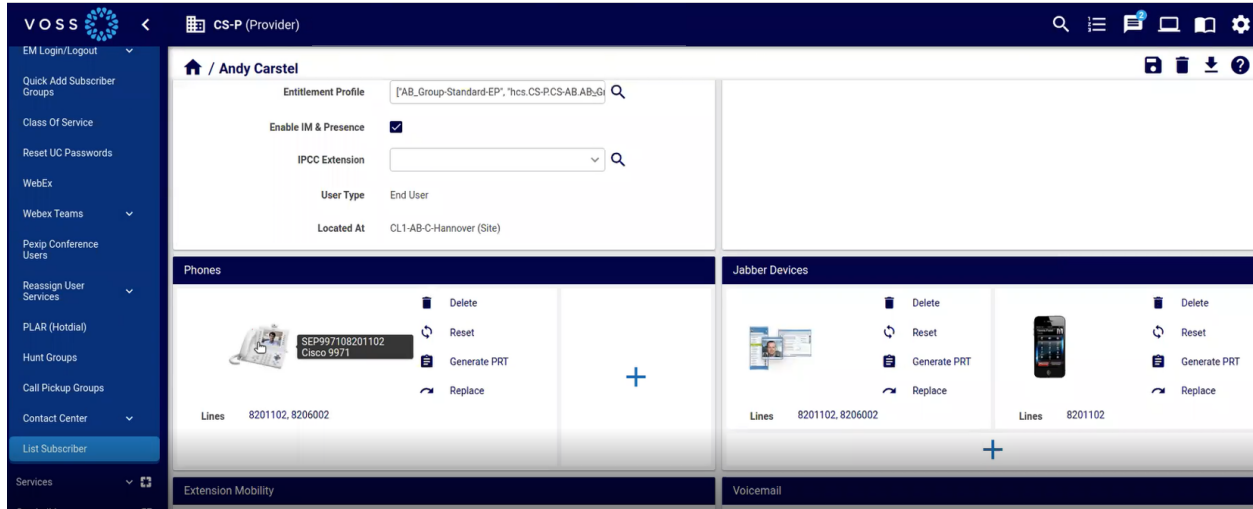
While a menu item added via a custom component displays the content of the list view with the look and feel of the Business Admin Portal, compare this with the following image, which displays the Subscriber list view of the standard Admin Portal.

User Id	First Name	Last Name	Email	Role	Entitlement Profile	Sync Type	User Type	Auth Method	Line
acarstel01	Andy	Carstel	acarstel01@ab-group.com	CL1-AB-C-HannoverSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
adervers01	Andy	Dervers	adervers01@ab-group.com	CL1-AB-C-RennesSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
fgertrand01	Frances	Gertrand	fgertrand01@ab-group.com	CL1-AB-C-GrenobleSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
fgourand01	Freya	Gourand	fgourand01@ab-group.com	CL1-AB-C-GrenobleSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
jbrown	Jim	Brown	jbrown@ab_berlin.com	CL1-AB-C-BerlinSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
jpeters01	James	Peters	jpeters01@ab-group.com	CL1-AB-C-GrenobleSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
kbrown	Kevin	Brown	kbrown@ab_berlin.com	CL1-AB-C-BerlinSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
kfurmer01	Kris	Furmer	kfurmer01@ab-group.com	CL1-AB-C-GrenobleSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
mvalder01	Mable	Valder	mvalder01@ab-group.com	CL1-AB-C-GrenobleSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
nfervier01	Neal	Fervier	nfervier01@ab-group.com	CL1-AB-C-RennesSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
nkasperson01	Neal	Kasperson	nkasperson01@ab-group.com	CL1-AB-C-HannoverSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C
rjosephe01	Ronald	Joseph	rjosephe01@ab-group.com	CL1-AB-C-GrenobleSelfService	AB_Group-Standard-EP	CUCM-Local	End User	Automatic	CL1-AB-C

Detail view of resource

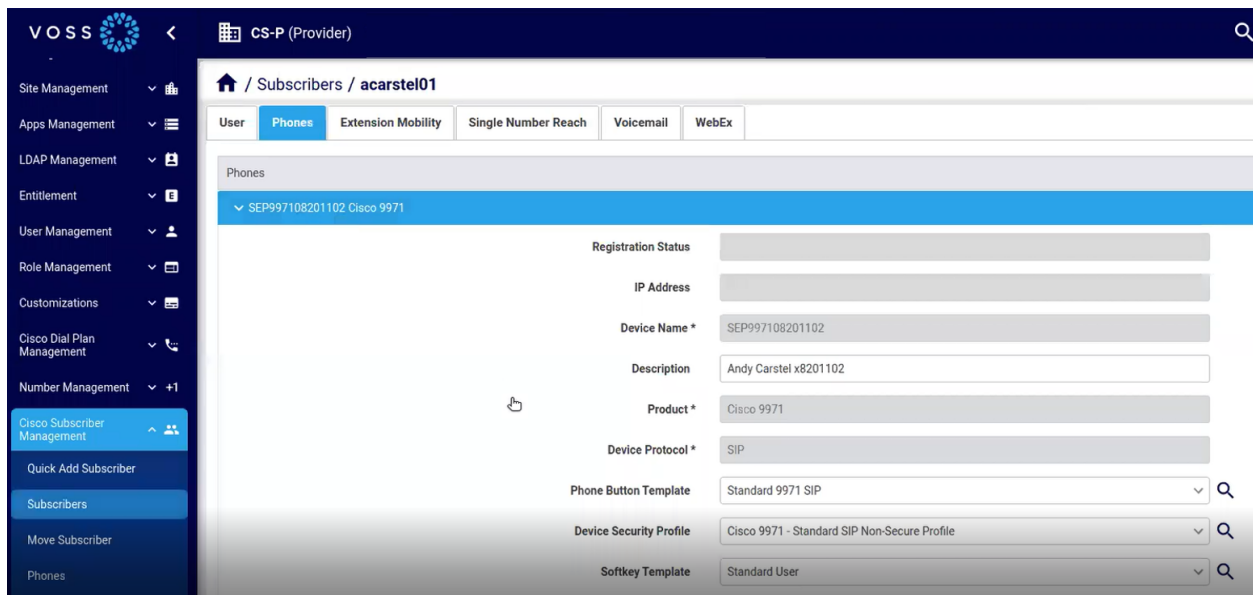
The image displays the detail view of a resource accessed from the list view of a custom component generated menu item (List Subscriber), which retains the look and feel of the Business Admin Portal.

Note: An exception exists, where links on forms display the standard Admin Portal view of the resource. For example, clicking on the Line link from the subscriber detail view opens the resource in Admin Portal mode (that is, it no longer has the Business Admin Portal look and feel).



While the detail view of a resource from a custom component generated menu item has the look and feel of the Business Admin Portal, compare the detail view display in the standard Admin Portal.

The image displays the detail view of a subscriber selected from the standard Subscribers list view in the Admin Portal:

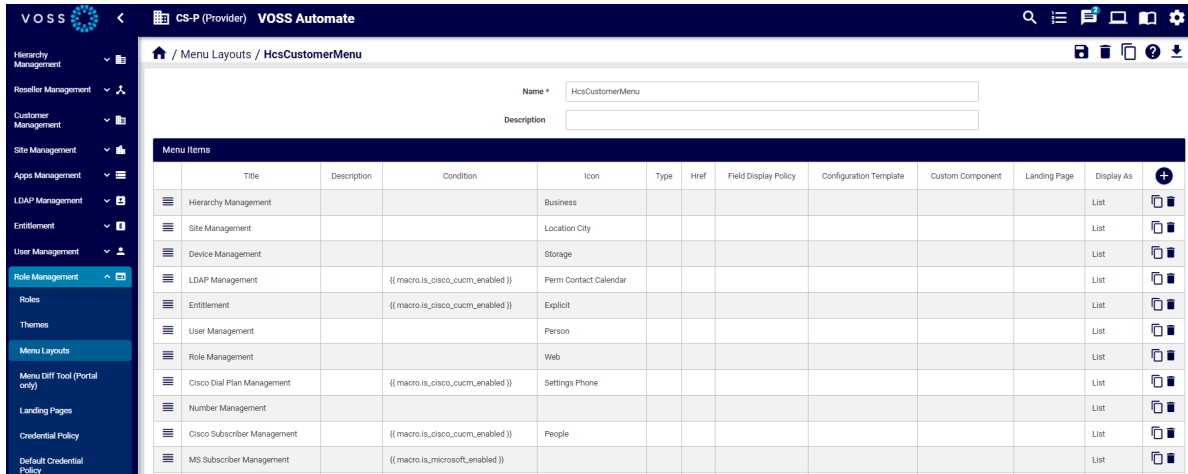


Add a Custom Component to a Menu Layout

This procedure adds a custom component to a menu layout.

Note: The steps are similar for adding custom components to landing pages.

1. Log in to the VOSS Automate Admin Portal.
2. Go to (default menus) **Role Management > Menu Layouts**.
3. Choose a menu layout in the list to open its editing screen.



4. Choose the menu group where you want to add a new menu item.
5. At **Menu Items**, click the Plus icon (+) to add a new row to the menus.
6. Fill out details for the new menu item.

Note:

- Title is the name of the new menu item.
- The model type you choose defines the available options in the **Custom Component** field.

Note that any custom component names or routes that contain the text *edit* are reserved for future development. For custom components named *Add/Edit*, only *add* is supported.

Please complete Menu Items information.

Title:
 Description:
 Condition:
 Type:
 Href:
 Field Display Policy:
 Configuration Template:
 Custom Component:
 Display As:

Fixed Filters

Configurable Filters

Menu Items									
Title	Description	Condition	Type	Href	Field Display Policy	Configuration Template	Custom Component	Display As	

7. Click **OK**.
8. Verify that the menu displays as required:

- Log out of the VOSS Admin Portal, then log in with the user role for which you added the new menu item.
- Navigate to the menu item, and select it to verify that it displays the relevant, associated page.

13.3.5. Fixed and Configurable Filters in Menus and Landing Pages

Configurable Filters

Use **Configurable Filters** to open the dialog to enter one or more filter options. If more than one filter is added, this results in a logical AND of the filter application.

- **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** - check box to manage the case of the **Filter String** value.

When the menu item or landing page link is then selected, a pop-up filter box is displayed and the administrator is prompted to apply or modify the filter. If a **Filter String** value is entered on **Configurable Filters**, this value can also then be accepted or modified in the pop up box.

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 "Filtering Lists".

Important: Standard list view filters on model types (for example if accessible by other landing pages or menu items) can still be used as described in "Filtering Lists", but these will be removed and replaced by any Configurable Filters on landing page links or menu items for the corresponding model type.

Fixed Filters

Only high-level administrators can add and modify pre-defined **Fixed Filters** to menus and landing pages. For these administrators, this option also shows on the Menu Layout and Landing Page 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 or landing page link is used by them. Fixed filter results can however be filtered further by Configurable Filters.

13.4. Credential Policy

13.4.1. Customized Credential Policy

A default credential policy called HcsCredentialPolicy ships with VOSS 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.

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. Choose **Role Management > Credential Policy**.
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.

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.

Field	Description
Number of Questions Asked During 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.
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: <ul style="list-style-type: none"> • 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**.

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. Choose **Role Management > 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](#).

13.4.2. Assign a Credential Policy to a User

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 (default menu) **User Management > Users**.
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.

13.4.3. Assign a Credential Policy to an Administrator

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 (default menu) **User Management > Admins**.
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.

13.5. Privacy Policy

13.5.1. Support for Privacy and Security Notices

VOSS 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 Banner](#).

- Privacy and Cookie Policy notices

When drafting cookie policy notices, VOSS Automate provides reference content - see: [VOSS Automate Cookie Policy](#)

- 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, refer to : [Customize Login Page Theme and Text in the Legacy Admin Portal](#).

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](#).

13.5.2. Privacy Policy Menu Items

In order to comply with General Data Protection Regulation (GDPR) requirements, VOSS Automate provides the means to manage privacy policy notices on the user interface.

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.

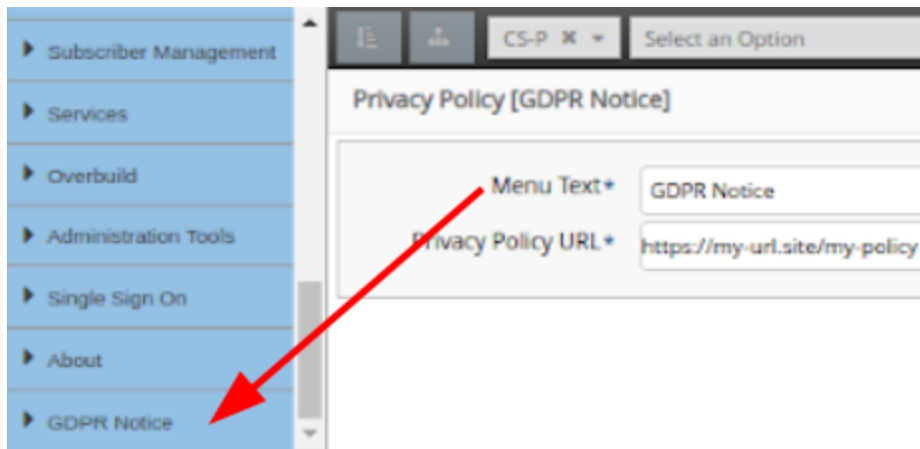
Note:

- 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**. Refer to [Customize Login Page Theme and Text in the Legacy Admin Portal](#).
-

13.5.3. Manage Privacy Policy Menu Items

1. Log in as an administrator with the required privacy policy management permissions and menu access.
2. Choose the menu item, 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.



13.5.4. VOSS Automate Cookie Policy

When formulating a cookie policy, customers should include details on the use of cookies by VOSS Automate. The text below provides details on the use of cookies in VOSS 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
```

14. Flow Through Provisioning Configuration

14.1. Flow Through Provisioning

14.1.1. Overview

VOSS Automate's flow through provisioning feature allows auto-provisioning of users and services during user sync from devices.

Note:

- VOSS Automate v21.2 introduced sync with flow through provisioning for Microsoft. VOSS Automate v21.3 extends this functionality to 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, the enhanced functionality introduced in this version is recommended.
 - Only *Add* is supported for syncs with flow through provisioning.
-

Related Topics

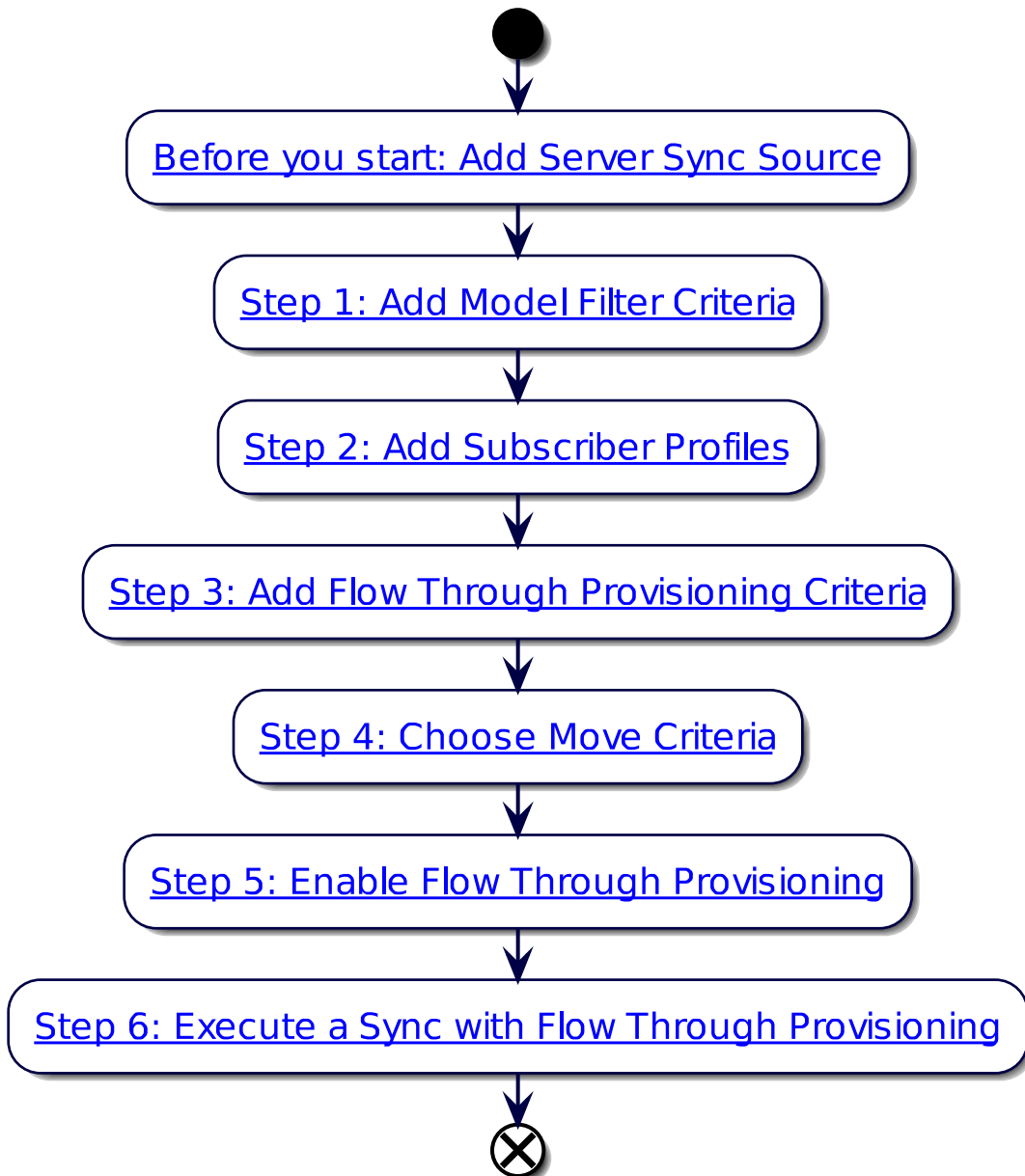
- LDAP Integration in the Core Feature Guide
- Add CUCM Server in the Core Feature Guide
- CUCM Configuration in the Core Feature Guide
- Microsoft Overview in the Core Feature Guide
- Sync with Flow Through for Microsoft in the Core Feature Guide
- Subscriber Profiles in the Core Feature Guide
- Model Filter Criteria in the Core Feature Guide
- Global Settings in the Core Feature Guide
- Site Defaults in the Core Feature Guide
- User Roles in the Core Feature Guide

This topic describes the steps for setting up your system to enable a seamless sync in of users to VOSS Automate from the hierarchy where the sync source device is set up (typically, Customer level), and the flow through provisioning of services to subscribers 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).

- To create a subscriber and provision resources and services, the flow through provisioning references subscriber profiles. See *Subscriber Profiles*.
- Each flow through provisioning criteria (one per customer) consists of one or more pairs of model filter criteria and a subscriber profile combinations.

14.1.2. Flow Through Provisioning Workflow



14.1.3. Before you Start: Add a Server as Sync Source

Users are imported from the server sync source to the Customer level in VOSS Automate. The flow through provisioning is generic functionality and supports a number of scenarios, including Microsoft, LDAP, CUCM, 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 Configuration](#), [LDAP Server](#), [Add a CUCM Server](#)

14.1.4. 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) to match the user to the correct site on import. Model filter criteria allows you to move the user to the correct site on import.

For details around adding the model filter criteria, see [Model Filter Criteria](#)

VOSS Automate interface showing the configuration for a Model Filter Criteria. The filter is named "MS user department is IT or SALES" and is used for "Flow Through Provisioning" with the type "device/msgraph/MsolUser". The criteria are defined as "Department is exactly IT OR".

Field	Value
Name *	MS user department is IT or SALES
Description	MS user department is IT or SALES
Usage	Flow Through Provisioning
Type	device/msgraph/MsolUser
Unary Operator	
Attribute *	Department
Condition *	Equals Exactly
Value *	IT
Conditional Operator	OR

Criteria: Department is exactly IT OR

Preview: Department contains ignoreCase SALES

14.1.5. Step 2: Add Subscriber Profiles

Flow through provisioning uses the subscriber profile to determine the services to be assigned to a subscriber once they're moved to the site.

For details around adding subscriber profiles, see [Subscriber Profiles](#)

14.1.6. 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 subscriber profile combinations. The flow through provisioning criteria defines how users are matched to both sites and subscriber profiles, allowing the tool to seamlessly move users to the sites (based on model filter criteria) and to create a subscriber and assign services from the subscriber 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 subscriber profiles for this customer and its sites. For example, if you have ten different subscriber profiles, you can add ten pairs of model filter criteria and subscriber profile combinations.

Note: Flow through provisioning criteria is configured via either of the following menu options (default menus):

- **Customizations > Flow Through Provisioning Criteria**
- **Flow Through Provisioning Configuration > Flow Through Provisioning Criteria.**

Before setting up the flow through provisioning criteria, configure the following:

- [Server sync source](#)
- [Model Filter Criteria](#)
- [Subscriber Profiles](#)

The screenshot displays the Voss Automate web interface for configuring Flow Through Provisioning Criteria. The left sidebar shows the navigation menu with 'Customizations' selected. The main content area shows the configuration for 'Alterlake FTPC'.

The configuration details are as follows:

- Name:** Alterlake FTPC
- Description:** Alterlake FTPC
- Criteria Order:** A list of criteria is shown, each with a 'Model filter criteria' and a 'Subscriber Profile' dropdown.

Criteria Order	Model filter criteria	Subscriber Profile
1	[MS user department is Engineering, "device/msgraph/MsolUser", "hcs-CS-PCS-NB-RND-East.AlterLake"]	MS with ES License and EV
2	[MS user department is IT or SALES, "device/msgraph/MsolUser", "hcs-CS-PCS-NB-RND-East.AlterLake"]	IT
3	[MS user title is CEO, "device/msgraph/MsolUser", "hcs-CS-PCS-NB-RND-East.AlterLake"]	
4	[MS user Department is Executive Management, "device/msgraph/MsolUser", "hcs-CS-PCS-NB-RND-East.AlterLake"]	
5	[MS user department contains Sales or Marketing, "device/msgraph/MsolUser", "hcs-CS-PCS-NB-RND-East.AlterLake"]	
6	[MS user department is DEVELOPER, "device/msgraph/MsolUser", "hcs-CS-PCS-NB-RND-East.AlterLake"]	

14.1.7. 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). The 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*
- *Subscriber Profiles*
- Flow Through Provisioning Criteria

Perform these steps:

1. Go to (default menus) **Site Management > Defaults**.
2. Click on the relevant site.
3. On the **Move Filter Criteria** tab, choose the criteria for the user types you're importing (Microsoft, LDAP, and/or CUCM).
4. Save.

14.1.8. Step 5: Enable Flow Through Provisioning

Enabling your system for flow through provisioning in the Global Settings allows VOSS Automate to perform a seamless sync in, to move users to the correct site (based on move filter criteria) as subscribers (based on the model filter criteria), and to provision these subscribers with appropriate services (based on the subscriber profile).

Prerequisites:

- Server sync source
- *Model Filter Criteria*
- *Subscriber Profiles*
- Flow through provisioning criteria
- Move criteria selected

Perform these steps:

1. Log in to the Admin Portal as Provider admin or higher.
2. Set the hierarchy to the level where the sync source device exists. Typically, this is at the customer.

- Go to (default menus) **Customizations > Global Settings**, and select the **Flow Through Provisioning** tab.

Note: Alternative menu: **Flow Through Provisioning Configuration > Global Settings**.

- At **Enable Move & Flow Through Provisioning**, select **Yes**.
- At **Enable Move & Provisioning after Add Sync**, select **Yes**.
- At **Flow Through Provisioning Criteria**, choose the flow through provisioning criteria to use at the customer level (for all sites at the customer).
- Save.

The screenshot displays the VOSS Automate interface for a provider named 'CS-P'. The main content area is titled 'Global Settings' and contains the following configuration options:

- Enable Flow Through Provisioning:** Set to Yes.
- Enable Provisioning after Add Sync:** Set to Yes.
- Flow Through Provisioning Criteria:** Set to [Alterlake FTPC].

The left sidebar shows a navigation menu with the following items:

- Hierarchy Management
- Reseller Management
- Customer Management
- Site Management
- Apps Management
- LDAP Management
- Entitlement
- User Management
- Role Management
- Customizations
- Flow Through Provisioning Configuration** (selected)
- Subscriber Profiles
- Model Filter Criteria
- FTP Provisioning Criteria
- Global Settings

14.1.9. 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*
- *Subscriber 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 Subscriber from Profile to create the subscriber, and checks the flow through provisioning criteria to match it to a subscriber profile.
6. Provisions the subscribers with appropriate services, from the subscriber profile.

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 (default menus) **User Management > Users**, and in the list view, check that synced in users are at the correct sites.
2. On the Subscribers list view, check that subscribers exist at the sites, with relevant services.

15. Customizations

15.1. 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
- Landing Page customization
- Field Display Policies
- Configuration Templates

15.2. Global Settings

15.2.1. 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.

This topic describes the global settings, which you can access via (default menu) **Customizations > Global Settings**.

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 [Change Inherited Settings](#).

You can select the following tabs on the Global Settings page:

- Number Inventory
- Number Inventory Alerting
- Webex App

- Pexip Conference
- Email
- Phones
- Voicemail
- User
- Flow Through Provisioning
- Enabled Services

15.2.2. Number Inventory Tab

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 .
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 the Number Management menu), display along with the numbers in the drop-down lists. For example, let's say you have a number and its description as follows: <i>1000 - CEO Internal</i> . When this setting is enabled (Yes), both the number (1000) and its description displays in the lists (when using features such as Quick Add Subscriber). 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.
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, subscriber, or service associated with the number is deleted, and the number is no longer associated with these entities. Options are: <ul style="list-style-type: none"> • 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.

Related Topics

- Number Cooling in the Core Feature Guide
- Number Cooling Auto Expiry Schedule in the Advanced Configuration Guide

15.2.3. Number Inventory Alerting Tab

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 <i>not configured</i> . Change to Yes to enable alerting.
Alert Aggregate Level	Choose a hierarchy level at which the <i>aggregate</i> 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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](#).

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

15.2.4. Webex App Tab

This tab configures the global settings for Webex App.

The table describes the fields on this tab:

Field	Description
Retain a Webex App User when a Subscriber is deleted	Defines whether to delete Webex App user when a subscriber 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 VOSS 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.

Related Topics

- Quick Add Subscriber Group 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

15.2.5. 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 Subscriber is deleted	Defines whether the Pexip conference set up from the subscriber interface is to be removed when the subscriber is deleted. By default the setting is inherited from the hierarchy level directly above the current one.

15.2.6. Email Tab

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 Subscriber	Defines whether an email is sent to a user when added via Quick Add Subscriber. The default is No . When set to Yes , and a SMTP server is set up (via the Apps Management menu), then selecting the option to send an email when using Quick Add Subscriber, a welcome email is sent to the new subscriber.

Related Topics

- SMTP Server in the Core Feature Guide
- Email in the Core Feature Guide

15.2.7. Phones Tab

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:

Field	Description
Delete existing Unassigned Phone when re-adding an identical phone	<p>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 <i>Inherit</i> (<i>No</i>, inherited from the hierarchy above), which triggers a transaction failure if you try adding a duplicate phone, for example, in a QuickAddSubscriber bulk load or when updating a subscriber. When set to <i>Yes</i>, a system check verifies whether the phone exists and/or if it is already assigned (whether ownerUserName field is populated):</p> <ul style="list-style-type: none"> • If the phone exists and is assigned to a different subscriber, 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 subscriber you're adding or updating. • If the phone exists and is already assigned to the subscriber you're working with. The system performs an update.
Retain Desk Phones when Subscriber is deleted	<p>Defines whether a subscriber's associated desk (hard) phones (phones prefixed with SEP or BAP) are deleted or retained when that subscriber is deleted. When set to <i>Yes</i>:</p> <ul style="list-style-type: none"> • The deleted subscriber's hard phones are retained. • The deleted subscriber'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 subscriber is deleted. <p>Default is <i>Inherit</i> (set to <i>No</i>). This setting defines hard phone delete/retain behavior for any method of deleting a subscriber, for example, delete subscriber via the Subscribers list view, or delete subscriber in LDAP import, purge or sync (where delete or purge mode is automatic). You can view the hard phones associated with the subscriber on the Phones tab in Subscriber settings.</p>
Update the Retained Desk Phone with Configuration Template	<p>This field displays only when Retain Desk Phones when Subscriber is deleted is set to Yes (True). Defines whether to update retained hard phones via a configuration template (CFT) when the associated subscriber 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 subscriber. You can choose a different CFT for the update step, if required.</p>

Field	Description
Include additional information in Phone dropdowns	Options are Yes, No, Inherit. Default is <i>Inherit</i> (inherited from the hierarchy above) Set to <i>Yes</i> 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 <i>Inherit</i> . Additional information options are <i>Description</i> , <i>First Line</i> , and <i>Description + First Line</i> . The default, <i>Description</i> , means that the phone description (if defined) displays in the phone selection drop-downs on the Replace Phone configuration screen (Existing Phone tab, Device Name drop-down), and on the Quick Add Subscriber screen, 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 <i>First Line</i> or <i>Description + First Line</i> , you can search for or choose phones based on this criteria.

Related Topics

- Replace Phone in the Core Feature Guide.
- Quick Add Subscriber for CUCM Users in the Core Feature Guide.
- Subscriber, Phones tab in the Core Feature Guide

15.2.8. Voicemail Tab

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 Subscriber is deleted.	Defines whether to retain a Cisco (CUCM) subscriber's voicemail account when the subscriber 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.

15.2.9. User Tab

This tab configures the global settings for users.

Note: When a user is either synced into or added manually on VOSS Automate, these settings apply by default. The settings can however be modified when adding a user from the **User Management** menu.

The table describes the settings on this tab:

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).

Related Topics

- User Authentication Methods in the Core Feature Guide.

15.2.10. Flow Through Provisioning Tab

This tab defines global settings for sync with flow through provisioning.

The table describes the settings on this tab:

Field	Description
Enable Move & Flow Through Provisioning	Defines whether move and flow through provisioning is enabled. The default is No.
Enable Move & Provisioning after Add Sync	Defines whether move and flow through provisioning on add sync is enabled. The default is No.
Flow Through Provisioning Criteria	Defines the default flow through provisioning criteria applied to a user to create the subscriber at the site and to assign services.

Related Topics

- Flow Through Provisioning in the Core Feature Guide.

15.2.11. Enabled Services Tab

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).

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 subscriber 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 subscribers, the default setting for services other than these 5 services is Inherit (False). To provision services to new subscribers (added after an upgrade), you will need to enable the vendor service in global settings.

- **Enable Cisco / Microsoft Hybrid:** When enabled, VOSS Automate allows for provisioning users and services from both Cisco and Microsoft devices. An administrator user parent menu called **Hybrid Cisco-Microsoft Management** and associated access profiles are made available. For details, refer to Hybrid Cisco-Microsoft Management in the Core Feature Guide. The default is No.

Related Topics

- Multi-vendor Subscribers in the Core Feature Guide
- Role-based Access for Multi-vendor Subscriber in the Core Feature Guide
- Configure Multi-vendor Subscribers in the Core Feature Guide
- Hybrid Cisco-Microsoft Management in the Core Feature Guide

15.2.12. Change 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.

15.3. Subscriber Profiles





15.3.1. Overview

Subscriber profiles allow you to group a number of services and resources into a profile that you can assign to a subscriber via Quick Add Group (QAG) templates. The subscriber profile can then for example be added to the QAG along with other configuration settings.

Subscriber profiles are used in the Admin Portal and in the Business Admin Portal. In the Business Admin Portal, subscriber profiles are also used for hybrid subscriber management.

Flow through provisioning uses the subscriber profiles to assign services to subscribers 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* subscriber profile is created at sys (System) level. Only a system level administrator may delete the system-level default profile. To add a new subscriber profile, it is recommended that you clone (create a copy) of an existing subscriber profile and create the new profile based on a valid (working) QAG.

Name *	<input type="text" value="Default"/>
Description	<input type="text" value="Default Subscriber Profile. This will not provision any services. Clone this profile to"/>
Entitlement Profile	<input type="text" value=""/>  
Quick Add Group *	<input type="text" value="Reference Quick Add Group"/>  
Cisco Voice	<input type="checkbox"/>
Cisco Extension Mobility	<input type="checkbox"/>
Cisco Voicemail	<input type="checkbox"/>
Webex Meetings	<input type="checkbox"/>
Webex App	<input type="checkbox"/>
Pexip Conferencing	<input type="checkbox"/>
Contact Center Express	<input type="checkbox"/>
Cisco Single Number Reach	<input type="checkbox"/>
Cisco Jabber	<input type="checkbox"/>
Microsoft Teams	<input type="checkbox"/>
Hybrid	<input type="checkbox"/>

15.3.2. Configure Subscriber Profiles

This procedure adds, edits, or deletes a subscriber profile.

Perform these steps

1. Go to (default menus) **Customizations > Subscriber Profiles**.

Note: Alternative step: **Flow Through Provisioning Configuration > Subscriber Profiles**.

2. Choose an option:
 - To update an existing subscriber profile, click on a profile in the list view. Go to step 3.
 - To delete an existing subscriber profile, select the profile in the list view, and click **Delete**.
 - To add a new subscriber profile, click **Add**. Go to step 3.

3. To add or update a subscriber profile settings, configure fields on the form, then save your changes.

The table describes options for configuring subscriber profiles:

Field	Description
Entitlement profile	Select an entitlement profile to define the resources and services that may be assigned to a subscriber.
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 Subscriber (QAS) and Quick Subscriber (for Microsoft users).
Cisco Voice	Assigns voice services. When enabled, a desk phone is created. The phone template in the QAG defines the phone type. When voice is disabled in the profile, the following fields are hidden on the Business Admin Portal Subscriber page: <ul style="list-style-type: none"> • Use generated phone name • Phone Name
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 subscriber line. Subscriber 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 subscriber is associated with two or more extension mobility profiles on the Unified CM, and you sync with VOSS Automate, only the first extension mobility profile displays on the Subscribers list view in VOSS Automate.
Cisco Voicemail	Assigns voicemail service for the profile. When enabled, and the service is added, the subscriber can be added as a voicemail user.
Webex Meetings	Allows Webex service.
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 subscriber profile, the subscriber 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 subscriber default extension displays, as well as (depending on the selected controlled device type - phone or extension mobility), the subscriber's phone or device profile.

Field	Description
Cisco Single Number Reach	Choose whether to include single number reach (SNR) service for the profile. Only one remove destination profile may be added for single number reach. If a mobile number has already been configured for a subscriber, it is used to pre-populate the Mobile Number field when adding SNR for that subscriber. 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: <ul style="list-style-type: none"> 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 Subscriber Profile is used.¹ The Class of Service drop-down field is exposed. Default value is empty.

Note: When both Microsoft Teams and Hybrid are selected in the Subscriber Profile, the Hybrid Quick Add Subscriber steps are skipped when adding a subscriber.

Related Topics

- [Flow Through Provisioning](#)
- [Voicemail in the Business Admin Portal Guide](#)
- [Webex App in the Business Admin Portal Guide](#)
- [Contact Center Management in the Business Admin Portal Guide](#)

15.4. Model Filter Criteria

15.4.1. Overview

Model filter criteria defines how users (for example, LDAP or MSOL user) are matched to corresponding data in VOSS 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 (for example, Microsoft, LDAP, or CUCM users).

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.

¹ See: [Hybrid Service Definitions](#)

The SDD provides options to choose a predefined model filter criteria (depending on the user type). Options are:

- MS 365 User Model Filter Criteria
- LDAP User Model Filter Criteria
- CUCM User Model Filter Criteria

15.4.2. 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 global settings (on the **Flow Through Provisioning** tab), via (default menus) **Customizations > 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 (default menu) **Customizations > Model Filter Criteria**.

Note: Alternative step: Go to (default menus) **Flow Through Provisioning Configuration > 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** (e.g. Overbuild) for the filter.
5. From the **Type** (model type) drop-down, select the source model, for example device/msgraph/MsolUser (for Microsoft users) or device/ldap/user (for LDAP users).

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:

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, <code>{{ macro.OVERBUILD_SITE_CITY_NAME }}</code> .
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.

Related Topics

- Microsoft Overview in the Core Feature Guide
- Sync with Flow Through in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide

15.5. Field Display Policies

15.5.1. Overview

Field Display Policies (FDPs) are applied to certain item types in order to modify the default form that is displayed when these items are created or accessed.

With FDPs, the fields on an item detail form can be grouped, disabled, and on-line help text can be added for a field. A field can be provided with a new label and its position on the form can be moved up or down.

More than one FDP can apply to a particular item type so that the selection of a particular policy will present another view of the form.

A FDP for an item type can be applied from a Menu Layout by selecting and associating it with the item on the Menu Layout. The Menu Layout is then selected to be part of a user Role so that users who have this role and log in will be able to have the item displayed according to the relevant FDP.

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 administration users at a certain level. Field Display Policies can then be made that are applied to the Menu Layout associated with the administration users at these levels.

A quick way to add a FDP is to clone an existing Field Display Policy, modify it as required and then to select it for the model on a user's menu layout. In this way a user's interface can be modified from the point of user access to the model on the menu.

There is a unique constraint on the name of the FDP per hierarchy level. The same name can be used on another hierarchy, but a new name is needed at the same hierarchy.

If a FDP is called `default`, it will apply to a model by default.

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.

Related Topics

- Multi-vendor Subscriber Field Display Policy in the Core Feature Guide
- Field Display Policy Input Reference in the Advanced Configuration Guide

15.5.2. 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.

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.

To order fields in a group, arrange them in the Selected box. Use the **Move Up** and the **Move Down** buttons under the box.

Ordering Rules

The following ordering rule applies:

The ordering of child fields and their parents depend 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

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.

15.5.3. 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 (default menus) **Customizations > 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.

15.5.4. Add or Edit a Field Display Policy

This procedure adds and edits a field display policy (FDP).

Note: To modify the default form available for an item, a FDP can be added to Data models, Relations, and Views.

1. Login as Provider administrator or higher.
2. Choose the relevant hierarchy.
3. Go to (default menus) **Customizations > Field Display Policies** to open the list of existing FDPs.
4. To edit an existing FDP, click on the relevant FDP and update the configuration, as required.

5. To add a new FDP, click **Add** on the toolbar, and configure the following:

- a. In the **Name** field, enter a name for the new FDP.
 - If the name is default, the FDP is applied to the target model type by default.
 - Each FDP at the same hierarchy level must have a unique name. FDPs at different hierarchies can share the same name.
- b. Optionally, enter a description.
- c. At **Target Model Type**, choose a model reference.

The target model type defines the fields available for use in the FDP.

- d. At **Groups**, click the plus icon (+), then configure the following:

All fields in the FDP must belong to a group.

Component	Description
Title	Mandatory. Enter the 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.
Display as Fieldset	Select this check box to display the group header and fields as a fieldset on the same page in the Admin Portal (not on a separate tab). Alternatively, if two or more groups have this checkbox enabled, the group title displays on a tab called Base .
Number of Columns	Enter a numeric value to define the number of columns. The default is a single column. Fields in the Selected transfer box display in these columns.
Fields	Choose fields to add. Select fields from the Available box and add them to the Selected box. The target model type you choose defines the available fields. Use the Move Up/Move Down buttons to adjust the position of any field.

- e. At **Field Overrides**, click the plus icon (+), then configure the following:

This step configures fields added to the **Selected** transfer box.

Component	Description
Field	Select the field.
Title	Define the label text. 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	Enter the text to display as the field online help and form tooltip. Alternatively, leave the field blank to use the model attribute description.
Disabled	Select this check box to display the field as disabled (unavailable).
Input Type	Select an option to choose how the input field displays.

6. Click **Save**.

If you're editing an existing FDP, your changes are saved.

If you're adding a new FDP, the FDP is created and is available for applying to the item by selecting it in a menu layout available to a role.

Field Display Policy Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the FDP.
Description	description	A description for the FDP.
Target Type Model *	target_type_model	The target model type to which the FDP applies.
Groups	groups.[n]	The groups that describe groupings of attributes that are displayed together on the user interface.
Title *	title	The name of a specific group of attributes.
Display as Fieldset	display_as_fieldset	Render this group as a fieldset in the form.
Number of Columns	num_cols	The number of columns of fields.
Fields	fields.[n[]]	Model fields that will form part of the particular group.
Field Overrides	field_overrides.[n]	FDP overrides to apply to a model fields.
Field *	field	Name of the model field to override.
Title	title	New title to display for field.
Help Text	help_text	New help text to display for field.
Disabled	disabled	Will set the field to read-only if checked.
Input Type	input_type	Overrides the input type of the field.

15.6. Configuration Templates

15.6.1. Overview

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). And they provide a mechanism 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).

Consider these examples:

- 1) 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.
- 2) A model such as Quick Add Subscriber (QAS), 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 Subscriber (for example, Voicemail account settings, conference account settings, phone, line, device profile settings, and so on).

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 Administrator can also customize these templates, including Field Display Policies.

Note:

- When modifying CFTs in the Admin Portal, numerical values need to be entered using the `fn.as_int` function, for example:

```
{{ fn.as_int 14 }}
```

- 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.
-

15.6.2. Add a Configuration Template

This procedure clones and edits an existing configuration template (CFT) to create a new CFT.

Perform these steps:

1. Log in as Provider Administrator or higher.
2. Go to **Customizations > Configuration Templates** to view the list of existing CFTs.
3. Click on a 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 Field Reference](#)

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.

15.6.3. Configuration Template Field Reference

The table describes general fields on the Configuration Template editing screen:

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.

15.6.4. Example: Add a CFT for a Cisco 6941 SCCP Phone

1. Choose the hierarchy where the CUCM 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**.
- 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**.

15.7. Business Admin Portal Profiles

15.7.1. Overview

Business Admin Portal profiles (Disabled, default, Read Only, or Full Access) are assigned to user roles via the Business Admin Portal custom interface type (`InterfaceBusinessAdminPortal`), and define the level of access a user has to the following functionality in the Business Admin Portal.

- Features (menus)
- MACDs/Day 2 functionality
- Dashboard widgets, such as charts

The table describes the predefined Business Admin Portal profiles that ship with `InterfaceBusinessAdminPortal`:

Profile	Description
Disabled	A user role with this profile is unable to access the Business Admin Portal.
default	<p>This profile is applied by default to new user roles, at the user's hierarchy level or the first level up. System-level administrators can clone this profile down the hierarchy and modify it to create custom default profiles for the Business Admin Portal interface type.</p> <p>A user role associated with the default profile:</p> <ul style="list-style-type: none"> • Has access to the Admin Portal: Allow switch to Admin mode is enabled. <p>An icon shows in the upper Business Admin Portal interface toolbar to allow switching. If users should not have access, this profile can be cloned to the appropriate hierarchy and the setting can be disabled.</p> <ul style="list-style-type: none"> • Has no access to the following Business Admin Portal menus: <ul style="list-style-type: none"> – Site management – Tools • Has view access (read-only) to data from other Business Admin Portal menus, including example model counts and charts.
Read Only	<p>The profile applied by default to all operator administrator user roles, with the same permissions as the default profile:</p> <ul style="list-style-type: none"> • No access to the following Business Admin Portal menus: <ul style="list-style-type: none"> – Site management – Tools • Read-only access (view) to data from other Business Admin Portal menus, including example model counts and charts.
Full Access	<p>This profile is applied by default to the provider admin role for new installations.</p> <p>User roles assigned with this profile have full access to all Business Admin Portal menus and features.</p>
MicrosoftOnlyBAP	<p>This profile is included in the user role <code>MicrosoftOnlyRole</code>, which is used to provide a Microsoft-only GUI experience in a Microsoft-only, single vendor environment. See Add and Edit Roles in the Core Feature Guide for more information around adding and assigning this role.</p> <p>This Business Admin Portal profile also ships with a field display policy for a Microsoft-only GUI.</p>

Note: When upgrading to Release 19.1.2 or higher, only the roles at the `sys.hcs` level are updated.

15.7.2. Business Admin Portal Profiles and Field Display Policies

The default Business Admin Portal profile is associated with the following field display (FDP) policies:

- `BusinessAdminPhoneFDP`
- `BusinessAdminLineFDP`
- `BusinessAdminVoicemailFDP`
- `BusinessAdminWebexTeamsUserFDP`
- `BusinessAdminUccxAgentFDP`
- `BusinessAdminUccxTeamFDP`
- `BusinessAdminUccxContactServiceQueueFDP`
- `BusinessAdminHuntGroupFDP`
- `BusinessAdminCallPickupGroupFDP`

These FDPs can be cloned and edited to create new customized FDPs. Or you can create completely new FDPs for the Business Admin Portal profile.

15.7.3. Multi Vendor and Business Admin Portal Profiles

The default FDP for multi vendor scenarios (`MultiVendorFDP`) is not associated with any Business Admin Portal profiles by default. You will need to manually enable multi-vendor for any of the Business Admin Portal profiles, which will then use the multi-vendor FDP.

To enable multi vendor for a Business Admin Portal profile:

1. Log in to the Admin Portal as a provider administrator (or higher).
2. Go to (default menus) **Customizations > Business Admin Portal Profiles**.
3. Click on the relevant profile to open the editing screen.
4. Clone the profile to create a new custom Business Admin Portal profile.
5. On the **Subscribers** tab, select **Enable Multi Vendor**.
6. Save the profile. Allowed features will now be determined via the multi vendor FDP.

15.7.4. Microsoft-Only Business Admin Portal Profile

VOSS Automate ships with a Microsoft-only Business Admin Portal profile (`MicrosoftOnlyBAP`), which is included in the `MicrosoftOnlyRole`, a Microsoft-only user role that provides a Microsoft-only GUI experience suited to a Microsoft-only (single-vendor) environment where you wish to hide functionality related to vendors other than Microsoft.

For more information around `MicrosoftOnlyRole`, see [Add and Edit Roles](#) in the [Core Feature Guide](#).

15.7.5. Add a Business Admin Portal Profile

This procedure adds a new Business Admin Portal profile.

1. Log in to the Admin Portal as a Provider administrator (or higher).
2. Go to (default menu) **Customizations > Business Admin Portal Profiles**.
3. Click on an existing Business Admin Portal profile to open its editing screen:
 - If you're using the VOSS Automate legacy Admin GUI, click **Actions > Clone**.
 - If you're using the new VOSS Automate Admin Portal, click the toolbar **Clone** icon.
4. Configure options on the **Details** tab of the Business Admin Portal profile:

Note: This is the **Base** tab in the legacy Admin GUI.

The screenshot shows the configuration interface for a Business Admin Portal profile. The title is "Interface Business Admin Portal [CS-P]". There are six tabs: "Base", "Dashboard", "Site Management", "Number Management", "Subscribers", and "Phones". The "Base" tab is active. The form contains the following fields and options:

- Name***: Text input field containing "CS-P".
- Description**: Text input field containing "Default System BAP Profile".
- Enable Business Admin**: Checkmark
- Site Management**: Checkmark
- Number Management**: Checkmark
- Subscribers**: Checkmark
- Phones**: Checkmark

1. Define a new name, and a description.
2. Select **Enable Business Admin** to display the **Dashboard** tab.

3. Select or clear the relevant checkboxes to enable access to menus and other functionality in the Business Admin Portal for this profile. The rest of the tabs on this form are hidden or display depending on whether the relevant checkbox is selected on this tab.
4. To add custom features to the Quick Actions card for a feature, click the Plus icon (+) in **Custom Features**; then, configure the custom feature:

5. Select an icon and an icon title.
6. From the **Feature Area** drop-down, select the feature, for example, Extension Mobility, or Phones.
7. From the **Type** drop-down, choose a model type.

Note: Similar to menu layout configuration, you'll need to set up additional configuration associated with the model type. The model type must be exposed in the user's access profile, if the custom interface type is associated with a user.

8. Choose a field display policy, and a configuration template.
 9. Click **OK**.
5. Configure options on the **Dashboard** tab of the Business Admin Portal profile:
 1. Enter a title for the dashboard.
 2. Optionally, select a landing page. When selecting a landing page, the header and line text details on the landing page **Welcome Header** tab display. See Create a Landing page in the Core Feature Guide.
 3. To select MACDs the admin will have access to on the dashboard, move options from the **Available** transfer box to the **Selected** transfer box.

6. On each feature tab you enabled via the **Details** tab, move required options from the **Available** transfer box to the **Selected** box to enable these features on the relevant dashboard.
7. On the **Miscellaneous** tab, configure functionality and display options for the Business Admin Portal:
 1. In **Display About Information**, define whether to show or hide the **Settings > About** menu.
 2. To display the **Export** action on the lists and forms, enable **Allow Data Export**; else, clear the field (disable).
 3. To display options such as Replay and Cancel on the transaction instances and the list view, enable **Transaction Log Actions**; else, clear the field (disable).
 4. To display options for showing and hiding selected information on the transaction when viewing a transaction instance, such as logs and sub-transactions, enable **Transaction Log Display Fields**; else, clear the field (disable).
8. On the **Subscribers** tab, configure functionality available on subscriber dashboards. Available options are defined via the User Details Display Policy you choose.
 - To enable multi vendor, select **Enable Multi Vendor**. The multi vendor subscriber field display policy (default name: MultiVendorFDP) is applied. To change any fields and available functionality, edit MultiVendorFDP, via (default menus) **Customizations > Field Display Policies**.
 - To disable multi vendor, clear the **Enable Multi Vendor** checkbox. In this case, the Subscribers landing page will now display a count card for both subscribers (total number of provisioned users) and for end users (total number of end users).
9. Save the profile.

A provider level admin can assign the new profile and the InterfaceBusinessAdminPortal interface type when adding or updating a user role.

Related Topics

- Multi Vendor Subscribers in the Core Feature Guide
- Assign a Business Admin Portal Profile to a Role in the Business Admin Portal Guide
- Add and Edit Roles in the Core Feature Guide

15.8. Configuration Mapping for Phones, DeviceProfiles, and Lines

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	<ul style="list-style-type: none"> 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 CUCM-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 subscribers.




15.8.1. Phone Configuration Mapping

There may only be one phone configuration mapping at any hierarchy. This phone configuration mapping must be Default.

Mapping Profiles

The mapping profiles define the list of phone types that can be selected, and includes:

- Profile name
- Profile items: Phone type, Protocol, Button template, Security profile
- Base configuration template (CFT)

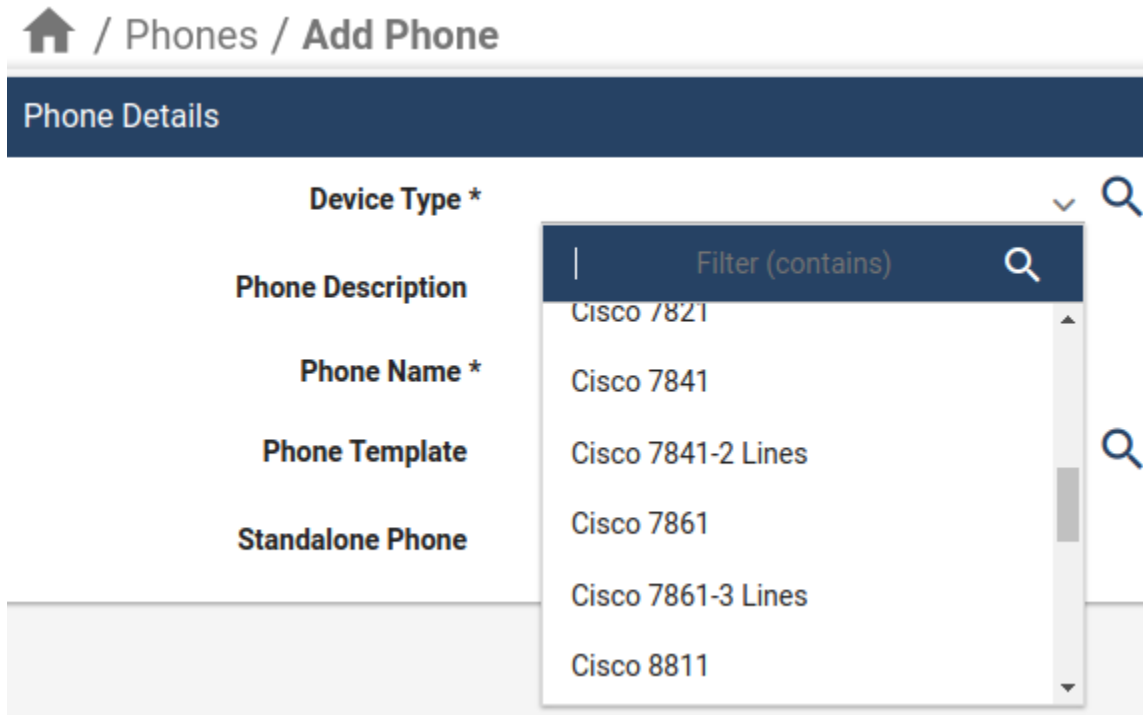
	Profile Name	Phone Type	Protocol	Button Template	Security Profile	Base Configuration Template	
☰	Cisco 7841	Cisco 7841	SIP	Standard 7841 SIP	Cisco 7841 - Standard SIP Non-Secure Profile	Basic Phone CFT	
☰	Cisco 7841-2 Lines	Cisco 7841	SIP	Standard 7841 SIP-2 Line	Cisco 7841 - Standard SIP Non-Secure 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 have a security profile called *Cisco 7841 - Standard SIP Non-Secure Profile*
- The phone configuration will come from a basic CFT called *Basic Phone CFT*



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 superceded 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.

The screenshot shows a web interface for adding a phone. The breadcrumb navigation is 'Home / Phones / Add Phone'. Below this is a dark blue header with the text 'Phone Details'. The form contains several fields:

- Device Type ***: A dropdown menu with a search icon.
- Phone Description**: A text input field.
- Phone Name ***: A text input field.
- Phone Template**: A dropdown menu currently showing 'Default' with a search icon.
- Standalone Phone**: A checkbox.

The 'Phone Template' dropdown menu is open, showing a search bar with the text 'Filter (contains)' and a search icon. Below the search bar, there are two options: 'CS-P Updated CFT' and 'Default', with 'Default' highlighted in blue.

Macros for Phone Configuration Mapping

The table describes the available context macro variables when defining configuration templates for the phone mappings:

Macro	Description
{{ input.standalone }}	Flag whether it is a standalone phone or being associated with a subscriber.
{{ input.username }}	Username of the subscriber 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 subscriber. Only when standalone is false.

15.8.2. 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 subscriber via the Subscriber Management page. See *Feature Templates* under [Phone Configuration Mapping](#).

Please enter details for the new Extension Mobility profile. ✕

Name *	Alicia.Coleman-UDP
Device Type *	Cisco 6921 ▼
Extension Mobility Profile Template	Default ▼
Line Template	Default ▼
Line *	2006 (Alicia.Coleman Line) ▼
Line Label	Coleman - 2006
Line Display	Alicia Coleman

Cancel
OK

15.8.3. 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 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 }}

```

- For secondaryCallingSearchSpaceName

```

{{ macro.CUCM_LINE_callForwardAll_secondaryCallingSearchSpaceName }}

```

- For voiceMailProfileName

```



{{ macro.CUCM_LINE_vmprofile }}

```

Line Configuration Mapping [Default] Save Delete Help Back Action

Name*

+ Line Templates

	Template Name *	Configuration Template *
 	<input type="text" value="Default"/>	<input type="text" value="Default CUCM Line Template"/>

15.9. Dropdown Filters

Administrators with access to the **Dropdown Filters** menu can manage the items available in dropdown lists on input forms. A filter would typically be used to define a shorter dropdown 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 it was created.

15.9.1. Add a Dropdown Filter

1. Navigate to the required hierarchy.
2. Select the **Dropdown Filters** menu and click **Add**.
3. Choose **Create a Dropdown Filter** From the **Select a Dropdown Filter Action** dropdown list.
4. Choose the **Target Model** and **Target Field** names to which the filter is to be applied.

This is the dropdown 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**.

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 that:

- The **Filter Field** can differ from the **Target Field**. In other words, the dropdown 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, in other words, 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)
- `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 dropdown 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 a created dropdown filter is opened, 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 dropdown filter macros by filtering the list by name starting with `DDF__`.

15.9.2. Example of a Dropdown Filter

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:

```
DFF__relation_LineRelationTarget_callForwardAll_callingSearchSpaceName
```

15.9.3. Merged Dropdown Filters

Two existing dropdown filters can be merged to create a new dropdown filter. The merged filter is a dropdown list that uniquely combines the lists from the two dropdown filters.

15.9.4. Merge Dropdown Filters

1. Navigate to the required hierarchy.
2. Select the **Dropdown Filters** menu.
 - Check that the two dropdown filters that you want to merge are showing in the list view at the hierarchy. Otherwise, add the dropdown filters.
3. Choose **Merge Existing Dropdown Filters** from the **Select a Dropdown Filter Action** dropdown list.
4. Choose the **Target Model** and **Target Field** names to which the filter is to be applied.
5. Choose the two dropdown filters from the **Dropdown Filters to merge** form.
6. Click **Save**. A merged dropdown filter is created.

Note: Only two filters can be merged.

If you wish to merge more than two dropdown filters, first create a merged filter of each filter pair and select it to be merged.

When a created merged dropdown 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 dropdown 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.

15.10. Line Delete Preferences

When deleting a phone, device profile or remote destination profile from VOSS Automate, the line or lines (Cisco Unified CM lines) in use by the phones or devices are not automatically deleted.

Line Delete Preferences provides the ability, for a reseller administrator (or higher) to control whether the lines are deleted when deleting the phone or device, or updated (using values contained in a specified configuration template).

A new menu (default = **Customizations > Line Delete Preferences**) allows the configuration of the following:

- 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:

Allow Line Deletion if unused

- If the line is not shared with another phone or device, the line will be deleted and the number inventory updated.
- See also [Delete 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, then 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

15.11. Email

15.11.1. Overview

Provider administrators can test email messages and manage email templates, if an email SMTP server is set up, and when emails are enabled via the Global Settings (Email tab). See: [Add a SMTP Server](#) and [Global Settings](#).

Email functionality is available for the following:

Component	Description
Quick Add Subscriber (QAS)	Enable email functionality via Global Settings > Email tab, then select a checkbox in QAS to send a welcome email to new subscribers added via QAS.
File Transfer Destinations	Configured by high level system administrators to transfer audit data for licensing. See the Licensing and Subscriber Data Export Guide.

Related Topics

- [Add a SMTP Server](#)
- [Global Settings](#)

15.11.2. Send Test Email

Via (default menus) **Customizations > Email > Send Test Email**, 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.

15.11.3. Email HTML Templates

You can view and work with email templates via (default menus) **Customizations > Email > Email HTML Templates**.

Email HTML templates contain placeholders for the email subject and body text, in HTML markup. The HTML markup can be modified as required (for example, by using an external WYSIWYG HTML editor).

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 Subscriber”, 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 Subscriber	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 Subscriber 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.

Quick Add Subscriber Email Template Variables

Values from the Quick Add Subscriber input form can be used to populate the Quick Add Subscriber email template by adding variables to the HTML template.

The table describes the variables available for the Quick Add Subscriber 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 }}

Example user details you can add to your QAS HTML template:

```
<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

info@voss-solutions.com
to me ▾

📧 12:23

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
```

15.11.4. Email Groups

The Email Groups input form is used to manage a group of email recipients.

Add a **Name** and **Description** to make this group and add a list of **Email Addresses**. This group can then be available for selection 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.

Related Topics

- *Add a SMTP Server*
- *Global Settings*

16. Cisco Dial Plan Management

16.1. Introduction to Dial Plan Management

Important: Contact your dedicated VOSS support representative for details on how to set up and configure the next generation dial plan management feature.

Note: If this feature is not exposed in the Admin Portal menu layout, refer to the Optional Features Appendix: Dial Plan Management - Menu Layout Changes and Access Profile Changes.

The VOSS Automate next generation dial plan management feature:

- Offers dial plan management that is independent of the hierarchy schema approach of the first generation dial plan management. However, the feature can also be used in together with schema-based dial plan management.
- Enables senior administrators to define complete complex dial plans and to allow the application of these to lower level administrators without the need to understand the complete dial plan.
- Can be used in place of the schema or schema group approach or in tandem with this approach, for example to add elements in an additional dial plan in an ad-hoc manner.
- All the available functionality of schemas are covered by the models of the feature, as well as call routing via route filters.
- Provides additional benefits:
 - More configuration options
 - A repeatable process to manage Cisco Call manager elements
 - Dial plan can be provisioned in a modular manner
 - A structure to store dial plan models

16.1.1. Scope

The following areas of Cisco Dial Plan deployment are covered by this feature:

- 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
- Time Schedules
- Partitions
- CSSs
- Route Patterns
- Transition Patterns
- Called Party Transformation Patterns
- Calling Party Transformation Patterns
- SIP Route Patterns

The entire group of dial plan elements is referred to as a “Dial Plan Model”. Each dial plan element is broken into its own container or model for storage in VOSS Automate. This allows for simple management of the dial plan model as a whole. The dial plan models may be bulk loaded into VOSS Automate and managed via the Admin Portal.

16.2. Dialplan Management Menu

The Dial Plan Management menus provide access to enhanced dial plan management functionality:

- **Dial Plan Maintenance** - an interface for the created dial plan to be push to or removed from a chosen, **Target Call Manager Cluster**.

The hierarchy on which this operation is carried out will filter the list of dial plans - according to the chosen **Dial Plan Type** when it was created on the **Dial Plan Models** menu.

This utility can also be used to push a dial plan to the cluster for inspection and then to remove it again, as long as no elements were added to the Call Manager cluster that rely on the dial plan elements (for example, adding phones on the Call Manager that would lock CSSs and partitions).

- **Dial Plan Viewer** - a tabbed form view of all the dial plan elements of a selected dial plan created from this feature. 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.

- **Delete Dial Plan Model** - from this menu, an entire dial plan created in this feature can be deleted with a single action, in other words, all dial plan model elements associated with the selected dial plan model are removed, as well as the dial plan model itself.

- **Dial Plan Input Data** - 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.

- **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 each have a menu item from which it can be managed.
- **Dial Plan Log** - a record of Push and Remove operations carried out from the **Dial Plan Maintenance** menu. Details such time and hierarchy of operation, target Call Manager and dial plan name are recorded.

This interface provides an overall view and does not allow any editing of the dial plan.

16.3. Dial Plan Maintenance

The Dial Plan Maintenance View is the mechanism by which dial plan is manipulated on Call Manager instances. There are no restrictions on the use of this tool from a hierarchy perspective. The naming of the dial plans should indicate at what level the dial plans may be used. There is an enhancement in place to tag dial plans in the dial plan model with Global/Site/No Specific Type so that a small amount of error checking can be introduced into this tool.

The dial plan tag 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.

Push Dial Plan Mode

Dp Maintenance View		Save	Help	Back	Action ▾
Tool Description	Dial Plan Maintenance Tool				
Notes	This tool allows you to Push Dial Plan elements to Customer and Site level. The tool can add and remove dial plan elements from Call Manager. To remove dial plan element those element must not be locked by an other informix relationships in Call Manager.				
Hierarchy level	sys.hcs.VLS.Tenant1.Vancouver				
Dial Plan Name*	Site_Level_DP ▾				
Target CUCM*	["10.5.25.21", "8443"] ▾				
Operation	Push Dial Plan ▾				

Remove Dial Plan Mode

Dp Maintenance View		Save	Help	Back	Action ▾
Tool Description	Dial Plan Maintenance Tool				
Notes	This tool allows you to Push Dial Plan elements to Customer and Site level. The tool can add and remove dial plan elements from Call Manager. To remove dial plan element those element must not be locked by an other informix relationships in Call Manager.				
Hierarchy level	sys.hcs.VLS.Tenant1.Vancouver				
Dial Plan Name*	Site_Level_DP ▾				
Target CUCM*	["10.5.25.21", "8443"] ▾				
Operation	Remove Dial Plan ▾				

Both modes of the tool work in the same manner:

1. A dial plan model is chosen from the **Dial Plan Name** drop-down.
2. A target CUCM is chosen from the **Target Call Manager Cluster** drop-down.
3. A operation is chosen from the **Operation** drop-down.

16.4. 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 Unified CM Clusters in a single step.

16.4.1. Procedure

Both modes of the tool work in the same manner:

1. Choose the **Dial Plan Name** to manage on the Unified CM 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 Unified CM clusters from the **Available** transfer box so these are shown in the **Selected** box.
4. Click **Save** to carry out the task.

16.4.2. Notes

- 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 Unified CM of the Network Device List (NDL) belonging to the site to verify if a dial plan is applied to this Unified CM.
- Sites cannot be excluded if a site level dial plan is applied. in the cluster.

16.5. Dial Plan Input Data and Macros

16.5.1. Overview

The input forms from the **Dial Plan Input Data** simplifies the update of dial plan data by exposing a set of values that can be provided to and then easily applied by lower level administrators.

No values are mandatory, and Field Display Policies can be used to hide unused fields if needed (for example, **Secondary SIP Trunk Destination IP** and **Secondary SIP Trunk Destination Port**).

In addition, a set of custom values can be added and macros are available so that these can be referenced in dial plan elements. (A Field Display Policy can then be used to rename the input field label if needed.)

Two types of dial plan input data 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

Input data may be used in combinations to build patterns dynamically, because 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 }}XXXXXX
```

when applied, could be inserted to Call Manager as 9.214XXXXXX for 10 digit dialing.

```
{{ macro.DP_Global_PSTNAccess }}.{{ macro.DP_Exchange }}XXXX
```

when applied, could be inserted to Call Manager as 9.256XXX for 7 digit dialing.

16.5.2. Global Dial Plan Data Single Instance

Data from the provided fields may be referenced with the provided 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 }}

16.5.3. Global Aggregation SIP Input Data Tab

Dp Global Dial Plan Data Save Help Back

Dial Plan Data | Aggregation SIP Input Data | Custom Dial Plan Data

Primary SIP Trunk Destination IP	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_PrimarySIPAddr }}"/>
Primary SIP Trunk Destination Port	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_PrimarySIPPort }}"/>
Secondary SIP Trunk Destination IP	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_SecondarySIPAddr }}"/>
Secondary SIP Trunk Destination Port	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_SecondarySIPPort }}"/>

Data from the provided fields may be referenced with the provided 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 }}`

16.5.4. Global Custom Dial Plan Data Tab

Dp Global Dial Plan Data Save Help Back

Dial Plan Data | Aggregation SIP Input Data | Custom Dial Plan Data

Dial Plan Custom Value 1	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal01 }}"/>
Dial Plan Custom Value 2	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal02 }}"/>
Dial Plan Custom Value 3	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal03 }}"/>
Dial Plan Custom Value 4	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal04 }}"/>
Dial Plan Custom Value 5	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal05 }}"/>
Dial Plan Custom Value 6	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal06 }}"/>
Dial Plan Custom Value 7	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal07 }}"/>
Dial Plan Custom Value 8	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal08 }}"/>
Dial Plan Custom Value 9	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal09 }}"/>
Dial Plan Custom Value 10	<input style="width: 100%;" type="text" value="{{ macro.DP_Global_CVal10 }}"/>

Data from the provided fields may be referenced with the provided 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 }}

16.5.5. Site Dial Plan Data Single Instance

Dp Site Dial Plan Data Save Help Back

Dial Plan Data Aggregation SIP Input Data Custom Dial Plan Data

Custom Site ID

External Breakout Number

Site Location Code

Published Number

Emergency Call Back Number

Dial Plan Model for Site

Local Area Codes

Dial Plan Pattern

Type

Area Code

Exchange

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 }}

16.5.6. Site Aggregation SIP Input Data

Dp Site Dial Plan Data Save Help Back

Dial Plan Data | Aggregation SIP Input Data | Custom Dial Plan Data

Primary SIP Trunk Destination IP:

Primary SIP Trunk Destination Port:

Secondary SIP Trunk Destination IP:

Secondary SIP Trunk Destination Port:

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 }}`

16.5.7. Site Custom Dial Plan Data Tab

Dp Site Dial Plan Data Save Help Back

Dial Plan Data | Custom Dial Plan Data

Dial Plan Custom Value 1:

Dial Plan Custom Value 2:

Dial Plan Custom Value 3:

Dial Plan Custom Value 4:

Dial Plan Custom Value 5:

Dial Plan Custom Value 6:

Dial Plan Custom Value 7:

Dial Plan Custom Value 8:

Dial Plan Custom Value 9:

Dial Plan Custom Value 10:

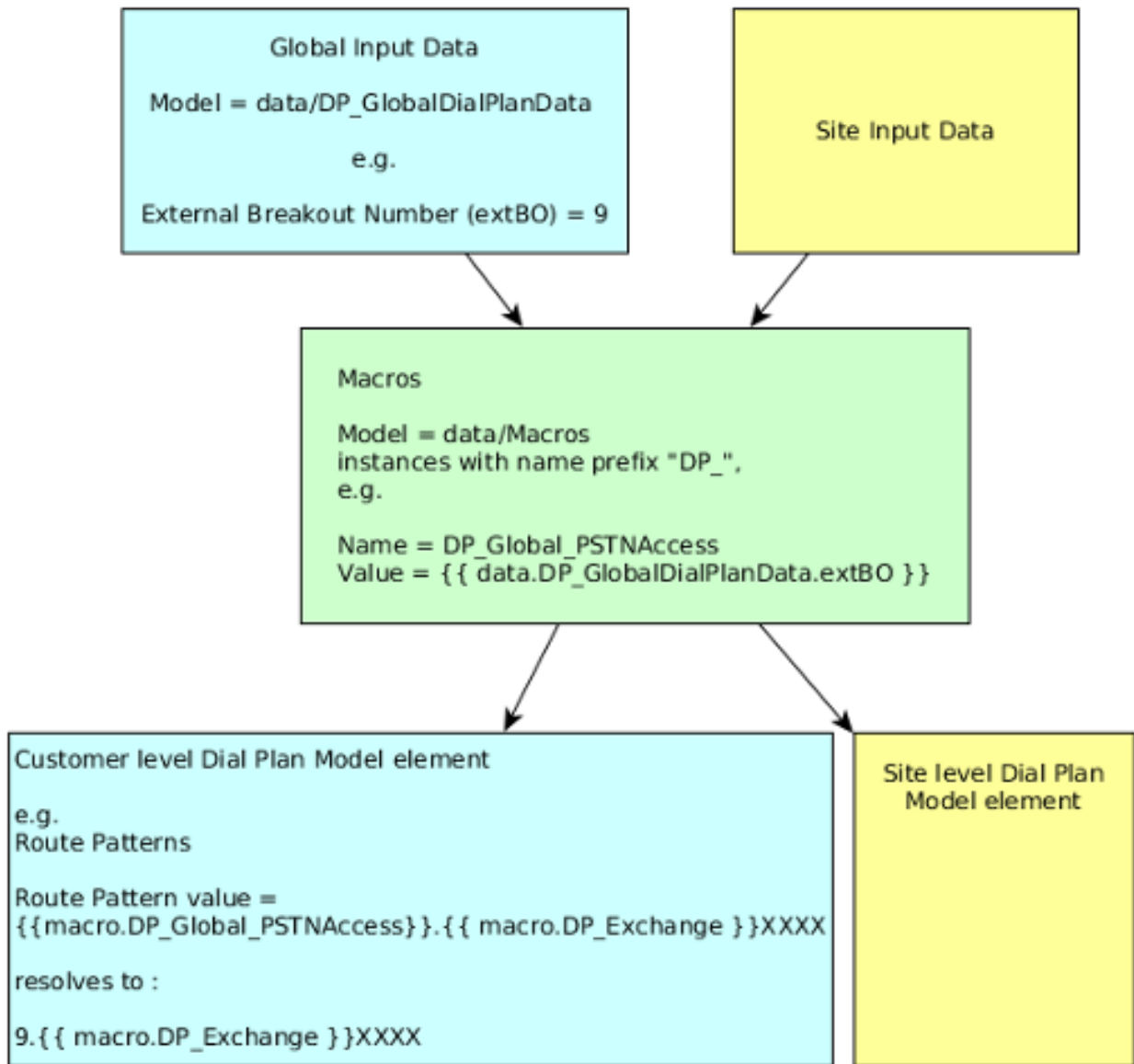
Data from the provided fields may be referenced with the provided macros:

- 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 }}`

16.5.8. Diagram Example

The diagram below provides an example of the use of a macro in a Global (customer) level dial plan element: **Route Patterns**.



16.6. Dial Plan Models

Dial plan models (default menu: **Dial Plan Management > Dial Plan Model**) 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.

16.6.1. 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)

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.

Route Patterns [Tiered_Cust_Level_DP]

Dial Plan Name*	Tiered_Cust_Level_DP
Local Dialing	<input checked="" type="checkbox"/>
Route Pattern	{{ macro.DP_Global_PSTNAccess }}-{{ macro.DP_AreaCode }}XXXXXX
Route Pattern Description	10 digit Digit Local
Route Partition	{{ macro.DP_CustomerName }}-LD-PT

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.

16.6.2. 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.

Dp Dp-Reg-Loc [Site_Level_DP] Save Delete Help Back Action ▾

Device Pool Region Location SRST Reference

Dial Plan Name	Site_Level_DP
Device Pool Name*	{{ macro.SITENAME }}-DP
Call Manager Group	Default
Region	{{ macro.SITENAME }}-REG
Location	{{ macro.SITENAME }}-LOC
SRST Reference*	{{ macro.SITENAME }}-SRST
Date/Time Group	CMLocal

- **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.

Dp Dp-Reg-Loc [Site_Level_DP] Save Delete Help Back Action ▾

Device Pool Region Location SRST Reference

Add Custom Region

Region Name*

Related Region

Related Region Name

Codec Preference

Audio Bandwidth

Video Bandwidth

Immersive Video Bandwidth

Lossy Network

- **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)
 - 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

Dp Dp-Reg-Loc [Site_Level_DP] Save Delete Help Back Action ▾

Device Pool **Region** **Location** **SRST Reference**

Add Custom Location

Location Name*

Within Audio Bandwidth

Within Video Bandwidth

Within Immersive Kbits

Between Location +

- +

Location Name

Audio Bandwidth

Video Bandwidth (kpbs)

Immersive Bandwidth

Weight

- **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**

Dp Dp-Reg-Loc [Site_Level_DP] Save Delete Help Back Action ▾

Device Pool **Region** **Location** **SRST Reference**

Add Custom SRST Reference

Name*

Port

IP Address*

SIP Network/IP Address

SIP Port

Is SRST Secure?

- **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?**

16.6.3. Time Period Model

This allows the administrator to define an unlimited number of time periods.

Dp Time Period					Add	Delete	Help	Action ▼
<input type="checkbox"/>	Dial Plan Name	Time Period Name	Description	Hierarchy				
<input type="checkbox"/>	Site_Level_DP	AllTheTime	AllTheTime	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	BusinessHours	BusinessHours	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	MonthEnd	MonthEnd	sys.hcs.VLS				
<input type="checkbox"/>	Tiered_Cust_Level_DP	MonthEnd	MonthEnd	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	BusinessHours	BusinessHours	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	AllTheTime	AllTheTime	sys.hcs				

Dp Time Period [Site_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name*	<input type="text" value="Site_Level_DP"/>					
Time Period Name*	<input type="text" value="BusinessHours"/>					
Description	<input type="text" value="BusinessHours"/>					
Time of Day Start*	<input type="text" value="07:00"/>					
Time of Day End*	<input type="text" value="17:00"/>					
Start Day	<input type="text" value="Mon"/>					
End Day	<input type="text" value="Fri"/>					
Start Month	<input type="text" value="None"/>					
Start Day of Month	<input type="text" value="0"/>					
End Month	<input type="text" value="None"/>					
End Day of Month	<input type="text" value="0"/>					

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.

- **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.

16.6.4. Time Schedule Model

This allows the administrator to define an unlimited number of time schedules.

Dp Time Schedule					Add	Delete	Help	Action ▾
<input type="checkbox"/>	Dial Plan Name	Time Schedule Name	Description	Hierarchy				
<input type="checkbox"/>	Site_Level_DP	WorkHours	Work Hours	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	AllPeriods	All Periods	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	AfterHours	Work Hours	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	BeforeHours	Work Hours	sys.hcs.VLS				
<input type="checkbox"/>	Tiered_Cust_Level_DP	AllPeriods	All Periods	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	WorkHours	Work Hours	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	AfterHours	Work Hours	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	BeforeHours	Work Hours	sys.hcs				

Dp Time Schedule [Site_Level_DP]		Save	Delete	Help	Back	Action ▾
Dial Plan Name	<input type="text" value="Site_Level_DP"/>					
Time Schedule Name*	<input type="text" value="WorkHours"/>					
Description	<input type="text" value="Work Hours"/>					
Time Periods	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> + - + - </div> <div style="margin-top: 5px;"> <p>Time Period Name <input type="text" value="BusinessHours"/></p> </div> </div> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> - + - </div> <div style="margin-top: 5px;"> <p>Time Period Name <input type="text" value="MonthEnd"/></p> </div> </div> </div>					

Time Schedule 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 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.

16.6.5. Transcoder Model

The transcoder dial plan model allows the administrator to define an unlimited number of transcoders.

Dp Transcoder				Add	Delete	Help	Action ▾
■	Dial Plan Name ^	Conference Bridge Name	Hierarchy				
<input type="checkbox"/>	Site_Level_DP	{{ fn.sub_string macro.SITENAME, 3,4 }}_XCODE_R1	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}_XCODE	sys.hcs				

Dp Transcoder [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▾
Dial Plan Name	Tiered_Cust_Level_DP ▾					
Transcoder Type	Cisco IOS Media Termination Point ▾					
Transcoder Name	{{ macro.DP_CustomerName }}_XCODE					
Description	{{ macro.DP_CustomerName }} Transcoder					
Device Pool	{{ macro.DP_CustomerName }}-DP					
Use Trusted Relay Point	Default ▾					

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 VOSS 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

16.6.6. Conference Bridge Model

The Conference Bridge dial plan model allows the administrator to define an unlimited number of Conference Bridges.

Dp Conf Bridge			Add	Delete	Help	Action ▼
■	Dial Plan Name	▲ Conference Bridge Name	Hierarchy			
<input type="checkbox"/>	Site_Level_DP	{{ fn.sub_string macro.SITENAME, 3,4 }}_CFB_R1	sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}_CFB	sys.hcs			

Dp Conf Bridge [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name	Tiered_Cust_Level_DP					
Conference Bridge Type	Cisco IOS Conference Bridge					
Conference Bridge Name	{{ macro.DP_CustomerName }}_CFB					
Description	{{ macro.DP_CustomerName }} Conf Bridge					
Device Pool	{{ macro.DP_CustomerName }}-DP					
Location	{{ macro.DP_CustomerName }}-LOC					
Use Trusted Relay Point	Default					

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 VOSS 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

16.6.7. Media Resource Group Model

The Media Resource Group dial plan model allows the administrator to define an unlimited number of Media Resource Groups.

Dp Media Resource Group				Add	Delete	Help	Action ▾
■	Dial Plan Name ^	Media Resource Group Name	Hierarchy				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-MRG	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-MRG	sys.hcs				

Dp Media Resource Group [Tiered_Cust_Level_DP]				Save	Delete	Help	Back	Action ▾
Dial Plan Name	Tiered_Cust_Level_DP ▾							
Media Resource Group Name	{{ macro.DP_CustomerName }}-MRG							
Description	{{ macro.DP_CustomerName }} Media Resource Group							
Devices for this Group	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; padding: 2px 5px;"> + - × </div> <div style="padding: 2px 5px;"> Media Resource <input type="text" value="{{ macro.DP_CustomerName }}_CFB"/> </div> <div style="border-bottom: 1px solid #ccc; padding: 2px 5px;"> + - × </div> <div style="padding: 2px 5px;"> Media Resource <input type="text" value="{{ macro.DP_CustomerName }}_XCODE"/> </div> </div>							

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.

16.6.8. 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.

Dp Media Resource Group List			Add	Delete	Help	Action ▼
Dial Plan Name	Media Resource Group List Name	Hierarchy				
Site_Level_DP	{{ macro.SITENAME }}-MRGL	sys.hcs				
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-MRGL	sys.hcs				

Dp Media Resource Group List [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name	Tiered_Cust_Level_DP					
Media Resource Group List Name	{{ macro.DP_CustomerName }}-MRGL					
Media Resource Groups	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border: 1px solid #ccc; padding: 5px;"> <div style="border: 1px solid #ccc; padding: 5px;"> Media Resource Group: {{ macro.DP_CustomerName }}-MRG </div> </div> </div>					

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.

16.6.9. Route List Model

The Route List dial plan model allows the administrator to define an unlimited number of Route Lists.

Dp Route List				Add	Delete	Help	Action ▾
■	Dial Plan Name	↑	Route List Name	Hierarchy			
☐	Site_Level_DP		{{ macro.SITENAME }}-AGGR-RL	sys.hcs.VLS			
☐	Site_Level_DP		{{ macro.SITENAME }}-UNITY-RL	sys.hcs.VLS			
☐	Tiered_Cust_Level_DP		{{ macro.DP_CustomerName }}-UNITY-RL	sys.hcs			
☐	Tiered_Cust_Level_DP		{{ macro.DP_CustomerName }}-AGGR-RL	sys.hcs			

Dp Route List [Site_Level_DP] Save Delete Help Back Action ▾

Dial Plan Name:

Route List Name:

Route List Description:

Call Manager Group Name:

Route List Enabled:

Members

Route Group Name:

Selection Order:

Use Calling Party's External Phone Number:

Mask:

Calling Party Transform Mask:

Calling Party Prefix Digits (Outgoing Calls):

Called Party Discard Digits:

Called Party Transform Mask:

Called Party Prefix Digits (Outgoing Calls):

Run On Every Node:

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
- **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

16.6.10. Route Group Model

The Route Group dial plan model allows the administrator to define an unlimited number of Route Groups.

Dp Route Group			Add	Delete	Help	Action ▼
■	Dial Plan Name	Route Group Name	Hierarchy			
■	Site_Level_DP	{{ macro.SITENAME }}-LRG	sys			
■	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-RG	sys			

Dp Route Group [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name	Tiered_Cust_Level_DP					
Route Group Name	{{ macro.DP_CustomerName }}-RG					
Distribution Algorithm	Circular					
Route Group Devices	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; padding: 2px 5px;"> + - </div> <div style="padding: 2px 5px;"> Device <input type="text" value="{{ macro.CustomerName }}-AGGR-SIPTRK-P"/> </div> </div> <div style="border-bottom: 1px solid #ccc; padding: 2px 5px;"> + - </div> <div style="padding: 2px 5px;"> Device <input type="text" value="{{ macro.CustomerName }}-AGGR-SIPTRK-S"/> </div>					

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.

16.6.11. SIP Trunk Model

The SIP Trunk dial plan model allows the administrator to define an unlimited number of SIP Trunks.

Dp Sip Trunk				Add	Delete	Help	Action ▾
■	Dial Plan Name	^	SIP Trunk Name	Hierarchy			
<input type="checkbox"/>	Site_Level_DP		{{ macro.SITENAME }}-SipTrunk	sys			
<input type="checkbox"/>	Tiered_Cust_Level_DP		{{ macro.DP_CustomerName }}-SipTrunk	sys.hcs			

Dp Sip Trunk [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▾
Dial Plan Name	Tiered_Cust_Level_DP					
SIP Trunk Name	{{ macro.DP_CustomerName }}-SipTrunk					
Description	{{ macro.DP_CustomerName }} SIP Trunk					
Device Pool	{{ macro.DP_CustomerName }}-DP					
Call Classification	OffNet					
Media Resource Group List	{{ macro.DP_CustomerName }}-MRGL					
Location	{{ macro.DP_CustomerName }}-LOC					
Run On All Active Unified CM Nodes	<input checked="" type="checkbox"/>					
Inbound Call CSS	{{ macro.DP_CustomerName }}-PSTNInbound-CSS					
SIP Information	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> <input type="checkbox"/> Destination Address is an SRV </div> <div style="padding: 5px;"> Destination Address: <input type="text" value="1.2.3.4"/> Destination Address IPv6: <input type="text"/> Destination Port: <input type="text" value="5060"/> </div> </div>					
SIP Trunk Security Profile	Non Secure SIP Trunk Profile					
SIP Profile	Standard SIP Profile					

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.
- **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.

16.6.12. Partition Model

The Partition dial plan model allows the administrator to define an unlimited number of Partitions.

Dp Partition				Add	Delete	Help	Action ▼
<input type="checkbox"/>	Dial Plan Name	Partition Name	Hierarchy				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-PSTNInbound-PT	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-Unity-PT	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-INTL-PT	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-LD-PT	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-LOCAL-PT	sys.hcs.VLS				
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-PT	sys.hcs.VLS				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTERNAL-PT	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-PSTNInbound-PT	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LD-PT	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-Unity-PT	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTL-PT	sys.hcs				
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LOCAL-PT	sys.hcs				

Dp Partition [Site_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name	<input type="text" value="Site_Level_DP"/>					
Partition Name	<input type="text" value="{{ macro.SITENAME }}-PSTNInbound-PT"/>					
Partition Description	<input type="text" value="{{ macro.SITENAME }} PSTN Inbound"/>					
Partition Time Schedule	<input type="text" value="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.

16.6.13. 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 ▾
<input type="checkbox"/>	Dial Plan Name	^ CSS Name	Hierarchy			
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-PSTNInbound-CSS	sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-LD-CSS	sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-LOCAL-CSS	sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-CSS	sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	{{ macro.SITENAME }}-INTL-CSS	sys.hcs.VLS			
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-PSTNInbound-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTL-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LD-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTERNAL-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LOCAL-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Site_Level_DP	{{ macro.SITENAME }}-LD-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Site_Level_DP	{{ macro.SITENAME }}-INTL-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-CSS	sys.hcs			
<input type="checkbox"/>	Tiered_Site_Level_DP	{{ macro.SITENAME }}-LOCAL-CSS	sys.hcs			

Dp Css [Tiered_Cust_Level_DP] Save Delete Help Back Action ▾

Dial Plan Name

CSS Name

CSS Description

Partitions

Route Partition Names *
Partition Index

Route Partition Names *
Partition Index

Route Partition Names *
Partition Index

Route Partition Names *
Partition Index

Route Partition Names *
Partition Index

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.

- **Route Partition Name:** Free text field to enter valid Partition name
- **Partition Index:** Free text field to enter the numeric id for Partition order.

16.6.14. 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.

Dp Route Pattern					Add	Delete	Help	Action ▾
<input type="checkbox"/>	Dial Plan Name	Local Dialing	Route Pattern	Route Filter	Hierarchy			
<input type="checkbox"/>	Site_Level_DP		9.911		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP		9.1[2-9]XX[2-9]XXXX		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP		9.0111		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	true	{{ macro.DP_extBO }},{{ macro.DP_Exchange }}XXX		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	true	{{ macro.DP_extBO }},{{ input.areacode.areaCode}}		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP		911		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP		8000		sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP		9.[2-9]XX[2-9]XXXX		sys.hcs.VLS			
<input type="checkbox"/>	Tiered_Cust_Level_DP		9.0111		sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP		911		sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP		9.1[2-9]XX[2-9]XXXX		sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP		8000		sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP		9.[2-9]XX[2-9]XXXX		sys.hcs			
<input type="checkbox"/>	Tiered_Cust_Level_DP		9.911		sys.hcs			
<input type="checkbox"/>	Tiered_Site_Level_DP	true	{{ macro.DP_extBO }},{{ macro.DP_Exchange }}XXX		sys.hcs			
<input type="checkbox"/>	Tiered_Site_Level_DP	true	{{ macro.DP_extBO }},{{ input.areacode.areaCode}}		sys.hcs			

Dp Route Pattern [Tiered_Cust_Level_DP] Save Delete Help Back Action ▾

Dial Plan Name	Tiered_Cust_Level_DP ▾
Local Dialing	<input type="checkbox"/>
Route Pattern	9.1[2-9]XX[2-9]XXXX
Route Pattern Description	{{ macro.DP_CustomerName }} Long Distance Dialing
Route Partition	{{ macro.DP_CustomerName }}-LD-PT
Numbering Plan	
Route Filter	
Route List	{{ macro.DP_CustomerName }}-AGGR-RL
Gateway Name	
Route Option	Route this pattern ▾
Release Clause	No Error ▾
Call Classification	OffNet ▾
Allow Device Override	<input type="checkbox"/>
Provide Outside Dial Tone	<input checked="" type="checkbox"/>
Allow Overlap Sending	<input type="checkbox"/>
Urgent Priority	<input type="checkbox"/>
Authorization Level	0
Require Forced Authorization Code	<input type="checkbox"/>
Require Client Matter Code	<input type="checkbox"/>
Use Calling Party's External Phone Number Mask	Default
Calling Party Transform Mask	
Calling Party Prefix Digits (Outgoing Calls)	
Called Party Discard Digits	PreDot ▾
Called Party Transform Mask	
Called Party Prefix Digits (Outgoing Calls)	
Calling Line Presentation Bit	
Calling Name Presentation Bit	
Connected Line Presentation Bit	
Connected Name Presentation Bit	
MLPP Precedence	Default ▾

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.
- **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-#

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

16.6.15. 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.

Dp Trans Pattern				Add	Delete	Help	Action ▾
<input type="checkbox"/>	Dial Plan Name^	Local Dialing	Translation Pattern	Hierarchy			
<input type="checkbox"/>	Site_Level_DP	true	{{ input.areaCode.areaCode}}XXXX	sys.hcs.VLS			
<input type="checkbox"/>	Site_Level_DP	true	{{ input.areaCode.areaCode}}XXXXXXX	sys.hcs.VLS			

Dp Trans Pattern [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▾
Dial Plan Name	Tiered_Cust_Level_DP					
Local Dialing	<input type="checkbox"/>					
Translation Pattern	6560000000					
Partition	{{ macro.DP_CustomerName }}-LD-PT					
Translation Pattern Description	656 digit dialing translation pattern					
CSS	{{ macro.DP_CustomerName }}-INTERNAL-CSS					
Use Originator's Calling Search Space	<input type="checkbox"/>					
Route Option	Route this pattern					
Release Clause	No Error					
Provide Outside Dial Tone	<input checked="" type="checkbox"/>					
Urgent Priority	<input type="checkbox"/>					
Do Not Wait For Interdigit Timeout On Subsequent Hops	<input type="checkbox"/>					
Route Next Hop By Calling Party Number	<input type="checkbox"/>					
Use Calling Party's External Phone Number Mask	<input type="checkbox"/>					
Calling Party Transform Mask						
Calling Party Prefix Digits (Outgoing Calls)						
Calling Line Presentation Bit	Default					
Calling Name Presentation Bit	Default					
Connected Line Presentation Bit	Default					
Connected Name Presentation Bit	Default					
Called Party Transform Mask						
Called Party Discard Digits						
Called Party Prefix Digits (Outgoing Calls)						

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
 - 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.

16.6.16. 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.

Dp Route Pattern [Site_Level_DP] Save Delete Help Back Action ▾

Dial Plan Name

Local Dialing

Route Pattern

Route Pattern Description

Route Partition

Numbering Plan

Route Filter

Route List

Gateway Name

Route Option

Release Clause

Call Classification

Dp Trans Pattern [Site_Level_DP] Save Delete Help Back Action ▾

Dial Plan Name

Local Dialing

Translation Pattern

Partition

Translation Pattern Description

Css

Use Originator's Calling Search Space

Route Option

Release Clause

16.6.17. 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.

Dp Cti Route Point					Add	Delete	Help	Action ▼
■	Dial Plan Name	^	Device Name	Description	Hierarchy			
■	Site_Level_DP		TestCTIRP1	Test CTI Route Point 1	sys.hcs.VLS			
■	Site_Level_DP		TestCTIRP2	Test CTI Route Point 2	sys.hcs.VLS			
■	Tiered_Cust_Level_DP		TestCTIRP1	Test CTI Route Point 1	sys.hcs			
■	Tiered_Cust_Level_DP		TestCTIRP2	Test CTI Route Point 2	sys.hcs			

Dp Cti Route Point [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▼
CTI Route Point		Associated Line				
Dial Plan Name*	Tiered_Cust_Level_DP ▼					
Device Name*	TestCTIRP1					
Description	Test CTI Route Point 1					
Device Pool*	Default					
Calling Search Space	{{ macro.DP_CustomerName }}-LD-CSS ▼					
Location	Hub_None					
Use Trusted Relay Point*	Default ▼					
Calling Party Transformation CSS	{{ macro.DP_CustomerName }}-LD-CSS ▼					
Geolocation	unspecified					
Use Device Pool Calling Party Transformation CSS	<input checked="" type="checkbox"/>					

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:

- 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.

Dp Cti Route Point [Tiered_Cust_Level_DP] Save Delete Help Back Action ▾

CTI Route Point Associated Line

CTI Route Point DN	<input type="text" value="1999"/>
CTI Route Point Line Description	<input type="text" value="Line 1999 CTI Route Point"/>
CTI Route Point Line Partition	<input type="text" value="{{ macro.DP_CustomerName }}-INTERNAL-PT"/>
CTI Route Point Line CSS	<input type="text" value="{{ macro.DP_CustomerName }}-LD-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.

16.6.18. Called Party Transformation Model

The Called Party Transformation dial plan model allows the administrator to define an unlimited number of Called Party Transformations.

Dp Called Party Transformation [Site_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name	Site_Level_DP					
Pattern*	**111					
Description	Transform 1111					
Route Partition	{{ macro.SITENAME }}-INTERNAL-PT					
Discard Digits						
Called Party Transformation Mask	2143360552					
Called Party Prefix Digits	3280					
Called Party Number Type	Cisco CallManager					
Called Party Numbering Plan	Cisco CallManager					

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

- National
- International
- Subscriber
- **Called Party Numbering Plan:** Drop-down providing Call Manager options:
 - Cisco CallManager
 - ISDN
 - National Standard
 - Private
 - Unknown

16.6.19. Calling Party Transformation Model

The Calling Party Transformation dial plan model allows the administrator to define an unlimited number of Calling Party Transformations.

Dp Calling Party Transformation [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name	Tiered_Cust_Level_DP					
Pattern*	2143560001					
Description	Test calling Party TP					
Partition	{{ macro.DP_CustomerName }}-INTERNAL-PT					
Use Calling Party's						
External Phone	Default					
Number Mask						
Calling Line ID						
Presentation*	Default					
Calling Party						
Transform Mask	123456					
Calling Party Prefix						
Digits (Outgoing Calls)	9988					
Calling Party Discard						
Digits						
Calling Party Number						
Type*	Cisco CallManager					
Calling Party						
Numbering Plan*	Cisco CallManager					

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:

- 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
 - Subscriber
- **Called Party Numbering Plan:** Drop-down providing Call Manager options:
 - Cisco CallManager
 - ISDN
 - National Standard
 - Private
 - Unknown

16.6.20. SIP Route Pattern Model

The SIP Route Pattern dial plan model allows the administrator to define an unlimited number of SIP Route Patterns.

Dp Sip Route Pattern [Tiered_Cust_Level_DP]		Save	Delete	Help	Back	Action ▼
Dial Plan Name*	Tiered_Cust_Level_DP					
Pattern*	sip:7654321@vls.com					
Description	SIP Route Pattern 7654321					
Usage*	Domain Routing					
Route Partition*	{{ macro.DP_CustomerName }}-LD-PT					
Route Option	Route this pattern					
Calling Party Transformation Mask						
Use Calling Party's External Phone Number Mask	Default					
Calling Party Prefix Digits (Outgoing Calls)						
Calling Line Presentation Bit	Default					
Calling Name Presentation Bit	Default					
Connected Line Presentation Bit	Default					
Connected Name Presentation Bit	Default					
Sip Trunk/Route List Name *	{{ macro.DP_CustomerName }}-AGGR-RL					
Dn or Pattern IPv6						
Route On User Part	<input type="checkbox"/>					
Use Caller CSS	<input checked="" type="checkbox"/>					
Domain Routing Css Name						

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.

- **Pattern:** Free text field to allow entry in standard Call Manager patterns uri patterns.
- **Description:** Meaningful description of the SIP Route Pattern.
- **Usage:** Drop-down 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:
 - 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.

16.7. 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	ndf	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	0	sys.hcs	Add						Tiered_Cust_Level_DP Global Dial Plan E	
7	##									
8	##									
9	##	Device Pool - Region - Location - SRST Reference								
10	entity: data/DP_DP-Reg-Loc; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template:									
11		hierarchy	action	search_fields	device	template	ndf	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	ndf	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	

16.8. 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
<input type="checkbox"/>	2017-06-29 20:05:57.931482	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
<input type="checkbox"/>	2017-06-29 20:39:03.092865	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
<input type="checkbox"/>	2017-06-29 20:44:48.719970	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
<input type="checkbox"/>	2017-06-29 20:47:13.973042	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
<input checked="" type="checkbox"/>	2017-06-29 20:48:13.449928	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
<input type="checkbox"/>	2017-06-29 20:53:32.707848	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
<input type="checkbox"/>	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
- 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.

16.9. Dial Plan Use Checklist

- 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 Call Manager 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 Call Manager 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.

17. Microsoft Teams Dial Plan Management

17.1. Introduction to Microsoft Teams Dialplan Management

To view and update information related to Microsoft Teams dial plans, go to (default menu) **MS Teams Dial Plan Management**, and select the relevant menu:

- Tenant Dialplan
- SBC Gateways
- PSTN Usages
- Voice Routes
- Voice Routing Policies
- Voice Normalization Rules
- Translation Rules

17.1.1. Related Topics

- Microsoft Overview in the Core Feature Guide
- Sync with Flow Through in the Core Feature Guide
- VOSS Automate Configuration and Sync in the Core Feature Guide
- Configure Microsoft Tenant Dialplan in the Core Feature Guide
- Number Management Overview in the Core Feature Guide

17.2. Configure Microsoft Tenant Dialplan

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 subscriber via Quick Add Subscriber, 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 (default menu) **MS Teams Dial Plan Management > Tenant Dialplan**.
3. View existing tenant dialplans.
4. Choose an option:
 - To edit an existing dialplan, click on a dialplan to open the editing screen. Make your changes, then save the dialplan.
 - 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.

17.2.1. Related Topics

- Configure Microsoft Connection Parameters in the Core Feature Guide
- Introduction to Microsoft Teams Dialplan Management in the Core Feature Guide
- Microsoft Overview in the Core Feature Guide
- Microsoft Configuration in the Core Feature Guide
- Sync with Flow Through in the Core Feature Guide
- VOSS Automate Configuration and Sync in the Core Feature Guide

18. Microsoft Teams Policies

18.1. Introduction to Microsoft Teams Policies

Microsoft Teams policies are synced between Microsoft Teams and VOSS Automate, to the customer level.

VOSS Automate provides an interface for managing Microsoft Teams policies. Updates in VOSS Automate are synced back to Microsoft Teams, and external changes are synced back to VOSS Automate.

You can view and choose default policies for sites in the site defaults via (default menus) **Site Management > Defaults** (and select the **MS Teams** tab).

Microsoft Teams policies are assigned automatically to subscribers via their user roles and profiles, and via quick add groups (QAG), as part of the initial sync and provisioning workflow.

To manage Microsoft Teams policies, go to (default menu) **MS Teams Policies**; then, select the relevant menu, for example:

- 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 Routing Policy
- Voicemail Policy
- Audio Conferencing Policy

Note: Some policies support full CRUD (create, update, delete) operations within VOSS Automate.

Manage a Subscriber's MS Teams Policies

To view and update the policies of individual subscribers via the Subscriber edit functionality:

Note: Some policies support full CRUD (create, update, delete) operations within VOSS Automate.

1. Go to (default menu) **Subscriber Management > Subscribers**.
2. Click on a subscriber to open the Subscribers [subscriber name] page.
3. Select the **MS Teams** tab.
4. View currently applied policies for the subscriber.
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.

Related Topics

- Microsoft Subscribers in the Core Feature Guide

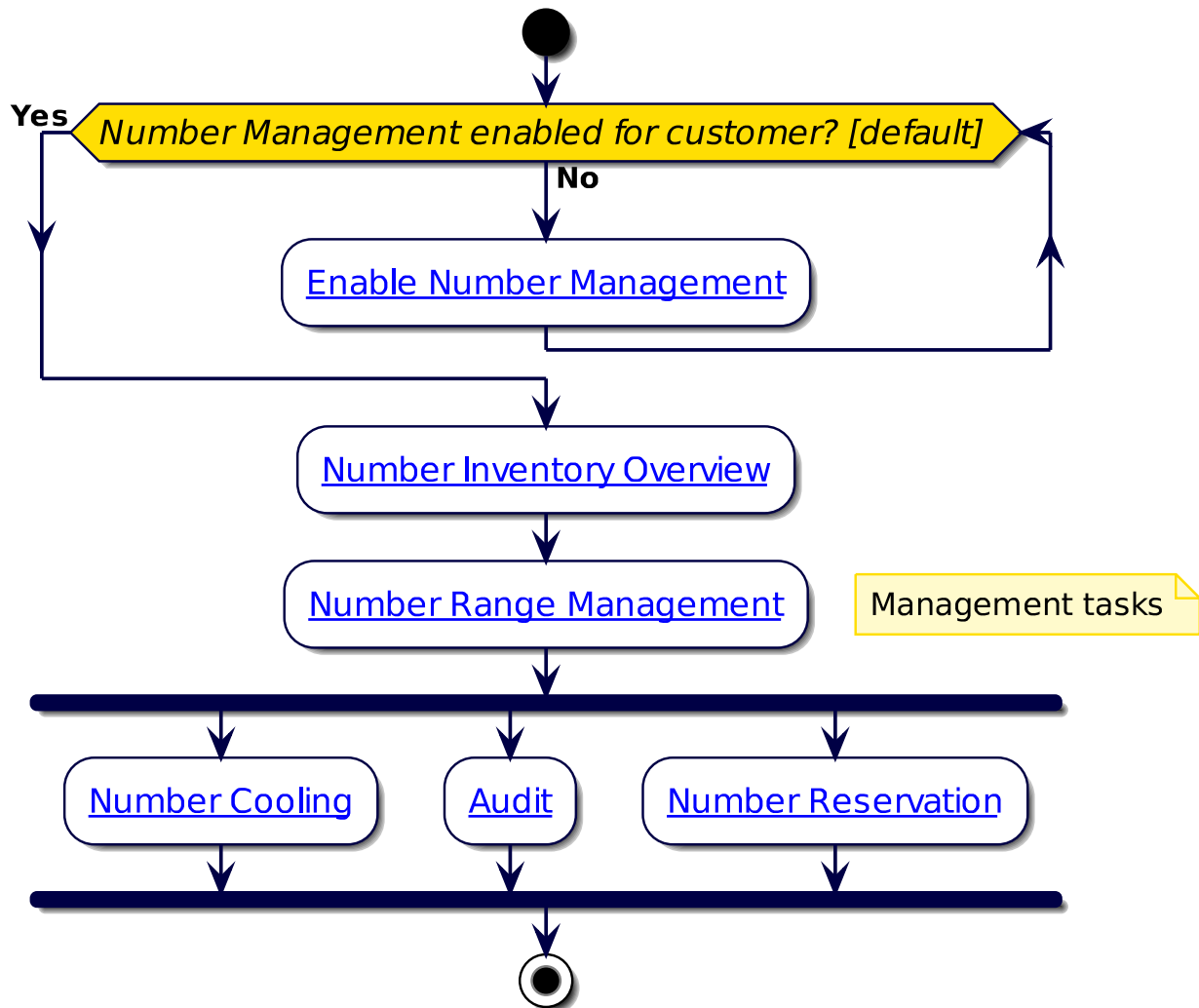
19. Number Management

Important: When upgrading from 19.X or earlier, refer to the *VOSS-4-UC 21.1 Release Changes and Impact* document for details on model and workflow changes. Customizations related to these changes may be affected.

When upgrading from 19.X or earlier, refer to the VOSS-4-UC 21.1 Release Changes and Impact PDF available on the Documentation Portal.

19.1. Number Inventory

- Note: Underlined flowchart titles refer to topic headings in this guide.



19.2. Number Inventory Overview

19.2.1. Overview

The number inventory (directory number inventory) allows you to view and manage the number inventory at the specified hierarchy level. You can track numbers to see how they're used in the system. Workflows in VOSS Automate ensure the selection of numbers is limited to those available, and includes the ability to:

- Add, modify, and delete numbers
- View the status of numbers (Used, Used-Utility, Available, Reserved, Cooling).
- Store additional business data about the numbers.

Note:

- To view the number inventory, go to (default menus) **Number Management > Number Inventory**.

- Internal numbers can't be added if **Number Management** is disabled for the customer. (See *Create and Modify a Customer*)
- Numbers created in the number inventory are in VOSS Automate only; they are not synced to Cisco Unified Communications Manager (CUCM, or CallManager).

Related Topics

- [Number Status and Usage](#)
- [Number Cooling](#)
- [Number Reservation](#)

19.2.2. Hierarchy

The number inventory can exist at a different hierarchy level to the lines for the users, services, and devices that consume them, which are typically at site level.

The inventory can also exist at customer level. This makes it easier if the allocation and availability of numbers is not site-specific. This saves moving numbers around sites to increase availability, and keeps a more central inventory of available numbers. It is also important if numbers are shared across sites. If you are a customer with multiple sites, ensure that the internal numbers you specify are unique across sites.

If the number allocation is site-specific, the numbers can be added or assigned to site level.

Note: The number inventory can only exist at Provider, Customer, or Site hierarchy. It is not applicable to the intermediate hierarchy.

19.2.3. Partition and Cluster

Number inventory is not partition or cluster aware. If the same numbers are used multiple times but in different partitions, then these all map to the same number. This should be taken into account when thinking about the hierarchy level at which the number inventory exists.

Also, not being cluster aware, if the same number exists on different clusters, this again will map back to the same inventory value unless numbers are assigned to the site level.

19.2.4. Reservation

Numbers can be reserved for future use. For example, for users who will soon be joining the company. When a number is reserved, it is unavailable and cannot be allocated to a subscriber, phone, device, etc.

19.2.5. Number Cooling

Numbers can be placed into a cooling period, either manually or automatically. 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.

Note: Automated number cooling is enabled and disabled in the *Global Settings*. The default is disabled.

While the number is in its cooling period, it is unavailable and cannot be allocated, for example, 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
- It is manually released from the cooling period

19.2.6. Number Inventory entries - End-user Provisioning Tasks

For more information on provisioning each of these tasks, refer to the relevant topics in the VOSS Automate Core Feature Guide.

Task	Menu Default Location	Notes
Lines	Subscriber Management > Lines	When lines are added through phones and subscriber, line details can be modified. The number for the line cannot be modified; if you attempt to change the number assigned to the line, the operation fails.
Phones	Subscriber Management > Phones > Lines tab > Dirn > Pattern	The Dirn > Pattern contains a list of available numbers. Numbers that are used are marked as “Used” in the Number Inventory. Only available numbers are listed.
Subscribers	Subscriber Management > Subscribers > Phones > Lines > Dirn	The Dirn > Pattern contains a list of available numbers. Numbers that are used are marked as “Used” in the Number Inventory. Only available numbers are listed.
	Subscriber Management > Subscribers > Voicemail	The “Voicemail Line” list contains numbers provisioned to lines.
Quick Add Subscribers	Subscriber Management > Quick Add Subscriber > Lines > Directory Number	The Number Inventory list contains available numbers. Numbers that are used are marked as “Used” in the Number Inventory. Only available numbers are listed.
PLAR (Hotdial)	Subscriber Management > PLAR (Hotdial)	Numbers provisioned to lines are displayed in the Hotdial Destination Pattern list. Numbers that are used are marked as “Used-Utility” in the Number Inventory.
Hunt Groups	Subscriber Management > Hunt Groups > Members > Directory Number	Numbers provisioned to lines are displayed in the Pattern list. Numbers that are used are marked as “Used-Utility” in the Number Inventory.
Call Pickup Groups	Subscriber Management > Call Pickup Groups > Call Pickup Group > Line	Numbers provisioned to member lines are displayed in the Pattern list. Numbers that are used are marked as “Used-Utility” in the Number Inventory.

19.3. View the Number Inventory

The **Number Inventory** list view (default menu **Number Management > Number Inventory**) displays the range of numbers that have been defined for the selected hierarchy.

Here you can view the list of numbers, delete a number, or select a number and edit the free text fields. Filter the numbers (by column) as needed.

To work with a specific number, click on the number in the list view to open its’ editing screen. See: [Number Range Management](#).

The table describes column values in the Number Inventory list view:

Column	Description
Internal number	Numbers created in the number inventory are in VOSS Automate only. These are not synced to Cisco Unified Communications Manager (CUCM / CallManager).
Status	Current status of the number. Options are: <ul style="list-style-type: none"> • Available • Used-Utility • Used • Cooling • Reserved
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 (when number cooling is enabled) the date on which a number that is currently in 'cooling' will become available.
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.
Reservation notes	A free text field, typically used to provide more details about a status Reserved number.
Vendor	Optional, typically used to designate vendor-specific information for a device in a multi vendor setup.
Internal Number Type	If Vendor = "Microsoft", then for connectivity options with MS Teams and Phone System, any of: "Direct Routing", "Calling Plan", "Operator Connect". The value can be managed and is used to determine user configuration when the number is assigned. If Vendor = "Cisco", then blank.
Extra	Extra1 to Extra9 fields are free text fields that are available to provide additional information for a given number or range of numbers.
Located At	The hierarchy where the number exists.

Related Topics

- [Number Range Management](#)
- [Number Reservation](#)
- [Number Status and Usage](#)
- [Number Cooling](#)

19.4. Number Status and Usage

Values in the **Status** and **Usage** columns in the Number Inventory allow administrators to understand how numbers are used at a specific hierarchy level.

Note: To access the Number Inventory, go to (default menus) **Number Management > Number Inventory**.

The table describes values in the **Status** and **Usage** columns in the Number Inventory:

Number Use	Device	Status	Usage	Vendor 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/RemoteDestinationProfile (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_DATA	Used-Utility	VOSS_Phone	phoneVendor
MS Teams Line URI	device/msteamsonline/CsOnlineUser (LineURI)	Used	User	Microsoft
Not used by anything		Available	blank	Microsoft ³
Number in cooling ⁴		Cooling	-	blank
Number reserved ⁵		Reserved	-	blank

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, i.e. 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

Related Topics

For details on call handlers and shared numbers, see Auto-Attendant Call Handler in the Core Feature Guide.

19.4.1. Cisco-Microsoft Hybrid Number Inventory

A Cisco-Microsoft hybrid setup is an integration of Cisco and Microsoft capability where we route Microsoft calls via Cisco Unified CM.

In a hybrid setup, the Internal Number Inventory (INI) can be set up in 2 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: The named macro called *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.

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 [Audit Number Inventory](#). In this case, an update of the inventory takes place so that these are not counted as two separate numbers.

The table below sums up the Number Inventory data for these cases.

Note that **Extra2** and **Extra4** hold the service type and E164 number (includes generated) respectively.

devices were added first to the number. Usage will typically be `Call_Handler_Pilot,Device`.

³ For Microsoft, number type: Operator Connect or Calling Plan.

⁴ If a number is currently in **Cooling**, the release date indicates when the number will come out of cooling.

⁵ 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.

Scenario	Status	Vendor	E164 Number ^{Page 601, 6}	Usage	Extra2	Extra4
Cisco-MS-Hybrid	Used	Cisco, Microsoft	Exists	Device, User	Cisco-MS-Hybrid	<blank>
Cisco-MS-Hybrid ⁷	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

19.4.2. Details and Usage

Selecting a specific number from the **Number Inventory** list view, opens the details view for that number.

The **Number Details** tab shows read only details for the number, for example Internal Number, Status, Usage, as well as editable fields such as Tag, Description, Reservation Notes, etc. In the case of Cisco-Microsoft hybrid entries, the vendor added would be “Cisco, Microsoft”.

The **Usage** tab provides links to all instances where the number is used. In the case of Cisco-Microsoft hybrid usage, the last vendor added would be appended, as seen above in the “Device, User” instances.

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.

⁶ If assigned (and associated with Extra4 - prefix e.g. +88800)

⁷ Generated TelURI will start with prefix e.g. +88800

19.5. Number Range Management

19.5.1. Overview

The Number Range management feature allows you to create a range of internal numbers at a customer or site level.

When adding a range that includes existing numbers, these cannot be modified. New unused numbers will be added only to complete the range. In other words, the range will show up as complete, with unused numbers in between numbers imported from Unified CM.

Number ranges can also be deleted. Numbers in the range that have a status of **Used**, **Used-Utility**, **Reserved** or **Cooling** will be ignored and can not be deleted. If these numbers are modified to the **Available** status, and not in use, they can then be deleted. The **Available** and **Reserved** status of numbers can also be modified manually once they are added.

Note:

- Using bulk loader sheet or 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.
-

19.5.2. Add, Modify, or Delete a Number or Number Range

Numbers can be added 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.

Since the number inventory is not partition aware, if the same directory number is used on a cluster but in different partitions, then VOSS Automate workflows will update the inventory when *any* of those instances are changed. For instance, if there is a number 1111 in the Cluster X partition and a number 1111 in the Cluster Y partition, then the number is marked as **Used**.

If one of those instances are deleted, we check to see if there are other instances of that line based on the number only (not partition), before clearing the **Used** flag. In this case, the other instance will be found and the inventory will stay marked as **Used**.

1. Browse to the hierarchy at which you want manage the number range.
2. Open the **Number Range Management** form (default menu **Number Management > Number Range Management**) and choose the target site from the **Target Site** drop-down (only applicable to Customers using an SLC-based dial plan).
3. From the **Operation** drop-down, choose **Add**, **Modify** or **Delete**.

Note:

- When adding or modifying a number range, the **Status** of the numbers is **Available** by default. However you can change this to **Reserved** from the **Status** drop-down. If set to **Reserved**, you can also enter the **Reservation duration (days)** value, e.g. 30, after which period the number/s will return to the **Available** status. If this value is left blank, the number/s will be reserved indefinitely. See also [Number Reservation](#).

- When deleting a number range, lines cannot be marked as **Available** or **Reserved**, and the check boxes are hidden.

4. Enter the **Starting Extension** and **Ending Extension**. The maximum allowed range is 1000 for a single action. The starting extension should always be smaller than the ending extension.

If you are adding or deleting a single number, the starting and ending extension number will be the same. If numbers in the range already exist, they will not be affected - only non-existing numbers will be added.

5. If **Vendor** is “Microsoft”, then **Internal Number Type** can be set.
6. **Internal Number Type**: If **Vendor** is “Microsoft”, then for connectivity options with MS Teams and Phone System, the drop down value can be any of: “Direct Routing”, “Calling Plan”, “Operator Connect”. The value can be managed and is used to determine user configuration when the number is assigned. If **Vendor** = “Cisco”, then blank.
7. Edit free text fields, for example **Tag**, **Description**, **Reservation notes** **E164Number** (if applicable), and **Extra1** to **Extra9**.
8. Click **Save** to save the single or range of numbers that you added, modified or deleted. If a number in a deleted range was set as **Used**, it will not be deleted.

The numbers at a specific hierarchy can be viewed on the **Number Inventory** list view (default menu **Number Management > Number Inventory**). See [View the Number Inventory](#).

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](#).

If number cooling is enabled, deleted numbers are automatically placed into a cooling period as specified in [Global Settings](#). During this period the number cannot be used.

Internal numbers are available when adding subscribers.

19.5.3. Modify an individual number

You can also modify an individual number from the list view ([View the Number Inventory](#)) by selecting it.

1. Click **Reserve Number** on the button bar of the number instance form to reserve it.
2. Edit free text fields, for example: **Tag**, **Description**, **Reservation notes**, **E164Number** (if applicable), and **Extra1** to **Extra9**.
3. Click **Save**.

19.5.4. Persisting and Modifying Values in Extra Fields

Note the following properties of the extra fields **Extra1** to **Extra9**:

- When managing the Number Inventory, users can modify the fields **Extra1** to **Extra9**.
- When the status of a number changes from for example **Used** to **Available** (for example, when an associated device is unassociated with the line), then any values originally of the fields **Extra1** to **Extra9** remain unchanged by default.

- A default custom Configuration Template (CFT) called **IniUpdateCustomCFT** that applies to data/InternalNumberInventory is available to clone to the user hierarchy and then to modify the custom persistence of extra field values. For details on CFT cloning and custom configuration, refer to 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.
 - Users of the VOSS Automate Hybrid or Multi-vendor functionality and who upgrade to VOSS Automate Release 21.3-PB3 should clone this CFT and populate it as specified in the *Method of Procedure (MOP) for 21.3 Patch Bundle 3 Installation and Upgrade Notes for VOSS Automate 21.3 Patch Bundle 3*.
-

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 VOSS Automate feature usage.

For details, see the **Number Inventory Flexibility and Description Customization** topic in the Advanced Configuration Guide.

- This CFT cannot be used to modify any other VOSS managed fields in data/InternalNumberInventory.

19.6. Number Cooling

19.6.1. 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 & Reservation** form (default menu **Number Management > Cooling & Reservation**) 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).

 [Enable Cooling](#)

 [Manage Cooling](#)

Related Topics

- [Global Settings](#)
- [Number Inventory Overview](#)
- [Audit Number Inventory](#)
- Number Cooling Auto Expiry Schedule in the Advanced Configuration Guide

19.6.2. 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 (default menus) **Number Management > Cooling & Reservation**.
3. On the **Cooling & Reservation** page, choose **Apply cooling** from the **Select action** drop-down.
4. Enter an optional cooling duration in days (max = 999) to apply to the selected numbers. This setting overrides the value set in their global settings. If this field is left blank, then the cooling duration set in [Global Settings](#) for each number will apply.
5. Set **Filters** to determine which numbers will be included 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 won't display used numbers; that is, it only display unused and available numbers.

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.

19.6.3. 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 (default menus) **Number Management > Cooling & Reservation**.
3. On the **Cooling & Reservation** form, choose **Remove from cooling** from the **Select action** dropdown.
4. Set **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.

19.7. Number Reservation

19.7.1. Overview

Number reservation allows numbers to be reserved for future use. Reserved numbers cannot be allocated to a device or line.

The **Cooling & Reservation** list view (default menu **Number Management > Cooling & Reservation**) 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 Overview](#)
- [Audit Number Inventory](#)
- [Number Cooling](#)

19.7.2. Reserve Numbers

1. In the Admin Portal, choose the relevant hierarchy level (Provider, Customer or Site) where you want to reserve numbers.
2. Go to (default menus) **Number Management > Cooling & Reservation**.
3. On the **Cooling & Reservation** page, at the **Select action** drop-down, select **Reserve**.
4. At **Reservation duration (days)**, define the number days to reserve the number/s.
5. Enter **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.
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.
 - 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 (default menu **Number Management > Number Inventory**) by clicking on the required number on the list view and then selecting **Reserve Number** on the button bar.

19.7.3. 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 (default menus) **Number Management > Cooling & Reservation**.
3. On the **Cooling & Reservation** page, choose **Unreserve** from the **Select action** drop-down.
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.

19.8. Audit Number Inventory

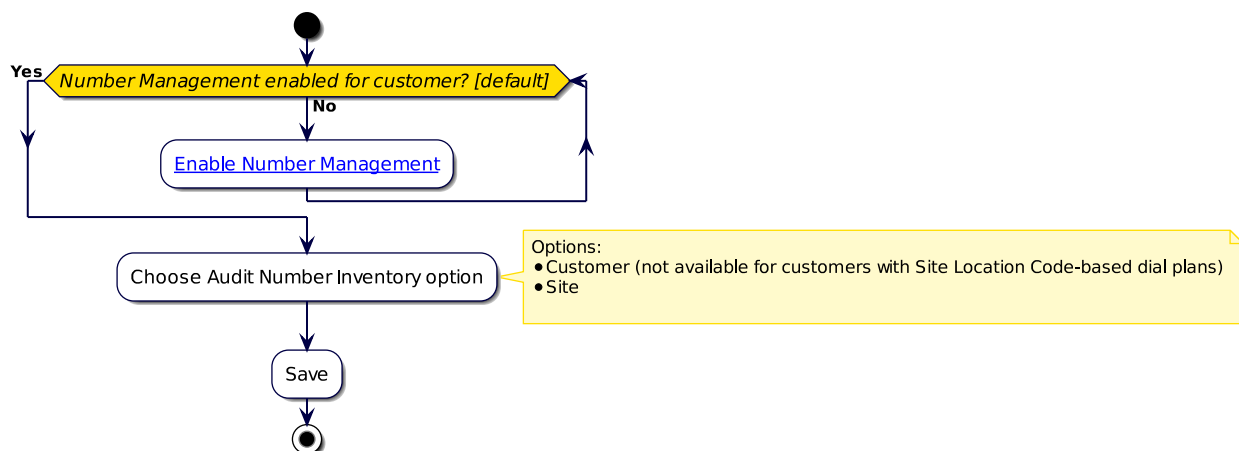
Note: You cannot run **Audit Number Inventory** if number management has been disabled for the customer (see *Create and Modify a Customer*).

This feature performs an audit of the number inventory and makes sure that the **Status** and **Usage** of each number aligns to the devices or services configured with these matching numbers. See *Number Status and Usage* for more details about these values.

For Microsoft environments, available numbers are added (else updated if present) to the inventory, with:

- status: Available
- vendor: Microsoft
- number type: Operator Connect or Calling Plan

The audit will create new numbers for devices or services that don't already exist, as well as update existing number entries to make sure the **Status** and **Usage** fields reflect the correct information at the time the audit is run. Number entries **will not be deleted**.



Specify where you want to run and create a new number inventory:

- **Customer**
 - Running the number inventory audit at **Customer** level will add directory numbers at Customer level for services which exist at Site or Customer, **provided 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 will also get 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 will only add and update 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 will add directory numbers at site level, and update 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.

For sites using Site Location Code-based dial plans, number inventories can be created only at the site hierarchy, the customer hierarchy will not be available.

From the **Number Inventory** form (default menu **Number Management > Number Inventory**), you can see a list of internal numbers and move, delete, and export them as desired.

19.8.1. Common Errors and Caveats

- Error: Duplicate device profiles (same profile name) in different clusters.
Resolution: Ensure device profiles are not duplicated across the sites.
- Error: Duplicate phones (same MAC) in different clusters.
Resolution: Ensure phones are not duplicated across the clusters
- Error: Same internal number in one or more clusters.
Resolution: Ensure internal numbers (even in different partitions) are not duplicated across clusters.
- Numbers that are in a Cooling or Reserved state will not be audited.

19.8.2. Run Audit Number Inventory

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.

1. Log in to VOSS Automate as provider or reseller administrator.
2. Open the **Audit Number Inventory** form (default menu **Number Management > Audit Number Inventory**).
3. Browse to the customer hierarchy at which you want to run **Audit Number Inventory**.
4. Choose either **Customer** or **Site** from the **Is Number Inventory deployed at Customer or Site Level ?** drop-down.
5. If you chose **Customer**, click **Save** to run **Audit Number Inventory** at all sites that are located under the selected customer.
6. If you chose **Site**, choose either **All** from the **Would you like to audit all sites or a subset of sites ?** to run **Audit Number Inventory** at all the sites under the selected customer, *or* choose **Specific** and specify the sites on which you want to run **Audit Number Inventory** (200 maximum).

7. Click **Save**. The number inventory is updated at the hierarchy you specified and below.

20. Unity SIP Integration

20.1. Overview

20.1.1. Introduction to Unity SIP Integration

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 the Optional Features Appendix: 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

20.2. Administration GUI Menus

20.2.1. Unity SIP Integration

The Unity SIP Integration feature can be used in place of your existing voicemail service. A list of menu 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.

Menu Name	Description and Notes
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.

20.2.2. Integrate Unity-Call Manager

This option allows you to create a SIP Integration between Cisco Unified Call Manager (CUCM) and Cisco Unity Connection (CUC).

Base

Note: Prior to completing this form, the **Provisioning Target Call Manager**, the **Provisioning Target Unity**, and the **Voicemail Service Dial Plan Profile** must be set. Based on these selections, other key values are auto populated on the form.

Complete, at minimum, the mandatory fields (red border):

UC Publisher Application Selection

- **Provisioning Target Call Manager** - Choose from the drop-down list.
- **Provisioning Target Unity** - Choose from the drop-down list.

Deployment Options

- **Voicemail Service Dial Plan Profile** - Choose from the drop-down list.
- **Dial Plan Advanced Mode** - Select this check box to unlock the fields for dial plan elements. You then have the ability to update those values 'live'.

Clear the check box to return the dial plan elements to the default voicemail dial plan profile values. This check box can be hidden from lower level administrators.

- **Provision CUCM-Unity in Redundant Mode** - Clear this check box for the 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 check box 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.

- **Unity Tenant(s) Present** - If the selected 'Provisioning Target Unity' server (see under **UC Publisher Application Selection** above) has tenants on it, this check box is automatically selected.

CUCM Global

- **SIP Profile** - To assign the configured settings in this SIP profile to the associated device.
- **SIP Trunk Security Profile** - To assign a single security profile to multiple SIP trunks in order to apply the configured settings to the SIP trunks.

These fields are auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.

Unity Port Group

Complete, at minimum, the mandatory fields (red border):

- **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

Complete, at minimum, the mandatory fields (red border):

- **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** -

CUCM Voicemail Pilot

Complete, at minimum, the mandatory fields (red border):

- **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

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

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**.

CUCM Route Group

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

Complete, at minimum, the mandatory fields (red border):

- **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

This tab is only visible if the **Provision CUCM-Unity in Redundant Mode** check box on the **Base** tab is selected.

Complete, at minimum, the mandatory fields (red border):

- **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.

20.2.3. Dial Plan Profile

This allows an advanced administrator to define all of the dial plan elements that make up the CUC integration.

Mandatory fields include; SIP Profile, SIP Trunk Security Profile, Device Pool, Route Group, Route List, SIP Trunk Inbound CSS, Call Manager Group and Voicemail Pilot CSS.

This form can be filled with static (exact) values if you want to deploy these same values over and over at Store level. This option is typically not used and is displayed for illustrative purposes only.

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.

Note: You can only add a SIP integration once a Dial Plan Profile has been configured.

20.2.4. Remove Integrate Unity-CallManager

This tool (**Unity SIP Integration > Remove Integrate Unity-CallManager**) takes the complete selected SIP integration back out of the Cisco Unified Call Manager (CUCM) and Cisco Unity Connection (CUC).

From the **Integration Label** drop-down, choose the integration that you want to remove and click **Save**.

20.2.5. Unity Tenant Management

Unity Tenant Management assists in creating groups of objects in Unity Connection that provide a basic “tenant services” application. In short 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.

You can add or delete unity tenants.

Add a Unity Tenant

Note: The description, alias and SMTP Domain name must all be unique among tenants in your system.

1. Choose **Unity Tenant Management > Unity Tenant Add** to open the **Unity Tenant Add** form.
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 make sure all objects in Connection are uniquely named.
 - **SMTP Domain** - a unique SMTP Domain name.
 - **Tenant Description** - .
3. Click **Save**.

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. Choose **Unity Tenant Management > Unity Tenant Delete** to open the **Unity Tenant Delete** form.
2. From the **Unity Tenant Name (Alias)** drop-down, choose the tenant to delete.
3. Click **Save** to remove the tenant.

20.2.6. Integration Log

This tool (**Unity SIP Integration > Integration Log**) will be populated with all the details relevant to the SIP Integration.

This includes when the integration was pushed, and other details so that the integration can be pushed back out again if required.

21. Teams Emergency Management

21.1. Teams Emergency Locations

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.

For your organization's physical location (civic address), more than one emergency dispatch location (e.g. parts of a building) can be set up.

Select **Teams Emergency Management > Teams Emergency Locations** to manage the location of your organization on the **Address** tab, as well as its associated places on the **Locations** tab.

21.1.1. Address tab

Note: For the address, the geo code (**Latitude** and **Longitude**) associated with it is mandatory. Ports cannot be added to a location at an address without latitude and longitude.

When adding a physical civic address, a default emergency location is added (**Is Default** is enabled, read-only for the location).

21.1.2. Locations tab

Additional specific location can be added, and data from the Location Information Server (LIS) can be also be added, such as subnet, port, switch, WAP (Wireless Access Point).

ELIN refers to the Emergency Location Identification Number.

Note: The default location cannot be deleted from the list of locations associated with a physical civic address. The default is only removed when the physical civic address is deleted.

Related Topics

- [Teams Emergency Location Networks](#)

21.2. Teams Emergency Location Networks

VOSS Automate allows for the *view only* of Microsoft Teams emergency location networks for emergency calling.

Higher level administrators can manage these networks directly from the device models on the menu: **Network Site**, **Network Subset** and **Trusted IP Address**.

Select **Teams Emergency Management > Teams Emergency Location Networks** to see the configured emergency location networks. The **Emergency Calling Policy** and **Emergency Call Routing Policy** associated with the networks are also shown.

Each Emergency Location Network can have on or more subnets configured. These are shown on the **Subnets** tab.

22. Subscriber Management

22.1. Cisco Subscriber Management

22.1.1. View and Manage Subscribers

Overview

This section describes how to:

- View a list of all subscribers
- Add a subscriber
- Update a subscriber
- Delete a subscriber

Related Topics

- Multi Vendor Subscribers in the Core Feature Guide

View Subscribers

In the Admin Portal, you can view a summary list of all subscribers (at the current hierarchy and down), which includes details of each subscriber's currently provisioned services, grouped by vendor.

To view subscribers in the Admin Portal, go to (default menus):

- **Subscriber Management > Subscribers** (single vendor environment)
- **User Management > User Services > Multi Vendor Subscribers** (multi vendor environment)

The table describes columns in the Subscribers summary list:

Column Heading	Description
Role	Subscriber role, typically a self-service user role.
Sync Source	The source application of user data, for example: LOCAL indicates that the user has been manually created in VOSS Automate and has not been synced from LDAP or from Cisco Unified CM. CUCM indicates that the user exists on both VOSS Automate and Cisco Unified CM, and is not synced from LDAP. The user may have been created first on VOSS Automate (top-down) or created on Cisco Unified CM and synced into VOSS Automate (bottom-up). As for User ¹
User Type	“Admin”, “End User” or “End User + Admin” - associated with the user role
Auth Method	As for User ²
Entitlement Profile	The Entitlement Profile associated with the Subscriber.
Located At	Displays an abbreviated version of the hierarchy showing the lowest point in the hierarchy. The hierarchy type is shown in brackets. When you filter 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.
PrimaryLine	The subscriber’s primary extension number, as selected from the Pattern drop-down list when adding the subscriber. For Multi Vendor only, the line extension used as the primary line (a pre-allocated administrator line, and associated E164 number).
ExtMobility	If a Subscriber is associated with more than one extension mobility profile on the Unified CM, and you sync with VOSS Automate, only the first extension mobility profile is displayed in this list view.
Single Number Reach	The remote destination number configured for the subscriber. Only if supported.
Voice	Multi vendor subscribers only. The subscriber’s provisioned phones, listed by vendor.
Voicemail	The Voicemail number allocated to the subscriber. In a multi vendor environment, the subscriber’s provisioned voicemail services are listed by vendor.
Conferencing	Enabled or disabled. In a multi vendor environment, the subscriber’s conferencing services are listed by vendor, for example, Webex App, MS Teams, Pexip, Zoom.
Collaboration	Multi vendor subscribers only. The subscriber’s messaging services, listed by vendor, for example, WebEx, MS Teams, Zoom.

¹ **Sync Source:** see: [User Sync Source](#).

² **Auth Method:** see: [User Authentication Methods](#).

Column Heading	Description
Webex App	Defines whether a subscriber is enabled for Webex App.
Contact Center	Enabled or blank. Indicates the contact center agent's Team and extension if the subscriber is an agent.
Phone	The phone associated with the subscriber. When you filter on this column, the results include all phones at the hierarchy level and below, regardless of the Phone column in which they reside.
Phone 2	The second phone associated to the subscriber.
Phone n	The number of phone columns displayed in the list view will be the same as the maximum number of associated to a particular subscriber. For example, if a subscriber is associated to 10 phones, the list view will show 10 Phone columns.
Device	IP Address or Host Name.

Add a Subscriber

This procedure adds a subscriber in VOSS 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 in (default menus) **Dial Plan Management > Site > Class of Service** 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 VOSS Automate.³

To add a subscriber:

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 (default menus) **Subscriber Management > Subscribers**.
3. On the **Subscribers** page, click **Add**.
4. If you're logged in as Customer admin, choose the site where you want to add the subscriber.
5. Configure subscriber details on the tabs of the form:
 - User tab
 - Phones tab
 - Extension Mobility tab
 - Single Number Reach tab
 - Voicemail tab
 - Webex tab

³ This only applies to the VOSS Automate *Provider* deployment.

- Webex App tab
- Pexip Conference tab
- Contact Center tab

6. Click **Save**.

Repeat this procedure to add another subscriber.

User Tab

The **User** tab defines the user details of a VOSS Automate subscriber you're adding or updating.

Note the following:

- Only alphanumeric characters are allowed.
- For Cisco users, available entitlement profiles are imported from Unified CM.
- When choosing an existing device (phone) to associate with a user and then saving the form, the **Phones** tab is populated with the phone details.
- When adding a LDAP user as a subscriber, **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 subscriber self-provisioning is set up (allowing subscribers 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 subscribers add a company or personal phone via the Self-service interface.

To enable Extend and Connect in VOSS Automate:

1. On the **Users** tab, select the **Enable Mobility** checkbox.
 2. Add the following three groups of users:
 - a. Standard CCM End Users
 - b. Standard CTI Enabled
 - c. Standard CCM Admin User
- For subscribers entitled to Webex App, you can add a standalone Webex Apps user by completing the following minimum fields on the User tab, then go directly to the Webex App tab: **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 subscriber 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 subscriber. Your choice displays in the **Primary Line** column on the **Subscribers** list view.

- Subscriber Language and Role is set up in the Site Defaults of the subscriber's site hierarchy. If this is not specified, hierarchy defaults apply.

Phones Tab

On the **Phones** tab you can add or update a subscriber's phone.

To add a phone:

1. On the **Phones** tab, 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** tab.
- 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 subscriber 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.
- **Enduser** - identifies the user for Presence; you can add a new User ID

Note: VOSS 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 **Uri 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.

Note:

- The administrator password from the `AdminLoginDetails` in Unified CM is not stored in VOSS Automate. Data in VOSS-4UC is obtained from Unified CM.
 - VOSS Automate cannot disable the `Override Enterprise/Common Phone Profile Settings` setting once this check box has been enabled in the Unified CM GUI. This setting may be disabled on Unified CM (if required).
-

Related Topics

- [Site Defaults](#)
- Global Settings in the Core Feature Guide

Extension Mobility Tab

The **Extension Mobility** tab configures a subscriber's extension mobility settings.

Consider the following:

- Only one EM Profile can be added for extension mobility in VOSS Automate. If a subscriber is associated with more than one EM profile on the Unified CM, and you sync with VOSS Automate, both will be displayed:
 - on the subscriber's EM tab (this tab)
 - 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 tab, see the descriptions for the **Phones** tab. The exception is remote destination information, which is not relevant for extension mobility.

- 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** tab, 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 Unified CM. 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 subscriber.

Single Number Reach Tab

On the **Single Number Reach** tab, 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 VOSS Automate, first complete the following task:

1. Select the **Enable Extend and Connect** check box.
2. Select the CTI remote device that you created from the **CTI Remote Device Name** drop-down list.

Voicemail Tab

The **Voicemail** tab configures the subscriber'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 subscriber's default line.

- When adding Voicemail for a subscriber, all **Call Forward To Voicemail** check boxes, 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 CUCM Line Voicemail Profile" (**Site Management > Defaults > Line Defaults**).

WebEx Tab

The **WebEx** tab configures the subscriber's Webex details, if a valid server is available. The mandatory fields on this tab are populated with the values entered on the **User** tab.

Note: Any updates on the **User** tab do not update these values; values are populated only during the Add workflow.

Webex App Tab

The **Webex App** tab adds a Webex App User and enables a subscriber'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 [Create Webex App Service](#))
 - Webex App is enabled in the Entitlement Profile associated with the Subscriber.
- The following fields are read only and cannot be edited: **Login Enabled** and **Invite Pending**
- Once you have successfully added the subscriber as a Webex App user, the Webex App column displays status *Enabled* for this subscriber.
- The Subscriber e-mail address is required to enable Webex App for the Subscriber.

Pexip Conference Tab

The **Pexip Conference** tab adds and configures the subscriber's Pexip services.

Consider the following:

- The **Pexip Conference** tab is only available if a Pexip Conference service has been configured at the required hierarchy (via the Quick Add Subscriber Group).
- Conferencing must be enabled in the entitlement profile associated with the subscriber.
- Once a subscriber is successfully added as a conferencing user, you can view the service as an enabled service in the **Conferencing** column on the **Subscribers** list.

Contact Center Tab

On the **Contact Center** tab you can add, remove, or update CCX agent capabilities for a subscriber.

See also: [Contact Center](#)

The **Contact Center** tab displays 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 subscriber.

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 subscriber.

Update a Subscriber

This procedure modifies settings for one or more subscribers.

Perform these steps:

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. Open the Subscriber summary list page:
 - In a single vendor environment, go to (default menus) **Subscriber Management > Subscribers**.
 - In a multi vendor environment, go to (default menus), **User Management > User Services > Multi Vendor Subscribers**
4. Click on the relevant subscriber to open the Subscriber settings.
5. Make the changes you require. For details, see [Add a Subscriber](#).

Note:

- You can add one or more phones.
- If Extension Mobility is associated with more than one subscriber, it will not be removed when removing it from one subscriber.
- Phone line settings can be edited directly on the Subscriber 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 Subscriber 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.

Note: Filtering on the following columns on the Subscribers 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.

Deleting Subscribers

Overview

Subscribers are deleted via (default menus) **Subscriber Management > Subscribers**.

The system performs various actions when deleting a subscriber via Subscriber Management. These actions depend on the user type and the subscriber's device associations.

Subscriber types

User types	Description
Non-LDAP synced users	<ul style="list-style-type: none"> • Users created in VOSS Automate and pushed to CUCM • Users provisioned in CUCM and synced in to VOSS Automate
LDAP Integrated at VOSS Automate Users	<ul style="list-style-type: none"> • Users that are LDAP integrated at CUCM and synced in to VOSS Automate
LDAP synchronized users	<ul style="list-style-type: none"> • Users directly synced from an LDAP server to VOSS Automate.

Subscriber associations

Subscribers can have no device associations, or they can be associated with devices such as the following:

- Phones
- Extension mobility
- Single Number Reach (SNR)
- Voicemail
- WebEx

VOSS Automate actions when deleting a subscriber

The system performs these tasks when deleting a subscriber via **Subscriber Management > Subscribers**, depending on the user type and whether the subscriber has associated devices:

User Type	With Devices	Without Devices
Non-LDAP Synchronized Users LDAP Integrated at Cisco Unified CM Users	Deletes all devices: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 VOSS Automate to retain desk phones (hard phones, prefixed SEP or BAP) associated with a subscriber you're deleting, and to update these phones via a configuration template (CFT) once the subscriber is deleted. To do this, go to (default menus) **Customizations > Global Settings**, and on the **Phones** tab, set **Retain Desk Phones when Subscriber 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 CUCM subscribers will be retained (or removed) in the LDAP user sync that handles deleted CUCM subscribers. This is done via **Customizations > Global Settings > Webex App** tab or **Voicemail** tab, as applicable).

Related Topics

- Global Settings in the Core Feature Guide
- Subscriber, Phones tab in the Core Feature Guide

Delete a Subscriber

This procedure deletes and unprovisions a subscriber.

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 (default menus) **Subscriber Management > Subscribers**.
4. Select the checkbox for each subscriber you want to remove; then click **Delete**.
5. Click **Yes** to confirm.

The deleted subscriber is removed from the list. All elements associated with the subscriber are removed, except lines.

Note:

- If you have the global setting for phones configured to retain the subscriber'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 CUCM, users are deleted from the LDAP directory and not from the VOSS Automate system. Set up a data sync to synchronize the removal of the user.

22.1.2. Create Subscribers with New Users

New users do not yet exist in VOSS Automate and Cisco Unified Communications Manager.

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**.
2. Choose a user from the **Username** drop-down list.
3. In the **First Name** field, enter the user's first name.
The user's first name is optional but is required if you want to provision the user with a WebEx account.
4. In the **Last Name** field, enter the user's last name.
The user's last name is required.
5. Choose a group to assign to the user from the **Quick Add Group** drop-down list.
The default value in the Quick Add Group list is "default".
6. If required, provision the user with services using the **Voice, Extension Mobility, Voicemail, WebEx, Pexip, Single Number Reach, Webex App, Jabber / Dual-Mode Device, and Enable Self Provisioning** fields.
7. Click **Save**.

22.1.3. Create a Subscriber with Existing User

This procedure adds a subscriber based on an existing user.

Note: View existing users via **User Management > Users**.

-
1. Go to (default menus) **Subscriber Management > Quick Add Subscriber**.
 2. Choose the relevant site.
 3. On the **User Details** tab:
 - Choose the username from the **Username** drop-down.

- View the details that populate for the user.
- Update the user details, and choose services you wish to provision for this user.

Note: Devices and services associated with the user display on the **Existing Services** tab. The visibility of fields associated with existing services in QAS is enabled and disabled at the Customer level via the Global Settings. Disabling a service in the Global Settings hides the field associated with the service on the QAS form. If you wish to enable and display the service in QAS, you need to enable it in the Global Settings.

- At **Quick Add Group**, choose the Quick Add Group to assign to the user.

Note: The default value for Quick Add Group is "default".

4. Click **Save**.

Related Topics

- Global Settings in the Core Feature Guide.

22.1.4. Move Subscriber

Overview

A Customer administrator (or higher) can move a subscriber 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 CUCM cluster and CUCxn cluster.

When moving a subscriber:

- The subscriber, phones, device profiles, SNR, voicemail, and VOSS Automate data are processed in the move.
- The subscriber is updated with a new primary extension, where appropriate.
- The following existing services (associated with this subscriber) are moved along with this subscriber:
 - Phones (and associated lines)
 - Devices
 - Device profiles
 - Single number reach
 - Voicemail
 - Webex
 - Webex App

– Contact center

- When moving between sites on the same CUCM cluster, subscriber 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 CUCM clusters, the move data is re-provisioned on the new cluster and deleted on the original cluster, except for the CUCM subscriber. When the CUCM subscriber is local, the old subscriber is removed.

Important: When moving a subscriber across clusters, while the subscriber 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 VOSS Automate subscriber is purged.

The user is removed from the `device/cucm/User` model of the source CUCM in VOSS Automate.

The home cluster flag is maintained such that it is only set to True on the CUCM cluster hosting the subscriber, even if the subscriber exists on other CUCM 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 subscriber is created against a chosen subscriber template. This will not copy custom settings for the CUCxn subscriber 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.
- When moving cross cluster, the CUCM 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 CUCM cluster changes.

Move Subscriber Configuration

You can move subscribers via (default menus) **Subscriber Management > Move Subscriber**, then configure options on the following tabs:

- *Subscriber Configuration Tab*
- *Desk Phone Configuration Tab*
- *Jabber/Dual-Mode Device Configuration Tab*
- *Line Configuration Tab*
- *Existing Services Tab*

Subscriber Configuration Tab

On this tab you choose the subscriber you're moving and their target hierarchy.

The table describes configuration options on the Subscriber Configuration tab:

Field	Description
Subscriber	The subscriber you're moving.
Move from Hierarchy	Auto-populated, based on the subscriber you choose. The hierarchy the subscriber is moving from.
Move to Hierarchy	Mandatory. Choose a target hierarchy for the move.
New Role	Optional. Choose the subscriber's role at the target hierarchy.
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 subscriber to a new CUCM cluster.
New CUC User Template	Mandatory when moving a subscriber to a different CUCM cluster.
User Template	Optional template (MoveUpdateUserCustom_CFT) for custom subscriber updates on CUCM. You can clone and customize this template, if required. Available user templates are listed on the Configuration Templates page at (default menus) Customizations > Configuration Templates .

Desk Phone Configuration Tab

This tab configures the desk phones of the subscriber you're moving.

Note: By default, existing desk phones are moved with the subscriber. However, desk phones can either remain at the old site or move with the subscriber. Existing softphone devices, such as Jabber or Dual Mode devices, are always moved.

Home / Move Subscriber

Subscriber Configuration | **Desk Phone Configuration** | Jabber / Dual-Mode Device Configuration | Line Configuration | Existing Services

Move Desk Phones

Create New Phone

Use Existing Phone Configuration

Desk Phone Profile * Cisco 6901

Desk Phone Feature Template Default

Phone Name *

This field is required.

The table describes configuration options on the Desk Phone Configuration tab:

Field	Description
Move Desk Phones	<p>Enabled by default. Defines whether to move the subscriber's (SEP prefix) desk phones to the target hierarchy. Phones that aren't moved remain at the origin hierarchy.</p> <p>When unchecked (disabled), the moved subscriber is disassociated from their existing desk phones.</p> <p>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 <i>Jabber/Dual-Mode Device Configuration</i>.</p>
Create New Phone	<p>Choose this option to create new phones for the subscriber at the target hierarchy. When enabled, configure the following fields on this tab:</p> <ul style="list-style-type: none"> • Use existing phone configuration (yes/no) • Desk phone profile • Desk phone feature template • Phone name
Use Existing Phone Configuration	<p>Displays when Create New Phone is enabled.</p> <p>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:</p> <ul style="list-style-type: none"> • Phone configuration source • Desk phone profile • Phone name
Phone Configuration Source	<p>Displays only when Use Existing Phone Configuration is enabled.</p> <p>Choose from a list of the subscriber's existing phones to create the new phone using the configuration of the existing phone.</p>
Desk Phone Profile	<p>Displays when Create New Phone is enabled.</p> <p>Defines the phone type (and associated configuration).</p>
Desk Phone Feature Template	<p>Displays when Create New Phone is enabled and Use Existing Phone Configuration is disabled.</p> <p>Optional configuration template. Choose a template from the the first Phone Mapping Configuration found up the hierarchy tree.</p> <p>The Move Subscriber 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.</p>
Phone Name	<p>Displays when Create New Phone is enabled.</p> <p>Choose a phone name from the drop-down, which displays options from the Phone Configuration Mapping page (Customizations > Phone Configuration Mapping).</p> <p>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.</p>

Jabber/Dual-Mode Device Configuration Tab

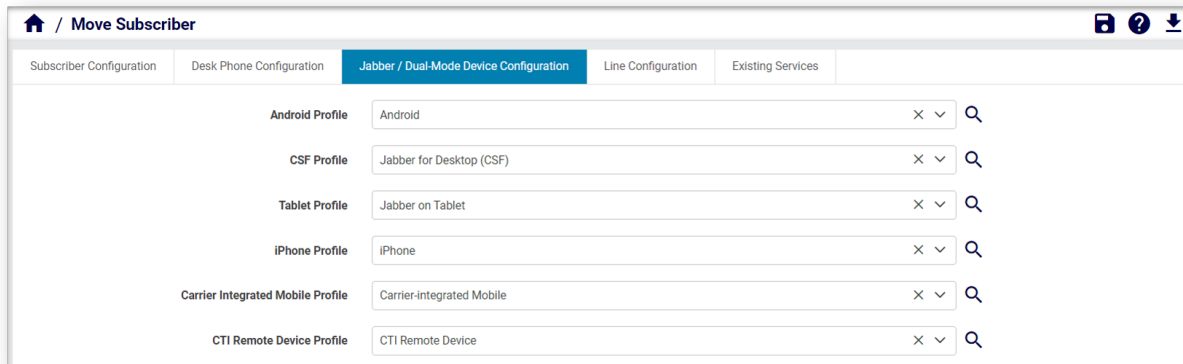
This tab configures Jabber and dual mode devices that are, by default, moved with the subscriber.

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 (default menus: **Customizations > Phone Configuration Mapping**).

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 subscriber.

When moving a subscriber, 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 subscriber 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.

The screenshot shows the 'Move Subscriber' interface with the 'Line Configuration' tab selected. On the left, there are checkboxes for 'Move Lines' (unchecked), 'Create New Line' (checked), and 'Use Default CSS' (checked). Below these is a 'New Lines' section with a '+', 'x', and '-' icon. A dropdown menu is open, showing 'No value set'. The main configuration area contains the following fields:

- Inventory Filter: Default
- Directory Number *: (empty)
- Label: 01_qas_10h23fn 01_qas_10h23ln x
- Display: 01_qas_10h23fn 01_qas_10h23ln
- Line Template: Default

Creating Lines

When moving a subscriber to another CUCM 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 VOSS Automate (if the required conditions already specified in this doc are met).

- Lines can only be moved if your system is using a type 4 dial plan, and only if the move is on the same cluster.
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 subscriber with their device profile and line:

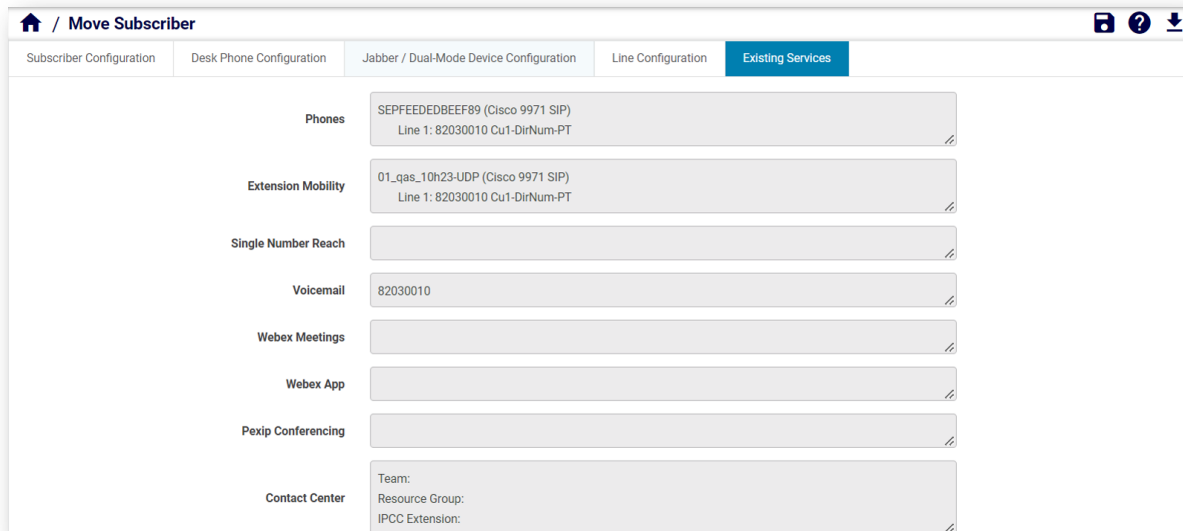
- The customer dial plan of the target site must not be SLC-based; that is, the following setting must be disabled in the target site's customer dial plan: *Site-Location Code (SLC) based dial plan*

You can view the customer dial plan configuration via (default menus) **Cisco Dial Plan Management > Customer > Dial Plan**.

Additionally, the global setting, *Enforce HCS Dialplan Rules*, must be disabled for the target site. You can view this setting via (default menus) **Customizations > Global Settings** and select the **Number Inventory** tab.

Existing Services Tab

This read-only tab displays the existing services of a subscriber you're moving.



22.1.5. Phones

Add a Phone (CUCM)

This procedure adds a phone.

Note: It is recommended that you use Smart Add phone to add standalone phones and use Quick Add Subscriber to add phones to subscribers. See [Smart Add Phone](#) and [Quick Add Subscriber for CUCM Users](#).

Before you start

Before adding phones in VOSS Automate, you will need to add and configure the following items on CUCM, and then import these items into VOSS Automate:

- Softkey templates (Softkey templates can be set up on CUCM or in VOSS Automate)
- Phone button templates
- Service parameters and enterprise parameters for subscriber services
- Custom SIP profiles

- Service profiles for Jabber
- Phone services

To add a phone (CUCM 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. Choose the hierarchy.
3. Go to (default menus) **Subscriber Management > Phones**.
4. On the **Phones** summary list view, view existing phones.

Note: An administrator with the required access profile can click **Fetch real-time phone status** on the toolbar to fetch the CUCM phone IP address and status *directly* from the CUCM. 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

Fetch data is not cached or stored in the database, and cannot 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.

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
```

5. Click **Add** to open the phone configuration screen, then fill out phone details on the following tabs:

Tab	Description
Phone	<p>At Device Name, fill out a device name, and add SEP before the mac address. For example, if the mac address is 00000000AB1, the device name must be SEP00000000AB1.</p> <p>Choose a product (for example, Cisco 7941), a device protocol (for example, SIP), and a device pool name (for example, RSMSimPhone_DP).</p> <p>If the Product type list doesn't contain the phone or endpoint you want, then, in CUCM, you'll need to install a COP file for the endpoint you want. Install the COP file only once for the CUCM instance where the endpoint is added. Then in VOSS Automate, import the phone button template from CUCM.</p> <hr/> <p>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 subscriber, or when adding a phone to an existing subscriber.</p> <hr/> <p>Default values are applied for some fields (such as Device Protocol, BAT Phone Template, and Device Security Profile), based on the selected product type. The Vendor Config settings are related to the selected phone type. Displayed fields are based on the selected Product (device type) and the Device Protocol (such as SIP or SCCP).</p> <p>The supported features available for each phone type are retrieved from the related CUCM.</p> <p>To override the default Phone Button Template, either choose another template, or enter a custom value. The new value is applied on the CUCM 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 CUCM, and then sync the template into VOSS Automate to have it appear in the drop-down.</p> <p>To enable Extend and Connect in VOSS Automate, perform these steps while creating a CTI Remote Device:</p> <ol style="list-style-type: none"> 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.
Lines	<p>This tab serves two purposes.</p> <ol style="list-style-type: none"> 1. To show all the lines that are associated with the device 2. To associate lines with the device. <p>The Lines sections reflect the Lines object in CUCM. You can add lines to this group and associate lines with the device. You can add custom lines by entering a line in the drop-down list. If Number Inventory is enabled, you can select a number from the list of available numbers.</p> <ul style="list-style-type: none"> • From the Pattern drop-down, choose a directory number. • At the Monitoring CSS Name drop-down, set the Monitoring Calling Search Space as the CSS that is configured in the Calling Search Space field in the Lines page.
	<ul style="list-style-type: none"> • At the Busy Trigger field, enter a busy trigger value, for example, 1. • At the Max Num Calls field, enter the maximum number of calls value, for example, 2.

Tab	Description
Dual Mode Settings	Only applies to a Dual Mode Phone, Spark Remote Device, or CTI Remote Device, and allows you to 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.
Certificate Authority Functions	Only applies to a Dual Mode Phone, Spark Remote Device, or CTI Remote Device, and allows you to 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](#).

6. Save your changes to add the phone.

Update a Phone

Note the following for updating a phone:

- The system checks that a line exists when you add it. If it doesn't exist, the line is added.
- The line edit form contains a hyperlink to the line settings that opens the Line relation details. Once you save your changes, the Phone page re-opens. Alternatively, you can use the browser Back button to return to the Phone editing page.
- If your menu layout has more than one entry for line management (`relation/LineRelation`) and associated Field Display Policy, then the form opened by the Link to Line hyperlink applies the first one (searching from top to bottom) found in the menu layout.
- The phone and User Remote Destination are updated.

Note: If the required CUCM setting “Customer Support upload URL” is configured at the Enterprise, Profile, or Device level, you can use **Action > Generate Prt Phone** to send a Problem Report Tool (PRT) file to the upload URL.

22.1.6. Delete Phones

This procedure deletes one or more phones, or phone settings.

When phones are deleted:

- The Remote Destination is removed first, so that the VOSS Automate cache remains in sync with the Cisco Unified Communications Manager (CUCM).
- The phone is deleted.

Note: Lines are not affected.

1. Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site, you can see all the fields described in this procedure. If you are logged on as the site administrator, you can see a subset of the fields that are available on the interface.
2. Choose a site from the hierarchy breadcrumb.
3. Choose **Subscriber Management > Phones**.
4. Choose one of the following methods to delete phones or phone settings:
 - Choose an individual phone to be deleted by selecting its check box in the far left column, then clicking **Delete**. From the popup window, click **Yes** to confirm the deleted phone.
 - Delete multiple phones at once by selecting the relevant check boxes, then clicking **Delete**. From the popup window, click **Yes** to confirm the deleted phones.
 - Remove phone settings as required by removing them from the relevant tab of a selected phone. Click **Save**.

When the delete action is complete, the phone disappears from the list.

Certificate Authority Functions

This 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 *	<p>From the drop-down list box, choose one of the following options:</p> <p>No Pending Operation: Displays when no certificate operation is occurring (default setting).</p> <p>Install/Upgrade: Installs a new or upgrades an existing locally significant certificate in the phone.</p> <p>Delete: Deletes the locally significant certificate that exists in the phone.</p> <p>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.</p> <p>Default: No Pending Operation</p>
Authentication Mode	<p>This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options:</p> <p>By Authentication String: Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone.</p> <p>By Null String: Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.</p> <p>By Existing Certificate (Precedence to LSC): Installs/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 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 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. 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.</p> <p>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 whether a LSC exists 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. 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.</p> <p>Default: By Null String</p>

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 Cisco Unified Communications 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

The **Vendor Config** settings will display if the Field Display Policy (FDP) allows it.

You can access the vendor configuration settings for a phone as follows:

1. In the Admin Portal, go to (default menus) **Subscriber Management > Phones**.
2. On the **Phones** list view, click on a phone to open its settings.
3. On the **Phones** tab, scroll down to the bottom of the page to locate the **Vendor Config** setting.
4. Click **Vendor Config** to open the configuration screen:

Settings can be enabled or disabled. 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 Unified CM, in some cases the value 0 is "Enabled" and in other cases 0 is "Disabled".
- It is recommended that settings on the Unified CM 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 Bulk Loaders, API, or custom Configuration Templates.
- 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 **Phones** list view (default menu **Subscriber Management > Phones**):
2. Click the **Generate PRT Phone** action to generate PRT log collection.

22.1.7. Phone Type Management

After you make changes to any phone model specific data in CUCM, 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 VOSS Automate, you need to do a sync of the CUCM.

Include the following models in the data sync - depending on what you changed:

- device/cucm/PhoneType - should always be included.

Note: This includes the expansion modules as well as the phone types.

- device/cucm/PhoneButtonTemplate - if button templates were changed
- device/cucm/PhoneSecurityProfile - if phone security profiles were modified

If you do a full sync or full import this will make the changes available in VOSS 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 allows you to run an ad-hoc sync with a very limited scope as needed - if changes are made in the CUCM 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

VOSS Automate supports the Cisco Unified CM (CUCM) capability for device onboarding using Activation Codes. This provides a simplified method to register a new phone in the system. This is supported from CUCM 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 has been activated and registered, the correct phone association takes place in VOSS 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 Subscriber/Phone Management capabilities:

- Phones
- Subscribers
- Quick Add Subscriber
- Smart Add Phone

Note: The selected phone type must also be included in the Subscriber's entitlement profile.

Setup and Onboarding Workflow

The high-level setup steps in VOSS Automate for phone onboarding with Cisco Activation Codes are as follows:

1. Initial setup - enabling Phone types for activation code.
2. Per Subscriber/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.

To 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 (default menus) **Apps Management > CUCM > 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** check box.
 - d. Click **Save**.

To complete the per Subscriber/Device setup to prepare the phone for onboarding:

1. Once enabled, you can add the phone, using any of the prescribed Subscriber Management methods (see above), making sure to select the **Use Activation Code Onboarding** check box. 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 **Phones** form (**Subscriber Management > Phones**).

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).

22.1.8. 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:
 - 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.

22.1.9. Replace Phone

Note: This software release currently only fully supports the replacement of an existing desk phone type with any other desk phone type.

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".
- 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 (default menus) **Customizations > Configuration Templates**. The new customized template is then available in the **Phone Button Template** drop-down of the Replace Phone feature.

See "Configuration Templates" for more details if required.

Replace a Phone

To replace a phone:

1. Log in as Site administrator or higher.
2. Go to (default menus) **Subscriber Management > 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).

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**.

Related Topics

- Global Settings in the Core Feature Guide.

22.1.10. 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](#)
 - [Create or Update a Schedule](#)
-

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.
-

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](#).

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	<p>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</p> <hr/> <p>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.</p> <hr/>
Model Specific Settings	
Models	E.g. 521, 522, 531, 532
Model Series	E.g 500
Model Firmware	<p>Select the required firmware version:</p> <ul style="list-style-type: none"> • 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	<p>Parameters as set on Unified CM:</p> <ul style="list-style-type: none"> • Name: e.g. SpeakerVolume • Value: integer, e.g. 5 • Access: e.g. User • Usage ID: e.g. 32 <p>One or more parameters can be set.</p>

See also "Headsets" in the Business Admin Portal

22.1.11. Phone Status Export

Overview

The Phone Status Export tool allows you to export the status of Unified CM 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.

Create and View a Phone Status Report

1. Browse to the required 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. From the **Phone Status Export** form (default menu **Subscriber Management > Status Export**):
 - a. Enter the **File name prefix**.
 - b. In the **Filters** section, define the required filters, namely the mandatory Status and Call Manager (Customer hierarchy only) fields as well as the optional **Device Name**, **Directory Number** and **IP Address** fields, noting the following:
 - Status of **None** = all phones that **do not** have a registration status on the API will appear in the phone status report.
 - Status of **Any** = all phones will appear in the phone status report regardless of the phone registration status.
 - **Device Name**, **Directory Number** and **IP Address** fields: only phones that match these filters are displayed in the phone status report. For example if you enter 'BAT' in the **Device Name** field, 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' in the filter will match 'BAT'.
3. Click **Save**. Once complete, the phone status report is saved under **File Management**.
4. Select the required phone status report (file-name-prefixXXXX.csv) from the **File Management** form (default menu **Administration Tools > File Management**) and click **Export** (JSON format).
5. From the resultant .zip file, open the .csv file in Microsoft Excel.

The first column on the report reflects the Phone hierarchy, and 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).

22.1.12. Smart Add Phone

Overview

The Smart Add Phone feature provides an easy way 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 the Smart Add Phone feature, the phone details that were added by the phone template can be seen and modified if needed by selecting the phone from **Subscriber Management > Phones**.

If you need a customized Phone Template, the default template can be cloned, renamed and modified from **Customizations > Configuration Templates**. This customization is then available in the **Phone Template** drop-down of the Smart Add Phone feature.

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 the Smart Add Phone feature. For details, refer to the topic on Custom Line Settings for Smart Add Phone Configuration Template in the Advanced Configuration Guide.

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 (default menus) **Subscriber Management > 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 Unified CM if the Unified CM 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 the **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 the **INI Enabled** field is **NO**, then the list of numbers are those Directory Numbers on Unified CM 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 (default menus) **Subscriber Management > Phones** to view and modify the phone that is added using the Smart Add Phone feature.

Added lines are shown on the **Lines** tab of the **Phones** page.

22.1.13. VOSS Phones

From the **Subscriber Management > VOSS Phones** menu item (default), phones are associated with the VOSS Phone Server (see: [VOSS Phone Server Overview](#) and [Managing VOSS Phone Servers](#))

- **Vendor:** all vendors configured in the library of phone types are offered. See also: [Adding Phone Types](#).
- **Model:** the phone model is selected. See also: [Adding Phone Types](#).
- **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.
- **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.

22.1.14. 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
- 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.

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.

22.1.15. Lines

Overview

The Lines menu allows you to add, modify, or delete individual lines and their associated line settings to or from the system.

Add Lines

This procedure adds and configures one or more lines (directory numbers) in VOSS Automate.

Note: If the Number Inventory feature is disabled by your administrator, you won't add lines; instead, you will select the relevant lines from a drop-down list of available numbers.

1. Go to (default menus) **Subscriber Management > Lines** to open the Lines view list.
2. Click **Add**.
3. Configure the line and its associated line settings in the tabbed windows on this page:

For details around filling out values for the line parameters, such as partitions and CSS, see the "Provider HCS Dial Plan Management Support Guide".

Note:

- If the **Enable CSS filtering** check box is selected at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the relevant site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.
- If the **Enable CSS filtering** check box is clear, then the list of available calling search spaces includes all CSSs that are configured on the Cisco Unified Communications Manager (Unified CM).

Tab	Description
Basic Information	Includes a directory number (mandatory), a route partition, calling search space, call pickup group (to which the line belongs), and other basic settings. 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	Includes various profiles, groups, and advanced settings for the line; for example, MOH Audio Source and voice mail profiles.
Shared Devices	Shows any phones, device profiles, or remote destination profiles that have been associated with the particular line.
Common Line Settings	Includes fields such as hold reversion ring duration, hold reversion notification interval, party entrance tone (chosen from a drop-down list).
AAR Settings	Automated alternate routing (AAR) handles the calls that are routed to the AAR Destination Mask or Voice Mail.
Park Monitoring	Includes text fields such as park monitoring forward no retrieve destination external or internal voice mail enabled check boxes, park monitoring forward no retrieve destination external, external calling search space, internal, internal calling search space, and park monitoring reversion timer text fields. Note: ¹ If the Enable CSS filtering check box is selected at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under Dial Plan Management > Site > Class of Service at the particular site. If the Enable CSS filtering check box is cleared, then the list of available calling search spaces includes all CSSs that are configured on the Unified CM.
Call Forwarding	Includes call forward all settings, call forward busy external and internal settings, call forward no answer external and internal settings, and so on.

4. Click **Save**.

All new and updated lines and their settings also reflect in Unified CM.

Once you've configured a line, you can verify the configuration via (default menus) **Administration Tools > Transaction**.

¹ This only applies to the VOSS Automate *Provider* deployment.

Edit Lines

To update an existing line and its settings:

1. Go to (default menus) **Subscriber Management > Lines** to open the Lines view list.
2. Click on a line to view its configuration settings in the tabs on this page.
3. Update the lines and its settings, as required.

For details around filling out values for the line 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 Unified CM before URIs will function.

Note that not all line settings are configured on the **Lines** form. Device specific settings such as caller ID display, line label, E.164 mask, and associated end user are configured via (default menus) **Subscriber Management > Phones**.

Delete Lines

This procedure deletes one or more lines, or line settings.

1. Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.
2. Choose a site.
3. Go to (default menus) **Subscriber Management > Lines**.
4. Choose one of the following methods to delete lines or line settings:
 - Choose an individual line to be deleted by clicking on its box in the leftmost column, then click **Delete**. From the popup window, click **Yes** to confirm the deleted line.
 - Delete multiple lines at once by checking the relevant check boxes, then clicking **Delete**. From the popup window click **Yes** to confirm the deleted lines.
 - Remove line settings from a line as required by removing them from the relevant tab of a selected line. Click **Save**.

Note: If lines are deleted while the numbers are in the Cooling or Reserved status, the numbers only become available once the release date has been reached.

When the delete action is complete, the line disappears from the list.

22.1.16. Intercom Lines

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 subscribers - they can then be set up and then associated to phones and subscriber 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 **Subscriber Management** menu for the site.

On the Intercom Lines page you can view a list of Intercom lines, and add, delete or modify Intercom lines.

Directory Number	Description	Alerting Name	Route Partition	Calling Search Space	Call Pk
8201140			A1_Intercom-PT	A1_Intercom-CSS	
8201141			A1_Intercom-PT	A1_Intercom-CSS	
8201142			A1_Intercom-PT	A1_Intercom-CSS	
8201143			A1_Intercom-PT	A1_Intercom-CSS	
8201144			A1_Intercom-PT	A1_Intercom-CSS	

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.

Intercom Lines [8201140]

Intercom Directory Number* 8201140

Route Partition A1_Intercom-PT

Description

Alerting Name

ASCII Alerting Name

Calling Search Space A1_Intercom-CSS

BLF Presence Group Standard Presence group

Default Activated Device

Auto Answer Auto Answer with Speakerphone

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 (default menus) **Subscriber Management > 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.

The screenshot shows the 'Phones' configuration page with the 'Lines' tab selected. A 'Line' configuration window is open, showing a 'Pattern*' dropdown menu with the value 'A1_Intercom-PT'. Below the dropdown, several fields are visible:

Route Partition Name	8201140 %494074371140 8201141 %494074371141 8201142 %494074371142 8201143 %494074371143 8201144 %494074371144
E164Mask	
Label	
Display	
Display Ascii	
Speed Dial	

- 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 Subscriber Management

1. Log in to the Admin Portal.
2. Choose the relevant site.
3. Go to (default menus) **Subscriber Management > Subscribers**.
4. When adding a phone to a subscriber, 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 Subscriber 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.

22.1.17. 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 (default menus) **Subscriber Management > Agent Lines**.
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.

22.1.18. Voicemail

Overview

VOSS Automate allows admin users to add, update, or delete Cisco Unity Connection (CUC) voicemail accounts (voicemail users), and their associated voicemail services, via (default menus) **Subscriber Management > Voicemail**.

Note: Optionally (depending on your deployment), VOSS Automate supports a Unity SIP integration feature that can be used in place of your existing voicemail service. See [Introduction to Unity SIP Integration](#)

The screenshot shows the VOSS Automate interface for configuring a CUC Account. The breadcrumb path is **Home / Voicemail / JohnD003**. The main form contains the following fields:

Field	Value
Voicemail Account Name *	JohnD003
First Name	John003
Last Name	Doe003
Email Address	johndoe003@aaaglobal.com
Voicemail Number *	82012003
Time Zone	(GMT+02:00) Africa/Johannesburg
Language	English(United States)
Language That Callers Hear	Inherit Language From Caller
Unified Messaging Account	+

Users and associated services added through VOSS Automate are also added to Cisco Unity Connection (CUC) voicemail system.

Related Topics

- Add, Update, or Delete a 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:

- VOSS Automate only supports either the Exchange or Office 365 Unified Messaging Service, Meeting-Place is **not** supported.

- Only **one** Unified Messaging Account (Single Inbox) per Subscriber can be added by VOSS Automate. However, if an existing Cisco Unity Connection subscriber is imported into VOSS Automate already has more than one account, then all associated services are imported, and will be available in VOSS Automate.
- Administrators must manually sync VOSS 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.
- VOSS Automate does not automatically integrate Cisco Unity Connection 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)

VOSS 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

Add, Edit, or Delete a Voicemail 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 VOSS Admin Portal, go to (default menus) **Subscriber Management > 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. On the **CUC Account** tab, configure CUC account details, such as voicemail account name (the subscriber), voicemail number, and the language the caller hears. For details, see [Unified Messaging Account](#)

Note:

- The **Voicemail Number** drop-down only shows numbers associated to the selected subscriber (chosen for voicemail account name).
- Email address is auto-populated when selecting an existing subscriber.
- 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 subscriber in VOSS Automate.

4. On the **Alternate Extensions** tab, 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 VOSS Automate.

5. From **Alternate Extension** choose the Partition from the drop-down and click **Save**.
6. On the **Message Actions** tab, 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. On the **Credentials** tab, 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 Subscriber Groups Default Model](#).

8. On the **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. On the **Caller Input** tab, 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](#).

Note:

- The **Caller Input** tab displays only once the CUC account (including voicemail account name) has been created and saved.
 - 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 subscriber, the lines used by any devices associated with the subscriber are updated to reflect the proper call forward and voicemail profile settings to enable the following buttons: **Call Forwarding to Voicemail** and **Voicemail**.

22.1.19. Extension Mobility

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.

VOSS Automate provides three ways to create, manage, and associate extension mobility profiles:

- Add an EM profile to a subscriber when adding a subscriber in a standard add process (see [Add a Subscriber](#))
- Add a subscriber using Quick Add Subscriber, 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 subscriber's extension mobility (EM) profile via **Subscriber Management > Subscribers**. From the list view, open a subscriber, and select the **Extension Mobility** tab. See [Add a Subscriber](#).
- Add or update a standalone EM profile via (default menus) **Subscriber Management > Extension Mobility**. 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:

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	<ul style="list-style-type: none"> • Extension mobility (EM) can be associated to multiple subscribers. If the Show Numbers belonging to this Subscriber option is chosen as the Inventory Filter, only the directory numbers associated to the first subscriber on the Subscribers tab are displayed. • 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.
Subscribers tab	Allows you to associate the EM profile to one or more subscribers. You can also disassociate an EM profile from a subscriber by clearing the name from the Username drop-down, and saving the change. The Subscriber link on an existing EM profile links to the associated subscriber's Extension Mobility form (default menu Subscriber Management > Subscribers).

Delete an Extension Mobility Profile

You can delete a standalone extension mobility (EM) profile via the list view (default menus, **Subscriber Management > Extension Mobility**).

When deleting an EM profile, the following elements are automatically removed/cleared:

- Speed dials
- Busy lamp fields
- Service URL's
- IP phone service subscriptions

22.1.20. Add Device to User

This procedure associates an existing phone or device profile to an existing user.

1. Log in to the Admin Portal, then go to (default menus) **Subscriber Management > Add Device to 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.

22.1.21. 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.
- 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**.

22.1.22. Quick Add Subscriber Groups

Overview

A Quick Add Group (QAG) is a collection of templates that configure the subscriber features.

Note: A Quick Add Group is mandatory when adding a subscriber using Quick Add Subscriber.

Quick Add Subscriber Groups allow administrators to group feature and configuration templates for use with Quick Add Subscriber and Add Subscriber. This grouping helps to quickly and easily configure subscribers.

For example, to add 100 back-office users and 50 sales users:

- Back-office users all use the 7965 phone with SCCP protocol and no services.
- Sales users all use the 8865 phone with SCCP protocol and Single Number Reach service.

To quickly configure these two groups, create two Configuration Templates:

- One for the 7965 phone with no services for the back-office users.

- One for the 8865 phone with the Single Number Reach service for the sales users.

You also create two Quick Add Groups:

- One for the back-office users which reference the back-office user Configuration Template.
- One for the sales users which reference the sales users Configuration Template.

You can manage Quick Add Group templates from the **QAG Settings** menu. To easily identify a Quick Add Group from the drop-down when managing Quick Add Subscriber Groups, a best practice naming convention here could include a pattern:

<friendly hierarchy name>-QAG-<user type>-<phone-template-name>-[description]

For example, GeoLogic-QAG_BasicUser - 69XX SIP - CallWaiting

When adding subscribers (with Quick Add Subscriber or Add Subscriber), choose the appropriate Quick Add Group for the user you're provisioning.

All subscriber services use configuration templates that belong to a Quick Add Group.

Add a Quick Add Subscriber Group

This procedure adds a Quick Add Subscriber Group (QAG).

1. Log in as Provider, Reseller, Customer, or Site administrator.
2. Go to (default menus) **Subscriber Management > Quick Add Subscriber Groups**.
3. Click **Add**.
4. In the **Group Name** field, enter a group name. This is a required field.
5. From the **Template** drop-downs, choose the required templates.

For example, perform these steps to create back-office QAS users with phone type 6911 using SCCP protocol (voice account):

- a. From the Default CUCM **Phone Template** drop-down, choose **Backoffice Phone 6911 SCCP**.
- b. From the Default CUCM **Line Template** drop-down, choose **Default CUCM Line Template**. This associates a line with the phone.
- c. You can also use custom configuration templates to assign to a Quick Add Subscriber Group.

Note: The custom configuration template can be at the same level in the hierarchy as the group, or higher.

6. Click **Save**.

Delete a Quick Add Subscriber Group

The default Quick Add Subscriber (QAS) Group resides at the sys hierarchy node.

Note: A QAS Group is required for the QAS function to work.

1. Go to (default menus) **Subscriber Management > Quick Add Subscriber Groups**.
2. Select the checkbox at the Quick Add Subscriber Group you want to delete.

- Click **Delete**, then click **Yes** to confirm.

Quick Add Subscriber Groups Default Model

Default Group Model for Quick Add Subscriber and Add Subscriber Wizard Functions

Title	Field Name	Configuration Template Name
Group		
Group Name*	group_name	N/A
CUCM and WebEx		
CUCM User Template*	default_cucm_user_template	Default CUCM User Template
Phone Template	default_cucm_phone_template	Default CUCM Phone Template
Extension Mobility Template	default_cucm_device_profile_template	Default CUCM Extension Mobility Template
Line Template	default_cucm_line_template	Default CUCM Line Template
Remote Destination Template	default_cucm_rd_template	Default CUCM Remote Destination Template
Remote Destination Profile Template	default_cucm_rdp_template	Default CUCM 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 CUCM Jabber Android Template
Jabber CSF Template	default_cucm_jabber_csf_template	Default CUCM Jabber CS Template
Jabber iPad Template	default_cucm_jabber_ipad_template	Default CUCM Jabber iPad Template
Jabber iPhone Template	default_cucm_jabber_iphone_template	Default CUCM 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)		
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 Add Subscriber 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 Add Subscriber applies this template and overrides CUC user template settings on CUC.

continues on next page

Table 1 – continued from previous page

Title	Field Name	Configuration Template Name
WebEx App		
Default Webex App User Template	default_spark_user_template	Default Webex App User Template
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_template	Default Webex App User iPhone Template
Default Webex App User Android Device Template	default_spark_user_android_device_template	Default Webex App User Android Template
Default Webex App User Tablet Device Template	default_spark_user_tablet_device_template	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
Pexip Conference		
Pexip Conference Template	default_pexip_conference_template	Reference Pexip Conference Template
Microsoft		
MS 0365 User Template		
MS Teams User Template		
Additional Services		
VOSS Phone User Template		

Fields marked with * are mandatory.

22.1.23. Class of Service

Customer administrators and higher level administrators can create and maintain a Class of Service (CoS) that apply to subscribers. A CoS specifies the Unified CM and Calling Search Spaces (CSS) for a subscriber'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 Unified CM 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 Unified CM, or else added. Macros can also be used when adding new CSSs, for example: CSS-Go1d-{{macro.SITENAME}}.

When a CoS is modified, the Unified CM cannot be modified. In order to refer to another Unified CM, either clone an existing CoS or else delete it and re-add it.

Add a Class of Service

1. Log in as a Customer administrator or higher.
2. Go to (default menus) **Subscriber Management > Class of Service**.
3. To add new CoS instance, click **Add**. If necessary, this will automatically direct the user to select a customer-hierarchy-level, if not already on it.
4. From the **CUCM** drop-down, choose the relevant CUCM.
5. Enter the Class of Service name in the **CoS Name** field.
6. From the **Device CSS** and **Line CSS** drop-downs, choose the relevant CSS types to be associated to this CoS item.

The value can also be a macro that evaluates to a valid CSS type which already exists on the selected CUCM. Blank values are also allowed.

22.1.24. 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.

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 a File](#).

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.
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 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**.

22.1.25. 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:

- *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*
 - 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 Subscriber](#)
- [Quick Add Subscriber for CUCM Users](#)
- [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
 - 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.

22.1.26. 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.
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.

22.1.27. Hunt Groups

Overview

A hunt group is a combination of the following elements:

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.

The site defaults auto-populates some values for hunt groups. To view or update the defaults, go to (default menus) **Site Management > Defaults**, 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 VOSS Automate and Cisco Unified Call Manager (CUCM).

Note: When adding a hunt group, you will 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 will 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 (default menus) **Subscriber Management > Hunt Groups**.
4. On the **Hunt Groups** list view, click **Add**.
5. Choose a network device list (NDL).

Note: For hunt groups configured at the customer level:

- 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.
7. Click **Save**.

A workflow is triggered to add the new hunt group:

- A hunt list is added with the details you configured.
- A hunt pilot is added with the details you configured.
- One or more line groups are created with the specified directory numbers as members.

Configure a New Hunt Group

This section describes the configuration options when adding a hunt group. You will need to configure the following sections of the **Hunt Groups/New Record** page:

- Pattern Definition
- Forward Hunt No Answer
- Forward Hunt Busy
- Queueing
- Park Monitoring
- Calling Party Transformations
- Connected Party Transformations
- Called Party Transformations
- AAR Group Settings
- Hunt List
- Line Groups and Line Group Members

Configure Pattern Definition

For hunt groups configured at the customer level, define 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.

Field	Description
<p>Hunt Pilot Pattern</p>	<p>Specify a hunt pilot pattern, or choose one from the the drop-down.</p> <p>A hunt pilot pattern can include numbers and wildcards (no spaces). 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.</p>
<p>Route Partition</p>	<p>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.</p>
<p>Route Filter</p>	<p>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.</p>
<p>Hunt List</p>	<p>Add the hunt list name to the Name field in the Hunt List section to auto-populate this field.</p>
<p>Call Pickup Group</p>	<p>Choose a call pickup group to associate with this hunt group.</p> <p>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.</p> <p>Call pickup group is the number that can be dialed to answer calls to this directory number (in the partition)</p>
<p>Alerting Name</p>	<p>Specify an alerting name for the hunt pilot in UNICODE format.</p> <p>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.</p> <p>If you don't enter a name, the hunt pilot DN displays on the phones.</p>
<p>Provide Outside Dial Tone</p>	<p>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.</p>

Configure Forward Hunt No Answer

1. At **Forward Hunt No Answer Action**, choose the hunt call treatment action setting.

- Choosing **Forward Unanswered Calls to Destination** enables these fields:

CFNA Destination	Defines the directory number where calls are to be forwarded.
CSS CFNA	Applies to all devices using this directory number. The drop-down displays all CSSs in the system. The default is the default line CSS of the site.

- Choose **Use Forward Settings of Device that Forwarded to Hunt Pilot** to use the call forwarding settings of the line group member.

2. At **Maximum Hunt Timer**, specify the maximum time for hunting without queuing.

Note: Do not use the same value for this field and for the **RNA Reversion Timeout** field in the associated line group.

Configure Forward Hunt Busy

At **Forward Hunt Busy Action**, choose the hunt call treatment action setting.

- Choosing **Forward Busy Calls to Destination** enables these fields:

CFB Destination	Defines the directory number where calls are to be forwarded.
CSS CFB	Applies to all devices using this directory number. The drop-down displays all CSSs in the system. The default is the default line CSS of the site.

- Choose **Use Forward Settings of Device that Forwarded to Hunt Pilot** to use the call forwarding settings of the line group member.

Configure Queueing

At **Queueing**, define whether to queue calls. Selecting this checkbox disables Forward Hunt Groups, and displays additional configuration options.

Note: These mandatory fields are auto-populated with default values:

- Maximum Number of Callers Allowed in Queue: 32
 - Maximum Wait Time in Queue: 900
-

Configure 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.

Configure Line Groups

Although you can configure an empty line group with no members (directory numbers), CUCM does not support this configuration for routing calls. If the line group contains no members, the hunt list stops hunting when the call gets routed to the empty line group. To avoid this scenario, ensure you configure at least one member in the line group.

You must define one or more directory numbers before configuring a line group. You can remove members from the line group after you configure or update the 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.

Field	Description
Line Group Name	<p>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.</p> <p>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.</p> <p>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.</p>
RNA Reversion Timeout	<p>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: <i>Try next number; then try next group in Hunt List</i></p> <p>The RNA Reversion Timeout applies at the line-group level to all members.</p>
Hunt Options No Answer	<p>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.</p>
Automatically Logout Hunt Member on No Answer	<p>Defines whether line members are automatically logged off the hunt list. Line members can log back in using the "HLOG" softkey or PLK.</p>
Hunt Options Busy	<p>Choose a hunt option for CUCM to use if a call is distributed to a member of a line group that is busy.</p>
Hunt Options Not Available	<p>Choose a hunt option for CUCM to use if a call is distributed to an unavailable line group member. The <i>Not Available</i> 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.</p>

Configure Line Group Members

To configure line group members:

- Choose a directory number.
- Choose a partition.
- Specify a position.

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.

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

22.1.28. Call Pickup Groups

Overview

Certain default values for call pickup groups are populated by the site defaults menu item, which can be viewed and edited (depending on your log in level). Choose **Dialplan Management > Site Defaults** and click on the required site name in the list view.

The Call Pickup Groups feature provides an administrator with the following:

- A single interface on which to create call pickup groups, and to select one or more lines as members of a pickup group.
- The ability to add Unified CM call pickup groups and to modify the call forward and call pickup settings of each Unified CM 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 feature, 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.
- The ability to 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 feature, 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. The **Route Partition Name** field is populated automatically based on the selected Pattern.

- The ability to delete a pre-existing call pickup group, and to 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.

Add a Call Pickup Group

This procedure adds a call pickup group in VOSS 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 **Subscriber Management > Call Pickup Groups**.
5. Click the **Add** button to open the **Call Pickup Groups** page.
6. Configure options on the **Call Pickup Group** tab:
 - Enter a name and a description.
 - 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**, or **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. Configure options on the **Member Lines** tab:
 - Click the Plus icon (+) to add an entry.
 - At **Directory Number**, choose a directory number, which auto-populates the **Route Partition** field.

Note: You can choose a different route partition, if required.

Call pickup group members will only be successfully added if their directory number exists in a valid route partition. Directory numbers in a 'null' route partition appear as selectable members, but saving them results in an error.

- Repeat this step to add more member lines to the call pickup group.

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 **Subscriber Management > Lines**. The call pickup group under **Lines** displays the associated call pickup group

Delete a Call Pickup Group

This procedure deletes a call pickup group in VOSS Automate.

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy to the Customer or Site level.
3. Choose **Subscriber Management > Call Pickup Groups**.
4. Choose the call pickup group, and then click **Delete**.

22.1.29. Contact Center

Overview

VOSS 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 VOSS Automate allows Contact Center device models in VOSS Automate to sync to the UCCX server:

UCCX server management	<ul style="list-style-type: none"> • Configure Contact Center Express (UCCX) Server
Day 2 integration	<ul style="list-style-type: none"> • Add a UCCX device to a hierarchy, add entitlement profiles, then configure subscribers as Contact Center agents. Additional management can be performed in VOSS Automate, including overbuild. See Objects Moved During the Overbuild • Contact Center Agent Quick Add • Add a Subscriber (Contact Center)
Direct management	<ul style="list-style-type: none"> • Agents (device/uccx/Agent), see Agents • Skills (associated with competency levels), see Skills • Teams (device/uccx/Team), see Teams • Resource Group (device/uccx/ResourceGroup), see Resource Groups • Contact Service Queues (device/uccx/ContactServiceQueue), see Contact Service Queues.
Associate agent devices association with CUCM users	<p>Admins can specify the agent's controlled device via:</p> <ul style="list-style-type: none"> • Quick Add Subscriber • Subscriber • Direct Agent management <p>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.</p>
VOSS Automate management interfaces for UCCX	<ul style="list-style-type: none"> • Manage agent profiles (see Agent Profiles) • Re-skilling Bulk manage (add, remove) agent skills and competencies via side-by-side transfer boxes for the following: <ul style="list-style-type: none"> – Agents – Teams – Resource groups See: Re-skill Agents

Agents

You can view a list of Contact Center agents that have been synced in, or agents added when adding subscribers at a customer or site, via (default menus) **Subscriber Management > Contact Center > Agents**.

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.

Teams

On the **Teams** page (default menus, **Subscriber Management > Contact Center > Agents**) 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 CUCX, via (default menus) **Customer Management > Network Device Lists**.

Resource Groups

Contact Center resource groups comprise one or more agent profiles. If you're creating resource groups directly in VOSS 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 (default menus) **Subscriber Management > Contact Center > Resource Groups**.

Skills

VOSS 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 (default menus) **Subscriber Management > Contact Center > Skills**.

Contact 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 (default menus) **Subscriber Management > Contact Center > Contact Service Queues**.

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.

VOSS 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 VOSS Automate, and you can manage the queues in VOSS Automate.

Note: When choosing queue type `EMAIL`, you will need to fill out details for the following mandatory fields:

- Email Username (`accountUserId`)
 - 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 Subscriber, you must first create the agent profile.

To view and manage agent profiles, go to (default menus) **Subscriber Management > Contact Center > 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 (default menus) **Subscriber Management > Contact Center**.

To re-skill agents:

1. In the Admin Portal, select the relevant customer from the organization picker.
2. Go to (default menus) **Subscriber Management > Contact Center > Re-skill Agents** to open 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.

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 (default menus) **Subscriber Management > Contact Center > Agent Profiles**.
6. Create a new agent. There are three options:
 - Using Quick Add Subscriber, via (default menus) **Cisco Subscriber Management > Quick Add Subscriber**.
 - Using Subscriber management functionality, via (default menus) **Cisco Subscriber Management > Subscribers**.
 - Or add the agent directly, via (default menus) **Cisco Subscriber Management > Contact Center > Agents**.

22.1.30. Provision the Extension Mobility Service

Overview

In VOSS 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'.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Device Profile Configuration

Save Delete Copy Add New

Status
Status: Ready

Association

Modify Button Items

- 1 [Line \[1\] - 82012000 in Cu1-DirNum-PT](#)
- 2 [Line \[2\] - Add a new DN](#)
- 3 [Add a new SD](#)
- 4 [Add a new SD](#)
- 5 [Add a new SD](#)
- 6 [Add a new SD](#)
- Unassigned Associated Items
- 7 [Add a new SD](#)
- 8 All Calls
- 9 [Add a new BLF Directed Call Park](#)
- 10 Call Park
- 11 Call Pickup
- 12 CallBack
- 13 Group Call Pickup
- 14 Hunt Group Logout
- 15 [Intercom \[1\] - Add a new Intercom](#)
- 16 Malicious Call Identification
- 17 Meet Me Conference
- 18 Mobility
- 19 Other Pickup
- 20 Quality Reporting Tool

User Device Profile Information

Product Type: Cisco 9971
Device Protocol: SIP
Device Profile Name*: JohnD000-UDP
Description: Created by default template
User Hold MOH Audio Source: < None >
User Locale: < None >
Phone Button Template*: Standard 9971 SIP
Softkey Template: < None >
Privacy*: Default
Always Use Prime Line*: Default
Always Use Prime Line for Voice Message*: Default
Feature Control Policy: < None >
 Ignore Presentation Indicators (internal calls only)
 Do Not Disturb
DND Option*: Ringer Off
DND Incoming Call Alert: < None >
Extension Mobility Cross Cluster CSS: < None >

MLPP and Confidential Access Level Information

MLPP Domain: < None >
MLPP Indication*: Off
MLPP Preemption*: Default

Logged Out (Default) Profile Information

Login User Id: < None >

Related Topics

- Introduction to EMCC in the Core Feature Guide
- Configuration Templates in the Core Feature Guide
- Extension Mobility Profiles in the Core Feature Guide

EMCC and Multi-Cluster CallManager

A large organization (set up at the VOSS 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).

The screenshot shows the VOSS Automate web interface. On the left is a navigation menu with options: Hierarchy Management, Reseller Management, Customer Management, Site Management, Apps Management (highlighted), VOSS Assurance, CUCM, and Servers. The main content area displays a table of servers under the heading 'Servers'. The table has columns for Cluster Name, CUCM Server Name, id, Located At, and Device. Two server entries are visible:

Cluster Name	CUCM Server Name	id	Located At	Device
AAAGlobal-CL1	192.168.100.15	4	AAAGlobal (Customer)	192.168.100.11, 8443, hcs
AAAGlobal-CL2	192.168.100.16	6	AAAGlobal (Customer)	192.168.100.11, 8443, hcs

A CUCM administrator configures cross-cluster via the CUCM Extension Mobility Cross Cluster (EMCC) feature settings on CUCM, and in VOSS Automate (via **Customer Management > EMCC**).

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.

The screenshot shows the 'User Device Profile Information' form. The 'Product Type' is Cisco 8865 and the 'Device Protocol' is SIP. The 'Device Profile Name' is user0011005-UDP. The 'Extension Mobility Cross Cluster CSS' field is highlighted in blue and set to EMCC-CSS-USA. Other fields include User Hold MOH Audio Source, User Locale, Phone Button Template, Softkey Template, Privacy, Always Use Prime Line, Always Use Prime Line for Voice Message, Ignore Presentation Indicators, Do Not Disturb, DND Option, and DND Incoming Call Alert.

Note: In VOSS Automate, EMCC groups define the clusters and countries to be used together for extension mobility. When saving an EMCC group, VOSS 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.

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.

The screenshot shows the VOSS Automate interface for configuring templates. The left sidebar lists various management categories, with 'Customizations' selected. The main content area is titled 'Configuration Templates [Reference CUCM User Template]'. Under the 'Pin Credentials' section, several fields are visible, including 'Pin Reset Hack Count', 'Pin Cred Locked By Administrator', 'Pin Cred Time Admin Lockout', 'Pin Cred Does Not Expire', 'Pin Cred Policy Name', 'Pin Cred User Cant Change', 'Pin Cred Time Changed', and 'Pin Cred User Must Change'. Below this, the 'Enable Extension Mobility Cross Cluster' field is set to 'True'. Other fields include 'Department', 'Confirm Digest Credentials', 'Repeat Confirm Digest Credentials', 'Primary Device', and 'User Group'.

Device Profiles and Extension Mobility Profiles

A CallManager device profile is called an extension mobility profile in VOSS Automate. Device profiles are configured in VOSS 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 **Subscriber Management > Quick Add Subscriber**, and choose a user from the **Username** drop-down list.
2. Select **Extension Mobility**.

The screenshot displays the configuration interface for adding a new CUCM user. The left-hand navigation pane is expanded to 'Cisco Subscriber Management', with 'Quick Add Subscriber' selected. The main configuration area contains the following fields and options:

- PIN:** A text field containing masked characters (*****).
- Repeat PIN:** A text field containing masked characters (*****).
- Entitlement Profile:** A dropdown menu showing the selected profile: ["RST Entitlement Profile", "hcs.CS-P"].
- Quick Add Group*:** A dropdown menu showing the selected group: Cisco 3905 Phone Type.
- Device Pools:** A dropdown menu.
- User status:** A text field containing the message: "Adding services to NEW CUCM user."
- Lines:** A section with a plus icon in a dark blue bar.
- Voice:** An unchecked checkbox.
- Extension Mobility:** A checked checkbox.
- EMCC:** A checked checkbox.
- Voicemail:** An unchecked checkbox.
- Webex Meetings:** An unchecked checkbox.

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). VOSS 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**).

22.1.31. 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.
-

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](#)

22.1.32. Provision the Voicemail Service

1. Choose **Subscriber Management > Subscribers**. From the **Subscribers** list, click on the name of the subscriber to be provisioned with voicemail.
2. Choose the **Voicemail** tab.
3. In the **Voicemail Account** field, click +. The **Voicemail Line** drop-down appears.
4. Choose a line from the **Voicemail Line** drop-down and click **OK**.

For details on the workflow, see [Voicemail](#).

5. Choose **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down list.
6. Choose the **Existing Services** tab.
7. Make sure that the voicemail line appears in the **Voicemail Extension** field.

22.1.33. Provision Webex Service

This procedure enables a subscriber for the Webex service.

1. In the Admin Portal, go to (default menus) **Subscriber Management > Subscribers**.
2. From the **Subscribers** list, click the name of the subscriber to be provisioned with WebEx service.
3. Select the **WebEx** tab.
4. In the **WebEx User** field, click the Plus icon (+) to display the Webex configuration fields.
5. Fill out the following details: First Name, Last Name, Email, Password
6. In the **Privilege** section, select relevant Webex privileges.
7. Click **OK**.
8. Go to (default menus) **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down.
9. Select the **Existing Services** tab, and ensure that "ACTIVATED" appears in the **WebEx** field.

Related Topics

- [Provisioning Subscribers with Webex App](#)

22.1.34. Provision the Pexip Conference Service

The **Pexip Conference** tab is only available if:

- Pexip Conference service has been configured and is available to the hierarchy (via the Quick Add Subscriber Group).
 - Entitlement Profile: the **Conferencing** check box has been selected and associated to the Subscriber.
1. Choose **Subscriber Management > Subscribers**. From the **Subscribers** list, click the name of the subscriber to be provisioned with Pexip Conference service.
 2. Choose the **Pexip Conference** tab.
 3. In the **Pexip Conference** field, click +. The Pexip Conference configuration fields appear.
 4. Enter information 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: choose **Subscriber Management > Quick Add Subscriber**, and choose 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 \(VMR\)](#)

22.1.35. Provision the Single Number Reach Service

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**, and choose the user for whom you want to provision Single Number Reach from the **Username** drop-down list.
2. Choose the **Single Number Reach** tab. The SNR Mobile Number field appears.
3. In the SNR Mobile Number field, optionally enter the mobile number. Do not add any spaces or special characters to the number.

The SNR Mobile Number can be the same as the user's Mobile Number shown in **User Management > Users**.

4. Click **Save**.
5. Choose **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down list.
6. Choose the **Existing Services** tab.
7. Make sure that the Single Number Reach displays the **Single Number Reach** profile name.

The Single Number Reach profile name is the user name followed by "-RDP". For example: jsmith-RDP.

22.1.36. Provision the Contact Center Agent

This procedure provisions a subscriber as a Contact Center agent.

Pre-requisites:

- The subscriber 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 (default menus) **Subscriber Management > Subscribers**.
2. From the **Subscribers** list, click on the subscriber to be provisioned as a Contact Center agent.
3. On the subscriber management page for the relevant subscriber, select the **Contact Center** tab.

Note: This tab is visible only if the subscriber is assigned an entitlement profile with Contact Center service enabled.

4. Provision the subscriber as a Contact Center agent.

22.1.37. Provision the Jabber or Dual Mode Device Service

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**. From the **Username** drop-down, select a user.
2. Select the **Jabber/Dual-Mode Device** check box. The **Jabber and Dual-Mode Devices** field appears.
3. Click + next to **Jabber and Dual-Mode Devices** to expose the **Jabber/Dual Mode Agent** drop-down and **Device Name** field.
4. Choose a device type from the **Jabber/Dual Mode Agent** drop-down. 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** check box to enable Mobile Identity if required:

- Android
- iPhone
- Carrier Integrated Mobile

5. Click **Save**.
6. Choose **Subscriber Management > Quick Add Subscriber**. From the **Username** list, choose the same user.
7. Choose the **Existing Services** tab.
8. Make sure that the **Phones** field displays the Jabber device.

For each device type, a Configuration Template that is associated with the Subscriber's Quick Add Group is used to provision the device. For defaults, see: [Quick Add Subscriber Groups Default Model](#).

Note: If a CSF Jabber device type is selected, all lines are associated to the CSF Jabber device by default.

22.1.38. Enable Self Provisioning

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**. From the **Username** drop-down list, select a user.
2. Select the **Enable Self Provisioning** check box. 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 Management > Self Provisioning > User Profile**.
4. In the **Lines** field, click +. The **Directory Number** drop-down appears.
5. Choose a line from the **Directory Number** drop-down.
6. Click **Save**.
7. Choose **Subscriber Management > Subscribers** and choose the same user from the Subscribers list view.
8. Make sure that the **Self Service** and **User Profile** fields display the same settings as those set in Quick Add Subscriber.

22.2. Microsoft Subscriber Management

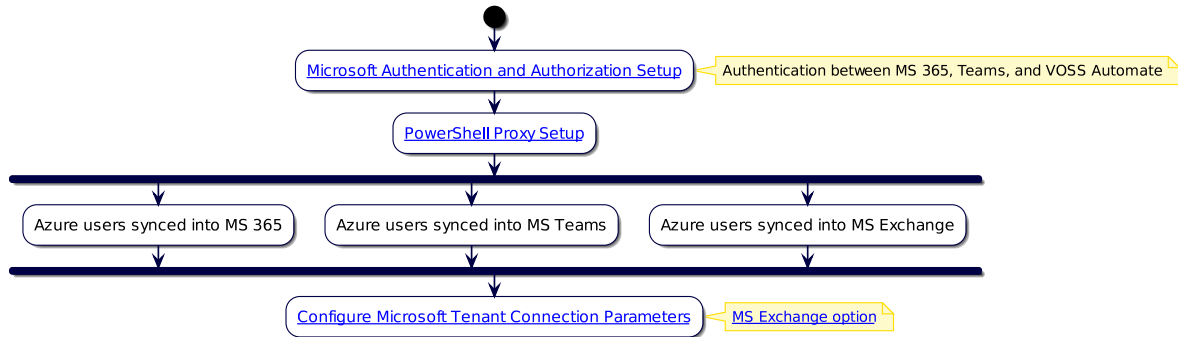
22.2.1. Microsoft Configuration

An organization using Microsoft to manage UC provisioning requires a number of different portals in a tenant: Azure, Microsoft 365 Admin Center, and (once users are licensed through Microsoft Office 365), a portal on the Microsoft Teams side for telephony. MS Exchange can also be added to the tenant.

VOSS 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 will need to install and configure a Microsoft Windows PowerShell Proxy server (one or more). This is to allow VOSS Automate to access Azure via the PowerShell. For details, see [PowerShell Proxy Setup](#)
- Once the Microsoft Windows PowerShell service is installed, you will use the IP address and credentials of the proxy server to configure the Microsoft tenant.



Next Steps

VOSS Automate Configuration and Sync in the Core Feature Guide

Related Topics

Microsoft Overview in the Core Feature Guide

22.2.2. Microsoft Subscribers

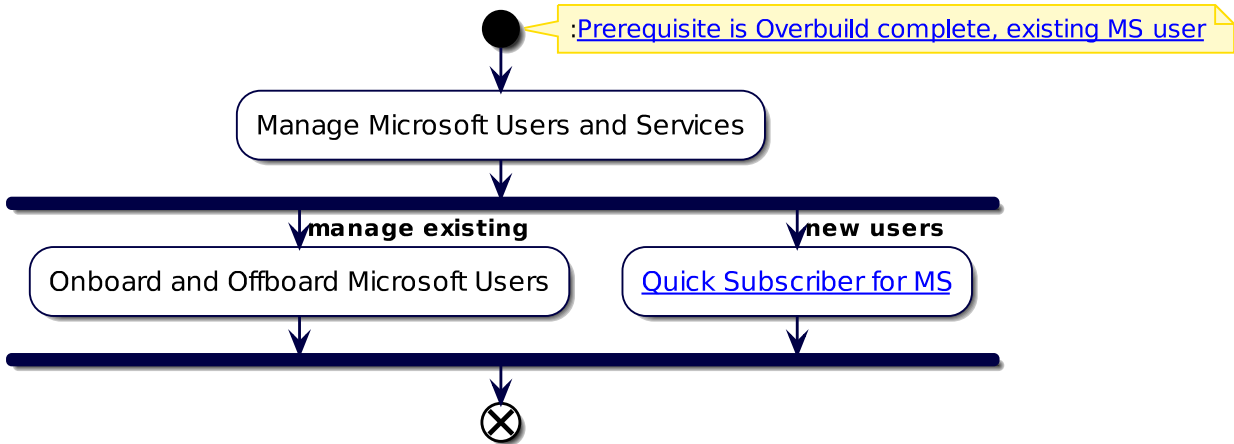
Overview

You will need to onboard Microsoft users to create Microsoft subscribers in VOSS 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 subscribers.

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 and subscribers via a single interface and login, from within the VOSS 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.



Related Topics

- Microsoft Overview in the Core Feature Guide
- VOSS Automate Configuration and Sync in the Core Feature Guide
- Sync with Flow Through in the Core Feature Guide
- Microsoft Exchange in the Core Feature Guide

Onboarding Microsoft Users

VOSS Automate provides two onboarding options for Microsoft users:

Sync users to customer level, and then to sites	<p><i>VOSS Automate Configuration and Sync</i></p> <p>This option starts with an initial import of dial plans, policies, licenses, and Microsoft users, to the customer level (sync all to the tenant).</p> <p>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, subscriber profiles, and number inventory). Finally, you have two options to move users to the sites as fully provisioned subscribers:</p> <ul style="list-style-type: none"> • Run the overbuild to move multiple users to your sites at once. • Update single users via Quick Subscriber (for Microsoft users) <p>When moving users to site, the VOSS Automate automated workflow applies the required configuration, services, lines, policies, and licenses.</p>
Sync users directly to sites	<p><i>Sync with Flow Through for Microsoft</i></p> <p>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 subscriber profiles.</p> <p>In addition, you will need to:</p> <ul style="list-style-type: none"> • Configure flow through provisioning criteria • Enable flow through in the Global Settings <p>Once changes are synced in from the Microsoft Cloud, VOSS 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 subscribers.</p>

Note:

- VOSS 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 CUCM (Call Manager).
- 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 CUCM users), see *Flow Through Provisioning*

Offboard a User

You can offboard a Microsoft subscriber by simply removing their Microsoft license, which removes all currently assigned services.

Note: In order to use this feature, you need to enable License Management in the Site Defaults Doc. Enable the setting **Manage Licenses and Allow User Staging** in your Site Defaults Doc.

If enabled, this setting will remove the license that is assigned to the user and will set the LineURI to null, i.e. disable MS Teams calling. If *not* set, then only the LineURI field is set to null and the user license is kept intact.

To offboard a user:

1. Log in to the Admin Portal.
2. Go to **MS Subscriber Management > Subscribers**.
3. Click on the relevant subscriber.
4. On the **MS Licenses** tab, delete the licenses.

View and Edit Microsoft Subscribers

This procedure displays and edits Microsoft subscribers.

View a summary list of all Microsoft subscribers

1. Log in to the VOSS Automate Admin Portal.
2. Choose the hierarchy.
3. Go to (default menus) **Microsoft Subscriber Management > Subscribers**.
4. On the **Subscribers** list, view a summary of Microsoft subscribers at the current hierarchy.

The Subscribers summary list view for Microsoft users provides details for the following, for each subscriber in the list:

- User principal name, first name, and last name
- Licenses
- Department
- City, country, phone number, location
- Associated device

View and update a single Microsoft subscriber

1. Log in to the VOSS Automate Admin Portal.
2. Choose the hierarchy.
3. Go to (default menus) **Microsoft Subscriber Management > Subscribers**.
4. On the **Subscribers** list, view a summary of Microsoft subscribers at the current hierarchy.
5. Click on a subscriber in the list to open the **Subscribers[subscriber name]** page.
6. Select one of the tabs on the page to view or update settings:

Tab	Description
MS 365	Microsoft user.
MS License	View, add, or delete this subscriber's Microsoft licenses.
MS Teams	The Microsoft subscriber's MS Teams details. The fields below are read-only: <ul style="list-style-type: none"> • User status • Interpreted User Type • Country or Region • Feature Types • Line URI • Line Type • Licenses Summary
Exchange Mailbox	The subscriber's user mailbox settings. You can update the mailbox display name, assign mailbox and calendar permissions to another user. See Microsoft Exchange in the Core Guide for details around managing other Microsoft Exchange mailbox types, such as shared or room mailboxes, or distribution groups.
Local User	The user corresponding with this subscriber.

4. Save your changes.

MS 365 MS Licenses MS Teams Exchange Mailbox Local User

User status: User Provisioned for MS Teams

Feature Types

- Teams
- PhoneSystem

Account Enabled

Is SIP Enabled

Line URI: tel:18683300050

Line Type: DirectRouting

Line URI TEL portion: 18683300050

Line URI EXT portion:

Dial Plan: Global

Meeting Policy: Global

Messaging Policy: Global

App Permission:

Subscribers [NestorW@vossautobuild.onmicrosoft.com]

MS 365 MS Licenses MS Teams Exchange Mailbox Local User

Display Name: Nestor Wilke

Permissions

- User: johnb
 - Access Rights
 - Read And Manage
 - Send As
 - Send On Behalf

Calendar Permissions

- User: PattiF
 - Access Rights
 - Owner
 - Publishing Editor

22.2.3. Microsoft Licenses

Overview

VOSS Automate can be used to assign, modify, and remove Microsoft user licenses.

To allow VOSS Automate to manage Microsoft user licenses, you will need to enable the following setting in the site's defaults (**Site Management > Defaults, MS Teams tab**): *Manage Licenses and Allow User Staging*

When VOSS Automate is enabled for license management:

- Admins can use Quick Subscriber to optionally configure the correct licensing and MS Teams configuration when onboarding new users.
- Microsoft license data can be synced in to VOSS Automate from the Microsoft cloud, and specified in the Quick Add Group (QAG) configuration templates as part of the provisioning workflow.

Users are placed in staging (an unsaved state) while license data is synced in to VOSS Automate. A licensed user may be assigned with a line and available number in VOSS Automate.

Targeted syncs may be scheduled from VOSS Automate to poll the Microsoft cloud for changes at regular intervals. Users are automatically provisioned in VOSS 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 VOSS Automate, and is flagged with the user's name.

Note:

- To view staged users, go to (default menu) **Subscriber Management > Subscriber Staging**.
 - Users can only be licensed and staged if the following setting in the site defaults is enabled (accessed via, default menus, **Site Management > Defaults**, on the **MS Teams** tab): *Manage Licenses and Allow User Staging*
 - Starting with VOSS 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.
-

View Microsoft Licenses by Customer

To view all Microsoft licenses synced currently synced in to VOSS Automate, go to (default menu) **Subscriber Management > Licenses**. The Licenses summary list view provides the following license details per customer:

- SKU ID
- Number of active licenses
- Number of used licenses
- Customer name

View a Subscriber's Microsoft Licenses

To view the license details of individual subscribers via the Subscriber management functionality:

1. Go to (default menu) **Subscriber Management > Subscribers**.
2. Click on a subscriber to open the Subscribers [subscriber name] page.
3. Select the **MS Licenses** tab.
4. View currently enabled licenses for the subscriber.

Offboarding Users and Licensing

Offboarding a user in VOSS Automate simply involves removing the user's licenses. See [Onboarding Microsoft Users](#)

Related Topics

- Microsoft Subscribers in the Core Feature Guide

22.2.4. VOSS Automate Configuration and Sync

Overview

When using VOSS Automate with Microsoft (as a single or multiple vendor deployment scenario), you'll need to pre-configure several settings in VOSS Automate before importing Microsoft users, licenses, policies, and dialplans.

Note:

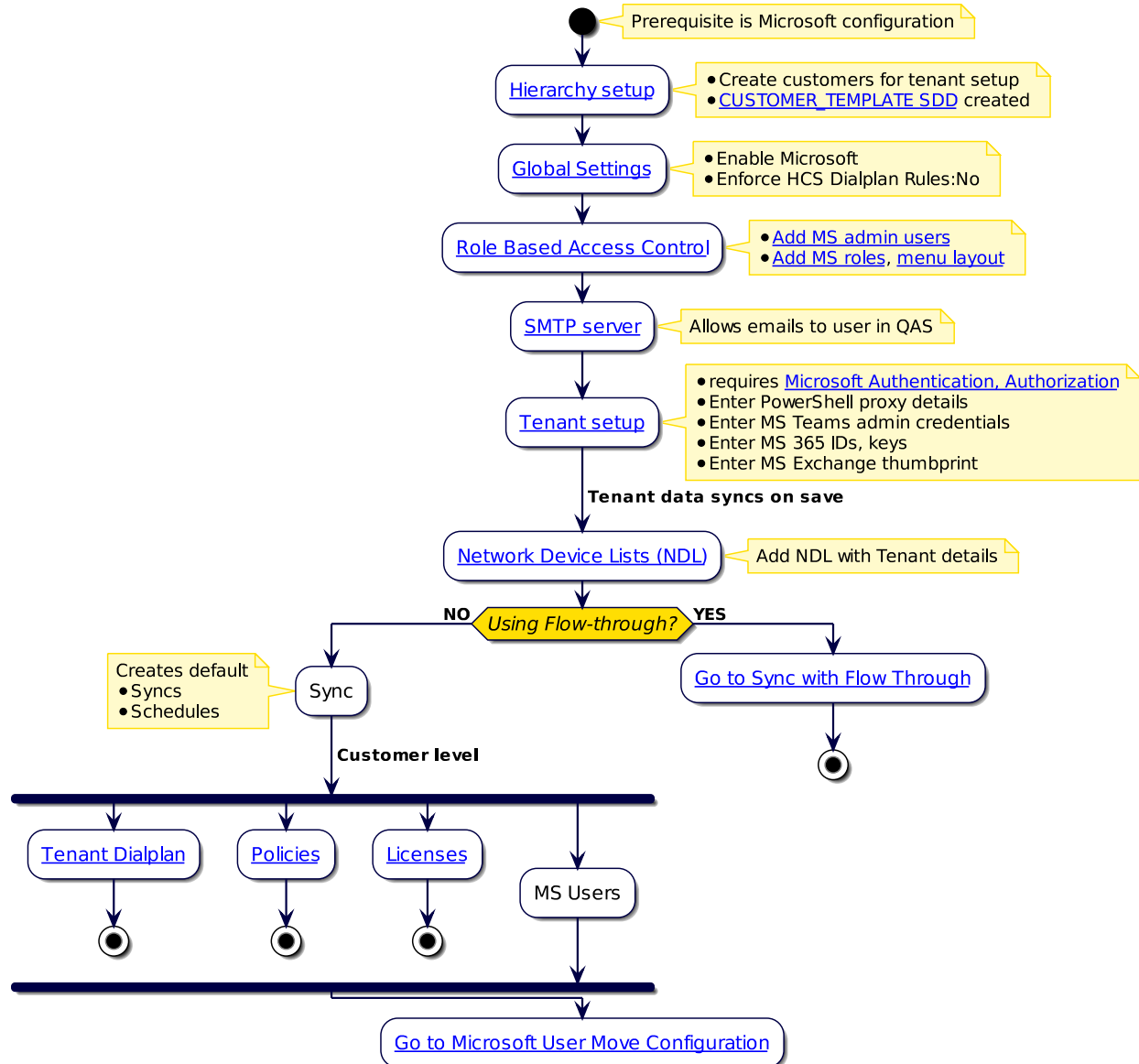
- VOSS Automate v21.2 introduced sync with flow through provisioning for Microsoft users. In 21.3, this feature extends the functionality to users synced in from LDAP and CUCM (Call Manager).
- Only *Add* is supported for syncs with flow through provisioning. Update and delete are not supported since the requirements may differ depending on the customer scenario.
- For details on the generic flow through provisioning feature (which includes Microsoft, LDAP, or CUCM users), see [Flow Through Provisioning](#)

Configuration Flowchart

The flowchart sets out the initial configuration of VOSS Automate for Microsoft services.

Prerequisites:

- [Microsoft Configuration](#)



Workflow for the VOSS Automate and Microsoft Configuration and Sync

The high-level workflow for the steps in the flowchart are as follows:

1. Log in to VOSS Automate as a provider admin.
2. Add customers.
3. Go to **Customizations > Global Settings** to enable Microsoft:
 - On the **Enabled Services** tab, enable Microsoft services.
 - 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:

Note: VOSS 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.

- Add an admin user. See [Add an Admin User](#).
 - Configure menu layouts, See [Add or Edit a Menu Layout](#).
 - Add user roles, and choose menu layouts for the roles. See [Add and Edit Roles](#).
 - Configure a SMTP server, if required. See [Add a SMTP Server](#).
-

5. Configure a tenant, one for each customer. See [Configure Microsoft Tenant Connection Parameters](#)

Note: The tenant configuration defines how VOSS Automate connects to the Microsoft Cloud to allow syncing of data between VOSS Automate and Microsoft Azure, Microsoft 365, Microsoft Teams, and Microsoft Exchange. Saving the tenant creates the default syncs and schedules.

6. Configure the network device lists (NDLs), which are required creating the sites. See [Add a Network Device List \(NDL\)](#)
7. Go to the tenant configuration screen, and click **Action > Sync All** to run a full pull sync.

The tenant dialplan, policies, licenses, and Microsoft users are synced to the customer level.

Note:

- If you're using flow through provisioning for Microsoft users, additional steps are required before running the initial sync. See [Sync with Flow Through for Microsoft](#)
- From release 21.3-PB1, an **Action > Sync New Users** option is available to *only import the users* to be added from the following models:
 - `device/msgraph/MsolUser`
 - `device/msteamsonline/CsOnlineUser`
 - `device/msteamsonline/ApplicationInstance`

In order for this sync method to be enabled initially after upgrade to 21.3-PB1, 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 are disabled by default.

Related Topics

- Microsoft Overview in the Core Feature Guide
- Sync with Flow Through in the Core Feature Guide
- Move users to the sites. See [Microsoft User Move Configuration](#)
- [Flow Through Provisioning](#)

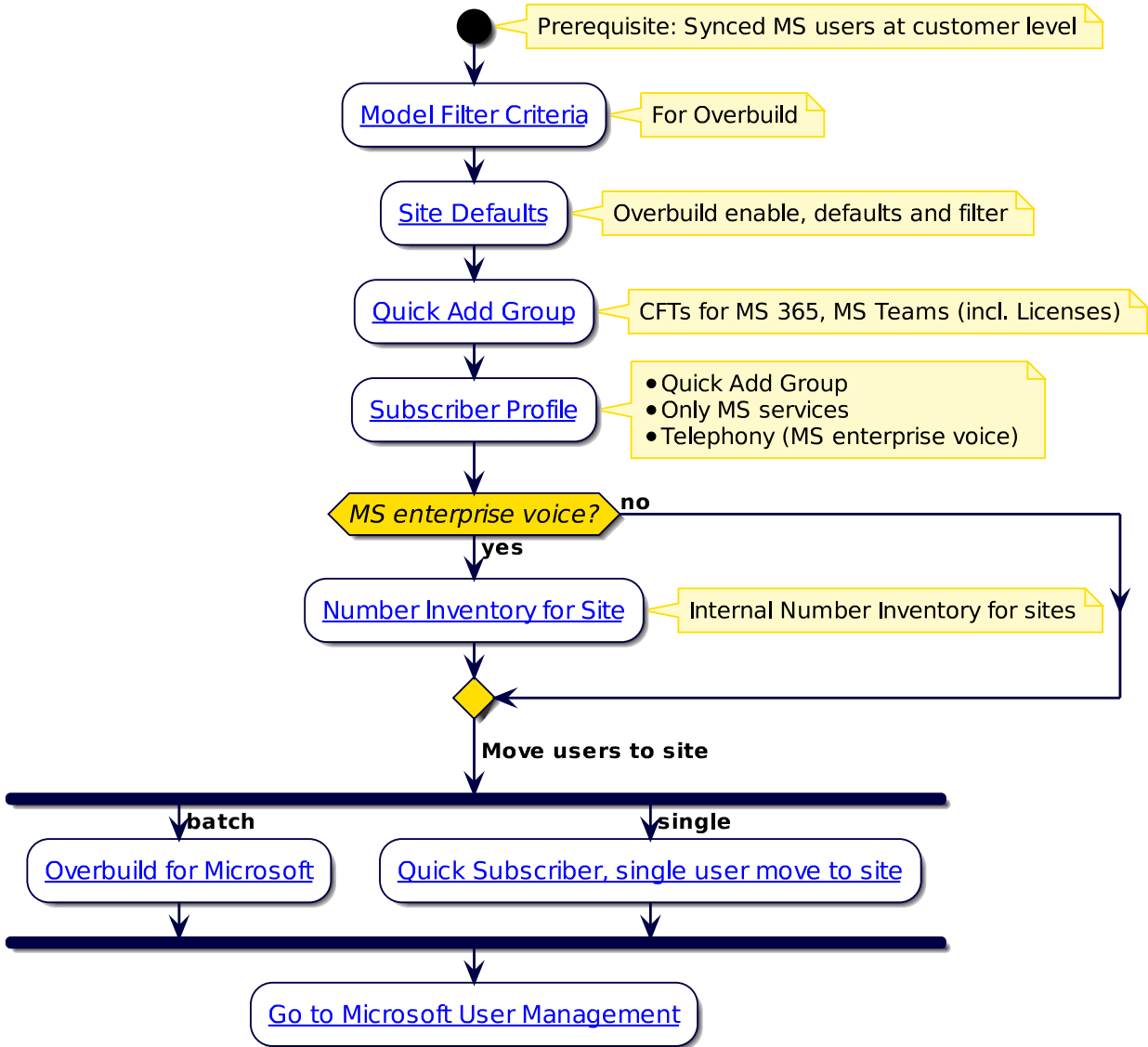
22.2.5. Microsoft User Move Configuration

This topic provides a workflow 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.

Prerequisites:

- [Microsoft Configuration](#)
- [VOSS Automate Configuration and Sync](#)

The flowchart sets out the steps to move Microsoft users to the sites after an initial sync to move users to the customer level:



Related Topics

- *Introduction to Microsoft UC Integration*
- *Sync with Flow Through for Microsoft*

22.2.6. Quick Subscriber for Microsoft Users

This procedure displays and updates a Microsoft user, and moves the user to the correct site, with all configuration and licensing applied.

Note: Quick Subscriber 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 Subscriber, you select the relevant QAG, and the automated workflows in VOSS 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 MS 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 (default menu) **MS Subscriber Management > Quick Subscriber**.
3. Choose the relevant site.
4. On the Quick Subscriber page:
 - Required. In the **Username** field, select the user to populate fields on the page.
 - To include users higher in the hierarchy in the **Username** drop-down, select **Include users at higher hierarchy**.
 - To send a subscriber 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*
-
- Required. From the **Quick Add Group** drop-down, select the relevant Quick Add Group (QAG) (licenses the user and applies settings defined in the QAG).
 - 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:

- The **Line URI** and **Use next available line** fields display *only* when **Feature Type** is *PhoneSystem*, or **Manage Licenses and Allow User Staging** is enabled (via the **MS Teams** tab in the site default docs).

- The **Enterprise Voice Enabled** option has been deprecated since PowerShell V4.0.0. Setting **Enterprise Voice Enabled** is no longer required. To enable a user for Voice, ensure the user has a **Line URI** set and that the **Feature Type** shown contains Teams, PhoneSystem.
- The **Line URI** drop-down displays available lines (staged lines 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.
- The default for **Use next available line** is False (disabled).

When selecting **Use next available line**:

- * If the user does not already have a line, they are 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 will not be used.

- Optionally, from the **Tenant dial plan** field, choose a tenant dial plan.

Note: Choosing a tenant dial plan different from the default set up in the site defaults (SDD) overwrites the default. If you don't choose an option for this field, the tenant dial plan set up in the SDD applies.

- 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 **MS Subscriber Management > Subscriber 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, which searches only for staged users (not all users from the tenant). Once the sync completes, the user becomes a fully provisioned subscriber, and the number is flagged as used. The subscriber receives a welcome email (if you've chosen this option, and you have a SMTP server configured).

Users can only be staged if the following setting in the site defaults is enabled (accessed via, default menus, **Site Management > Defaults**, on the **MS Teams** tab): *Manage Licenses and Allow User Staging*

Starting with VOSS 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.

6. Verify that the subscriber is configured and licensed:

- Go to (default menu) **Subscriber Management > Subscribers**.

Note: The **Located At** column on the Subscriber list displays the hierarchy location of each subscriber added to the system, for example, customer or site.

- Click on the subscriber to open the Subscribers[name] page.

- On the **MS Licenses** tab, view the subscriber's license details.
- On the **MS Teams** tab, verify the following:
 - The user's number is allocated
 - Policies are assigned

Related Topics

- Microsoft Subscribers in the Core Feature Guide
- Microsoft User Move Configuration in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide
- Subscriber Staging (Microsoft Users) in the Core Feature Guide
- Microsoft Licenses in the Core Feature Guide

22.2.7. Subscriber Staging (Microsoft Users)

When onboarding Microsoft users into VOSS Automate, unlicensed Microsoft 365 users are synced in to VOSS Automate from the Microsoft Teams cloud portal.

It is possible to license Microsoft users from within VOSS Automate. You could use Quick Subscriber 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, VOSS Automate places the user in a staging queue while it waits for the Microsoft cloud process to complete.

A scheduled staging sync and workflow executes every 30 minutes. This workflow removes the user from staging, re-runs the Quick Subscriber workflow, updates the Microsoft Teams user with their correct provisioning details, provisions the subscriber in VOSS Automate, and flags their number as used.

Note: While the staging workflow runs every 30 minutes, 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, you can perform an un-stage action on the Subscriber Staging page to immediately execute the workflow.

Related Topics

- Microsoft Subscribers in the Core Feature Guide
- Quick Subscriber for Microsoft Users in the Core Feature Guide
- Site Defaults in the Core Feature Guide

22.2.8. Overbuild for Microsoft

Important: It is recommended that VOSS Automate training and/or VOSS Services are engaged during the initial use of the feature to help ensure optimized processes and guidance.

The Overbuild feature enables Provider and Reseller Administrators to integrate existing, deployed Microsoft Tenants into VOSS Automate without re-provisioning, unless required.

In VOSS 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 VOSS Automate components as a hierarchy or a subscriber, the relationship with Microsoft Tenant components makes it possible to, for example, create a VOSS Automate subscriber 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 VOSS Automate that can be set up to run at a selected interval.

The table describes overbuild logic for handling users and subscribers:

Component	Description
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 .
Subscribers	A Microsoft tenant user can be set up with services using Quick Subscriber.

Related Topics

- [Quick Subscriber for Microsoft Users](#).

Configure Overbuild Site Defaults for Microsoft

Pre-requisite:

- [Microsoft User Move Configuration](#)

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.
- 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 VOSS Automate Admin Portal, go to (default menus) **Overbuild > Site Defaults**.

Note: Alternatively, go to (default menus) **Site Management > Defaults** and select the **Overbuild Defaults** tab.

2. Select the **Overbuild Defaults** tab.
3. Configure the following:
 - Enable **Include Site for Overbuild**
 - Enable **Microsoft Users**.
 - From the **MS 365 User Model Filter Criteria** dropdown, select the relevant filter. For more information about filters, see [Model Filter Criteria](#).

Run Overbuild

1. In the VOSS Automate Admin Portal, go to (default menus) **Overbuild > Run Overbuild**.
2. Choose the site.
3. In a Microsoft-only environment, select only **Microsoft Users** to include in the overbuild.

Note: This allows Microsoft users to move to the site. VOSS 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: The overbuild:

- Imports and provisions subscribers, including number assignment (INIs).
- 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 [Audit Number Inventory](#).

Related Topics

- Microsoft User Move Configuration in the Core Feature Guide
- Model Filter Criteria in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide

22.2.9. Sync with Flow Through for Microsoft

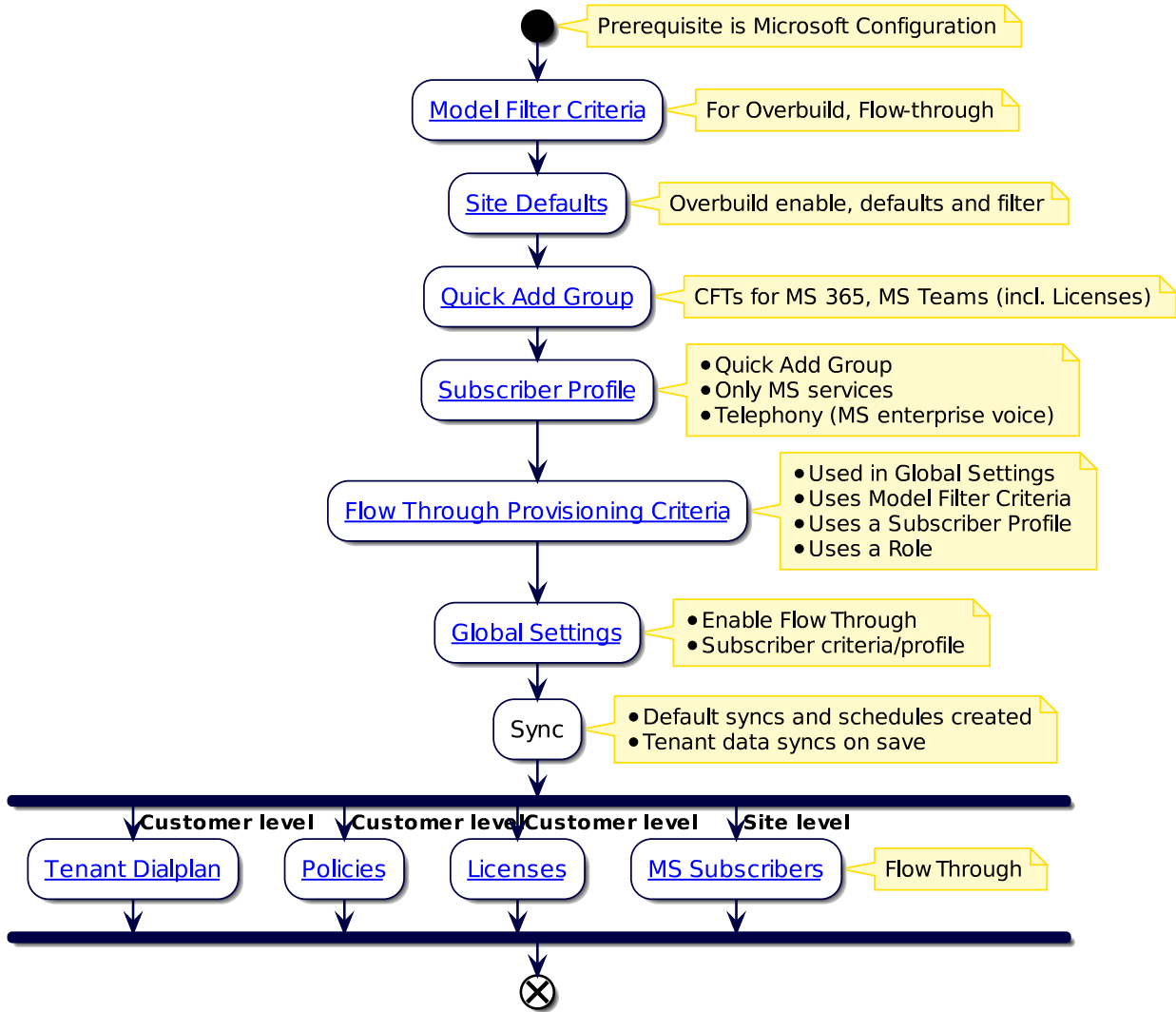
When using sync with flow through provisioning for Microsoft users, you will need to configure several settings in VOSS Automate (including flow through provisioning criteria) before the initial sync from the Microsoft Cloud. This allows VOSS Automate to apply the correct configuration, licenses, policies, 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, as subscribers.

The flowchart sets out the sync with flow through of Microsoft user and services.

Prerequisites:

- Microsoft Configuration in the Core Feature Guide
- VOSS Automate Configuration and Sync in the Core Feature Guide



Related Topics

- Microsoft Overview in the Core Feature Guide
- Flow Through Provisioning in the Core Feature Guide

22.2.10. Microsoft Exchange

This feature allows you to manage Microsoft Exchange Online mailboxes and calendars from within VOSS Automate, including assigning access and calendar permissions to users and team members licensed for Microsoft Office.

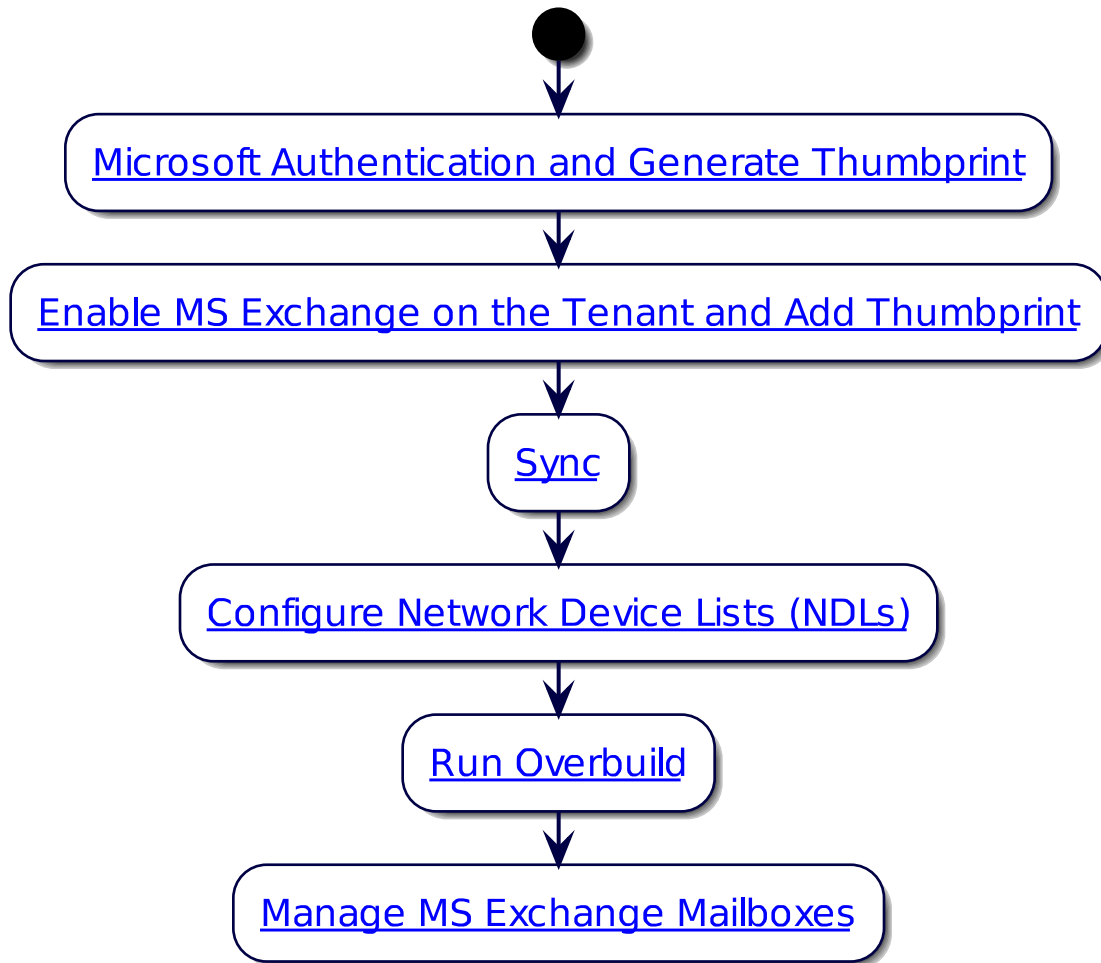
Note:

- VOSS Automate does not support adding Microsoft Exchange mailboxes from Quick Subscriber (for Microsoft users).

- Any admin role (Provider, Customer, Site) can access and work with Microsoft Exchange mailboxes, provided that Microsoft is enabled at the hierarchy.

Microsoft Exchange Integration

The diagram displays the workflow steps for integrating VOSS Automate with Microsoft Exchange:



The table describes the steps in the Microsoft Exchange integration workflow diagram:

Integrate Microsoft Exchange	Description
1. Generate thumbprint	Upload certificates on Microsoft Cloud, and generate the authentication thumbprint required for integration.
2. Configure Microsoft tenant	To prepare for the sync in of Microsoft Exchange components to VOSS Automate, enable Microsoft Exchange on the Microsoft tenant in VOSS Automate, and add the certificate thumbprint generated on Microsoft Cloud.
3. 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.
4. 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 (the thumbprint generated on Microsoft Cloud) to the network device lists (NDLs) for sites with subscribers requiring mailbox management in VOSS Automate.
5. 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.
6. Manage mailboxes	<p>Once you've set up VOSS 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 VOSS Automate:</p> <ul style="list-style-type: none"> • Assign access and calendar permissions for user mailboxes • Add, update, or delete shared mailboxes, including assigning or removing mailbox access and calendar permissions

Supported Microsoft Exchange Mailboxes in VOSS Automate

Four types of Microsoft Exchange mailboxes are supported in VOSS 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 VOSS Automate.

Any changes made to the mailboxes and their associated calendars are synced between the Microsoft Cloud portal and VOSS Automate. This allows a VOSS Automate admin user to manage mailboxes from within VOSS Automate, and have these changes seamlessly update on the Microsoft Cloud.

The table describes the Microsoft Exchange mailboxes supported in VOSS Automate, and the ways in which you can work with these mailboxes:

Mailbox type	Description
User	<p>User mailboxes are assigned to a single, licensed, Microsoft Office user. These mailboxes are created on Microsoft Exchange Online and synced in to VOSS Automate.</p> <p>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.</p>
Shared	<p>Shared mailboxes can be created on Microsoft Exchange and synced in to VOSS Automate, or they can be added, updated, or deleted on VOSS Automate, and any changes are then synced back to the Microsoft Cloud portal.</p> <p>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 calendar permissions on the shared mailbox.</p> <p>The owner, or user principal, of a shared mailbox is a 'dummy', unlicensed user on the Microsoft Cloud, and does not add to the VOSS Automate subscriber count. The user principal name of a shared mailbox is auto-generated based on the display name you define.</p>
Room	<p>Room mailboxes can be created on Microsoft Exchange and synced in to VOSS Automate, or they can be added, updated, or deleted on VOSS Automate, and any changes are then synced back to the Microsoft Cloud portal.</p> <p>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.</p>
Distribution Group	<p>Distribution Groups can be created on Microsoft Exchange and synced to VOSS Automate, or they can be added, updated, or deleted on VOSS Automate, and any changes are then synced back to the Microsoft Cloud portal.</p> <p>A distribution group is typically used to send emails to a group of recipients.</p>

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 VOSS 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 VOSS Automate. User mailboxes may be updated in VOSS Automate, but they can be added or deleted only on the Microsoft Cloud portal.

To manage Microsoft Exchange mailboxes in VOSS Automate:

1. Log in to the VOSS Automate Admin Portal.
2. Go to (default menus) **Microsoft Subscriber Management > Exchange**
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.

5. Choose an action in the list view:
 - To move one or more mailboxes to a different level of the hierarchy, select the relevant checkboxes, then click **Move**.
 - To export the data of one or more mailboxes, select the relevant checkboxes, then click **Export**. Choose an export format, and click **Export**.
 - To delete one or more mailboxes (shared or room mailboxes, or distribution groups only), select the relevant checkboxes, and click **Delete**.
 - To 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, and click **Save**. Go to step 6 to update the mailbox permissions and settings.
 - To view or update a mailbox, click in the relevant row to open the mailbox management screen. Go to step 6 to update the 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.
 - Delete is allowed for shared or room mailboxes, or distribution groups only.
 - If this is a room mailbox:

- 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.
- If this is a distribution group, add one or more members (users with access permissions for sending emails as a selected user, or on behalf of a selected user).

7. Assign or remove permissions:

- 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.
- 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.

8. Save your changes.

Related Topics

- [Configure Microsoft Tenant Connection Parameters in the Core Feature Guide](#)
- [Overbuild for Microsoft in the Core Feature Guide](#)

22.3. Multi Vendor Subscribers

22.3.1. Multi Vendor Subscribers

The multi vendor subscribers feature allows you to provision and manage services from one or more vendors on the VOSS Automate platform. For example, to use both Microsoft meeting and collaboration tools and Cisco tools.

Single or Multi Vendor Subscribers

VOSS Automate supports provisioning for a number of categories of subscriber, representing either a single or multi vendor deployment:

Single or Multi Vendor	Description
Single vendor subscriber	Subscribers using services from a single vendor, for example, either all Cisco services, or all Microsoft services.
Multi vendor subscriber	Subscribers using services from two or more vendors.
Multi vendor hybrid subscriber	Subscribers using services from two or more vendors, with services configured for integration, for example, with dial plans and routing.

View Multi Vendor Subscribers (Lists)

You can access a multi vendor subscribers service summary list view from:

Interface	Description
Admin GUI	Go to (default menu): User Management > User Services > Multi Vendor Subscribers
Business Admin Portal	<p>View subscribers from (default menu):</p> <ul style="list-style-type: none"> • Subscribers menu • Home page <ul style="list-style-type: none"> – Subscribers service card – Quick Actions link (View Subscribers) <hr/> <p>Important: Multi vendor subscriber must be enabled (via the Subscribers tab in the Business Admin Portal profile) for both multi-vendor subscribers and hybrid subscribers.</p> <hr/>

Related Topics

- **Configuration**
 - Configure Multi Vendor Subscribers in the Core Feature Guide
 - Global Settings
 - Role-based Access for Multi Vendor Subscriber in the Core Feature Guide
- **Field Display Policies**
 - Multi Vendor Subscriber Field Display Policy in the Core Feature Guide
- **Profiles**
 - Business Admin Portal Profiles in the Core Feature Guide
 - Entitlement in the Core Feature Guide
- **Subscribers and Users**
 - View and Manage Subscribers in the Business Admin Portal Guide
 - Users and Subscribers in the Core Feature Guide
 - Subscribers in the Business Admin Portal Guide
 - Enable User to Host Conference Now in the Business Admin Portal Guide
- **Interface**
 - View Subscribers in the Core Feature Guide

22.3.2. Configure Multi Vendor Subscribers

This procedure enables multi vendor subscriber, and involves the following tasks:

- Configure Global Settings
- Configure the multi vendor field display policy (MultiVendorFDP)
- Enable multi vendor in the Business Admin Portal profile.
- Assign the Business Admin Portal profile configured for multi vendor to relevant user roles.
- Configure entitlement profiles.
- Verify that you have appropriate servers installed and configured.

Perform these steps:

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. Configure the Global Settings for multi vendor:
 - Go to (default menu) **Customizations > Global Settings**.
 - On the **Enabled Services** tab, enable services, as required.
 - Save your changes.

Note: For new installs of VOSS Automate, once a CUCM is imported and a customer hierarchy and some sites have been created, CUCM services are enabled by default at system level; other services must be enabled, as required. The Global Settings are retained on upgrade.

4. Configure the multi vendor subscriber field display policy:
 - Go to (default menu) **Customizations > Field Display Policies**.
 - Click on the default multi vendor field display policy (MultiVendorFDP) to open its editing screen.
 - Click **Action > Clone** to create a copy of the default FDP.

Note: It is recommended to clone default templates rather than overwriting default settings. The multi vendor FDP is associated with the model relation/MultiVendorSubscriber.

- Edit the cloned multi vendor FDP:
 - 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.

- * Change card titles.
- * Choose whether to display the card as a fieldset with columns.
- * Change fields 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 subscriber**
 - `_qa` is *Quick Action*

If a service or action is disallowed in the global settings, entitlement profile, or the Business Admin Portal 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 Subscriber management dashboard (defined via the FDP), and the subscriber cannot be provisioned with this service.

- Save your changes.

5. Enable multi vendor in the Business Admin Portal profile:

Note: Required only if you're using the Business Admin Portal. Only admin users with an access profile that allows updates to the Business Admin Portal profiles may perform this step.

- In the Admin Portal, go to (default menu) **Customizations > Business Admin Portal Profiles**.
- Click on the relevant profile to open the editing screen. Update an existing cloned profile, or clone a profile to create a new custom profile.
- On the **Subscribers** tab, select **Enable Multi-Vendor**. The multi vendor field display policy is applied.
- Save your changes.

6. Assign the multi vendor-enabled Business Admin Portal profile to relevant user roles:

Note: Required only if your organization uses the Business Admin Portal.

- Go to (default menu) **Roles > Role Management**.
- Click on the user role to open its editing screen.

- In **Custom Interfaces**, from the **Interface Type** field, select `InterfaceBusinessAdminPortal`, and in the **Name** field, select profile name.
 - Save your changes.
7. Optional. Configure entitlement profiles for multi-vendor:
 - Go to (default menu) **Entitlement > Profiles**.
 - Click on the relevant entitlement profile to open its editing screen.
 - Select the services you wish to enable for the profile.
 - Save your changes.
 8. Verify that you have appropriate servers installed and configured:
 - Go to (default menu) **Apps Management**, and select the relevant server, for example, for CUCM, select **CUCM > Servers** to view and manage the servers.
 - Repeat this step to verify the presence of all required servers.
 9. Verify that you can view multi vendor subscribers in the Business Admin Portal (if applicable):
 - In the Business Admin Portal, log out and log in (or refresh the page) to apply the new profile.
 - Click the **Subscribers** menu to view multi vendor subscribers.
 - The Subscribers list view **Services** column presents service icons and tooltips indicating the vendor.
 - The Subscriber dashboard displays service cards selected for the multi vendor field display policy.

Note: Service cards are loaded dynamically based on the configuration defined via the FDP. You can edit the FDP to change the content and display of the service cards.

Related Topics

- Multi-vendor Subscribers in the Core Feature Guide
- Global Settings
- Business Admin Portal Profiles in the Core Feature Guide

22.3.3. Role-based Access for Multi Vendor Subscribers

Overview

Role access profiles define the permissions that allow subscribers to access services and resources.

Validation Checks

When provisioning multi vendor services, the system runs validation checks for multi vendor subscriber 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:

Validation	Interface	Description
1. Global Settings	Admin Portal Navigation (default menu): Customization > Global Settings (Enabled tab)	Enable the service type at the user's hierarchy level, or above.
2. Entitlement profile	Admin Portal Navigation (default menu): Entitlement > Profiles	Enable the service in the entitlement profile assigned to the subscriber, at the relevant site. Services can only be provisioned to a subscriber if their entitlement profile allows those services. The entitlement profile lists the provisioning vendor (per service).
3. Device management	Admin Portal Navigation (default menu): Apps Management > Servers	The relevant servers must be installed and configured before a service can be provisioned. For example, a CUCM server must be installed before CUCM services, such as phones, can be provisioned. If you have two or more vendors provisioning devices, VOSS 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: Navigation (default menu) Customizations > Field Display Policies Enable multi vendor in the Business Admin Portal profile: Navigation (default menu) Customizations > Business Admin Portal Profiles	Clone and edit the default multi vendor subscriber field display policy (default name: MultiVendorFDP). Enable multi vendor in the Business Admin Portal profile (Base/Details tab, and Subscribers tab), and select the multi vendor FDP to define the services the subscriber can view and manage in the Business Admin Portal lists, dashboards, and service management screens.

Multi Vendor Subscriber 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 subscriber 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 subscriber services
- The site admin may not add or delete subscriber services

The table describes the configuration steps to set up this scenario, and the result:

<p>Configuration steps</p>	<ol style="list-style-type: none"> 1. Ensure the system has multi vendor subscriber functionality installed. 2. At customer level or above, in the Global Settings (Enabled Services tab), enable CUCM only. 3. In the Entitlement Profile for this user, enable CUCM Voice Service only. 4. At site level, select Multi Vendor Enabled for the Business Admin Portal access profile for subscribers, and choose the multi vendor subscriber field display policy (default name: MultiVendorFDP) 5. At site level, configure the multi vendor subscriber field display policy for the profile: <ul style="list-style-type: none"> • Remove all service cards except Voice. • Remove Add/Delete fields from the Quick Actions panel.
<p>Result</p>	<p>The site admin logs in to a multi vendor subscriber enabled system, at the relevant site hierarchy, and:</p> <ul style="list-style-type: none"> • Can view subscriber voice services in the Business Admin Portal. • 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 Subscribers in the Core Feature Guide
- Global Settings in the Core Feature Guide
- Multi Vendor Subscriber Field Display Policy in the Core Feature Guide
- Business Admin Portal Profiles in the Core Feature Guide
- Entitlement in the Core Feature Guide

22.3.4. Multi Vendor Subscriber Field Display Policy

The multi vendor subscribers field display policy (default: `MultiVendorFDP`) defines the look and feel of the **Subscriber** dashboard in the Business Admin Portal, and shows/hides services and MACD actions for multi vendor subscribers.

This field display policy allows you to:

- Change card titles
- Define the content displayed on the cards, including display fields in User Details, and actions in Quick Actions
- Re-order the card layout on the dashboard

The multi vendor FDP must be associated with a Business Admin Portal profile to allow users to view and work with multi vendor subscribers in the Business Admin Portal.

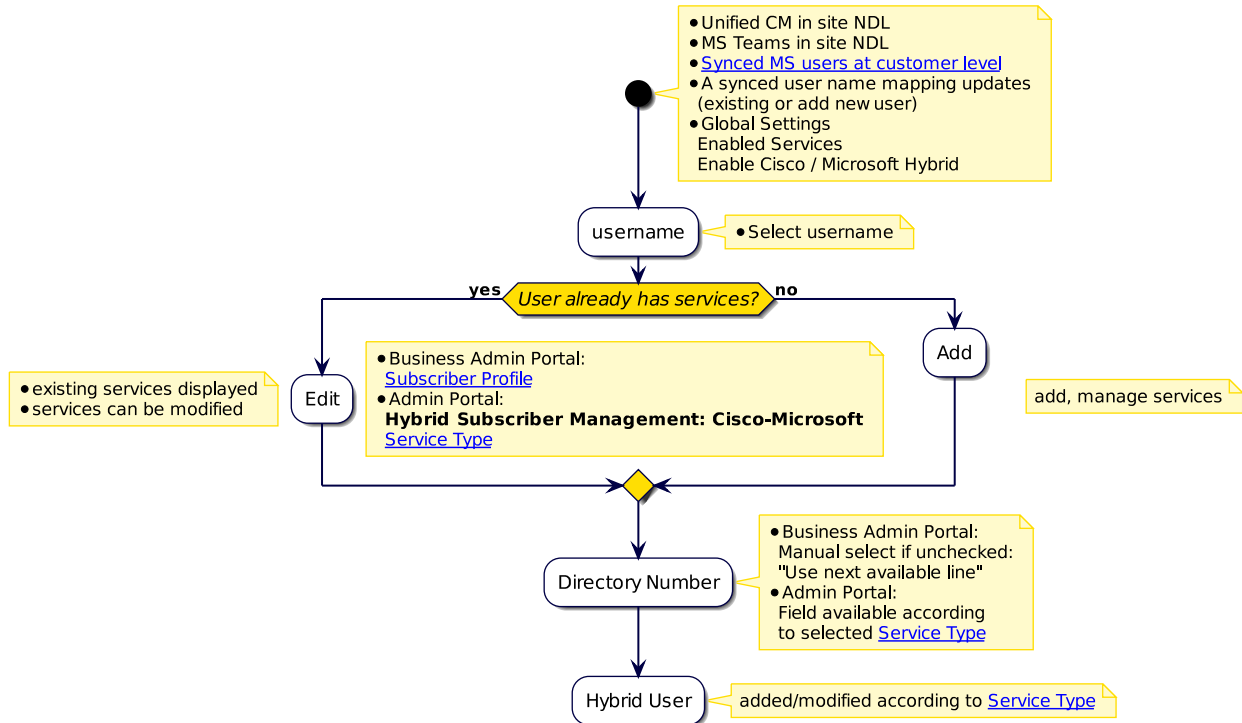
When enabling multi vendor in a Business Admin Portal profile (**Subscribers** tab), the profile uses the multi vendor FDP. The Business Admin Portal profile must be assigned to a user role to allow users with this role to view and manage multi vendor subscribers.

Related Topics

- Multi Vendor Subscribers in the Core Feature Guide
- Configure Multi Vendor Subscribers in the Core Feature Guide
- Field Display Policies in the Core Feature Guide

22.4. Hybrid Cisco-Microsoft Subscribers

22.4.1. Overview: Microsoft - Cisco Hybrid



22.4.2. Hybrid Cisco-Microsoft Management

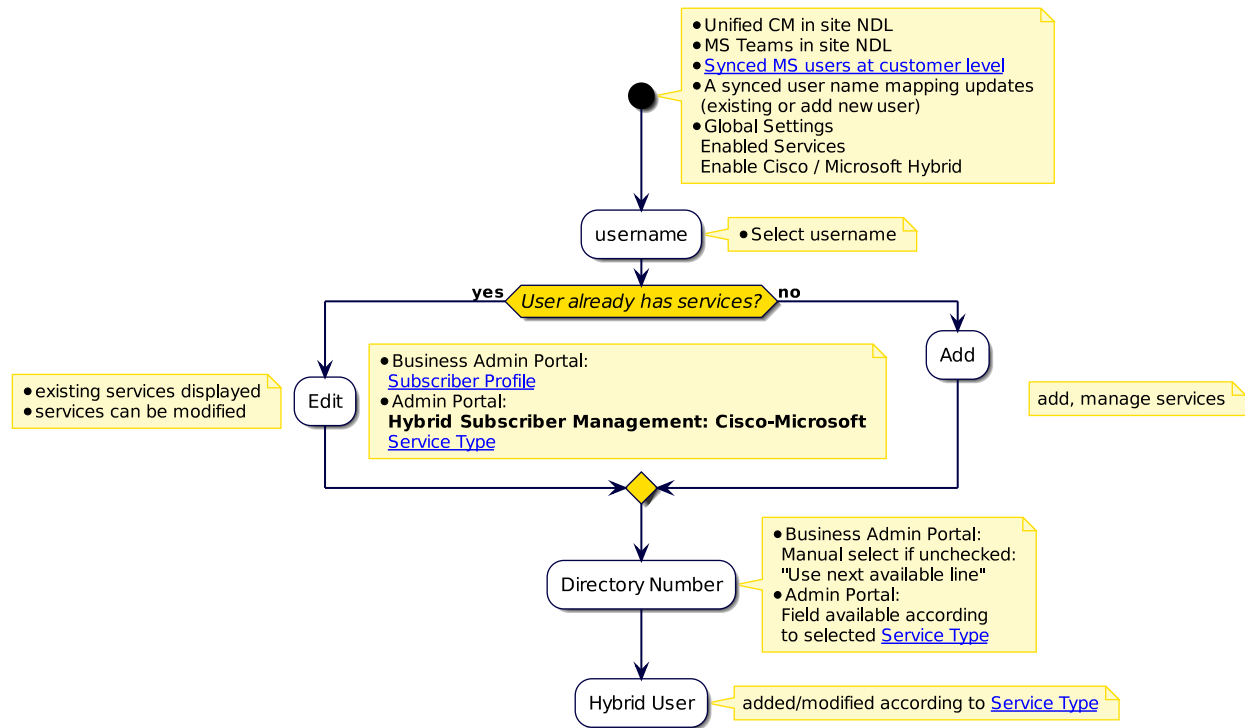
Use the **Hybrid Subscriber Management: Cisco-Microsoft** menu to provision and manage subscribers with Cisco and Microsoft devices and services.

Note: In the Business Admin Portal, these tasks can be carried out by means of the selection of a **Subscriber Profile** for the user where the **Hybrid** option is the selected **Subscriber Profile** and a **Hybrid Service** is selected.

See:

- [Subscriber Profiles](#)
- [Hybrid Service Definitions](#)

Provisioning Flow



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 Configuration](#).

Perform these steps

Note: For a selected user from the **User Management > Users** menu, 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 (default menu) **Hybrid Cisco-Microsoft Management > 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.
 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](#).

Related Topics

- [Global Settings](#)
- [Hybrid Service Definitions](#)
- [Subscriber Profiles](#)
- the Number Inventory Updates for Hybrid Support topic under Number Management

22.4.3. 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 **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
- **Class of Service** and **Entitlement Profile:** by default empty

The service type offers automatic configuration of services according to the selected **Directory Number** in the Admin GUI or in the Business Admin Portal: disabling **Use next available line** and then the selected **Line**. This is carried out by a workflow selecting the appropriate dialplan template addition.

Important: VOSS 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

- **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.

- **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

- **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

- **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

- **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

Related Topics

- [Hybrid Cisco-Microsoft Management](#)
- [Subscriber Profiles](#)
- the Cisco - Microsoft Hybrid Number Inventory topic under Number Management

22.5. Quick Add Subscriber

22.5.1. Quick Add Subscriber for CUCM Users

Overview

VOSS Automate Quick Add Subscriber (QAS) for Cisco Unified Communications Manager (CUCM) provides a single page where you can:

- Add users to CUCM.
- Add users to voicemail and WebEx accounts.
- Provision users with services, such as Voice, Extension Mobility, Voicemail, Single Number Reach (SNR), and conferencing and collaboration services. For example, see [Provision the Voice Service](#)
- Add lines for CUCM users.
- Associate a device pool directly from the user interface to a subscriber's newly associated devices or services other than the device pool provided in the Site Defaults Doc (SDD) or reference Configuration Template (CFT) in the Quick Add Group (QAG). See [Quick Add Subscriber Device Pool](#) for details.
- Associate Calling Search Space (CSS) values to a subscriber's newly associated lines, devices, or services other than the CSS's provided in the Site Defaults Doc (SDD) or reference Configuration Template (CFT) in the Quick Add Group (QAG), by selecting a Class of Service (CoS) directly from the interface. See [Quick Add Subscriber Class of Service](#) for details.

User types supported by QAS

QAS for CUCM users supports several user types, including:

- LDAP users
- Cisco Unified Communications Manager (CUCM) integrated users
- LDAP-integrated users on CUCM
- Manually created users

Note: If the default Self-service Language is set on the site default docs (SDD), users are assigned the corresponding Self-service language.

Quick Add Groups and Quick Add Subscriber

You will need to choose a Quick Add Group (QAG) when adding a subscriber via QAS. If Webex App is enabled, select the QAG that configures the required Jabber devices.

QAS default template

To add subscribers using QAS, a default user template called "voicemailusertemplate" must exist on the CUCM. This default can be updated by editing the default CUC User Template value in the SDD.

Self-provisioned phones and QAS

For self-provisioned phones to show as being associated with a subscriber, perform a CUCM data sync after setting up a self-provisioned phone.

Updating a subscriber added via QAS

Any changes you want to make to a subscriber or their associated services after adding the subscriber via QAS is done from the relevant service menu items.

Enabling services via QAS

When adding a subscriber via Quick Add Subscriber (QAS), you can enable user services, such as voicemail, extension mobility, single number reach, conferencing (meetings), and collaboration (messaging) services (such as Webex App).

See also: [Webex App Quick Add](#)

The QAS page only displays services that are included in the entitlement profile you select on this page. For example, if the entitlement profile does not include 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).

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 Subscriber Template.
The default value (voicemailusertemplate) should already exist on the CUCM and is automatically populated on an HCS system when a voicemail pilot is created.
- A CUC device must be configured at the related NDL (Network Device List) 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 Subscriber 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 CUCM (call manager) must be configured at the subscriber's hierarchy. If this does not exist, the QAS bulk load transactions and API calls display the following warning: *No Call Manager has been configured*

Webex App Quick Add

Selecting the **Webex App** checkbox on the QAS 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.

If you want customized values, clone the **Webex Teams User Template (Customizations > Configuration Templates)** and edit as required. The Webex Teams User Template for CUCM 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.

Related Topics

- [Provisioning Subscribers with Webex App](#)

Add a CUCM User via Quick Add Subscriber

This procedure adds a CUCM user via Quick Add Subscriber (QAS).

Pre-requisites:

- To choose phones by their description or description and line, configure the Global Setting (Phones tab) for displaying additional information.
- Configure Quick Add Groups. See [Quick Add Subscriber Groups](#)
- If required, expose Device Pools and Class of Service in Quick Add Subscriber. See [Expose Device Pools and Class of Service in Quick Add Subscriber](#)
- Ensure the site defaults are correctly configured.

Note: Devices and services associated with the user display on the **Existing Services** tab on the QAS form. The visibility of fields associated with existing services in QAS is enabled and disabled at the Customer level via the Global Settings. Disabling a service in the Global Settings hides the field associated with the service on the QAS form. If you wish to enable and display the service in QAS, you need to enable it in the Global Settings (**Enabled Services** tab).

Perform these steps

1. Log in to the Admin Portal, then go to (default menus) **Subscriber Management > Quick Add Subscriber**.
2. On the **User Details** tab:
 - Select the username, and specify a first name and last name.
 - Fill out the user's email address, and define whether to send the user a welcome email.
 - Fill out a password and PIN.
 - Select an entitlement profile, and a Quick Add Group.
 - Choose a device pool.

- Add lines, and choose a directory number.

Alternatively, select **Use next available line** to automatically populate the **Directory Number** field with the next available line. The default for **Use next available line** is False (disabled).

- Select **Voice**, then fill out the additional configuration fields that display when this option is chosen.
- Select additional services, such as extension mobility, voicemail, Webex App, Single Number Reach (SNR), Jabber / Dual-Mode device, and define whether you wish to enable self provisioning for this user.

Note: 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).

3. Save your changes.

Related Topics

- Global Settings in the Core Feature Guide.

22.5.2. Quick Add Subscriber Device Pool

A Device Pool contains system, device, and location-related information, and is mandatory when adding a Subscriber using Quick Add Subscriber. A Device Pool can be referenced by:

- Site Defaults Doc (SDD)
- Reference Configuration Template (CFT) referenced in the Quick Add Subscriber Group (QAG)
- Admin Portal (if exposed)

Site Defaults Doc

The Device Pool referenced in the SDD makes sure that a Subscriber'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.

Quick Add Subscriber Group (QAG)

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 Subscriber Groups](#) for details.

Admin Portal

An Administrator can expose a Device Pool drop-down on the QAS page on the Admin Portal by editing or cloning the Field Display Policy. See [Expose Device Pools and Class of Service in Quick Add Subscriber](#). 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: 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 make sure 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)
-

22.5.3. Quick Add Subscriber Class of Service

A Class of Service (CoS) allows the user to specify a Calling Search Space (CSS) for devices and lines, respectively. A CSS, in turn, is mandatory for lines and devices when adding a Subscriber using Quick Add Subscriber. A Calling Search Space can be referenced by:

- Site Defaults Doc (SDD)
- Reference Configuration Template (CFT) referenced in the Quick Add Subscriber Group (QAG)
- Admin Portal via the Class of Service field (if exposed)

Site Defaults Doc

The Calling Search Space values referenced in the SDD ensure that a Subscriber'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 QAG or via the Class of Service field in the Admin Portal drop-down (see below) the value defaults to the SDD.

Quick Add Subscriber Group (QAG)

The Calling Search Space values referenced by a Configuration Template (CFT) in the QAG 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 Subscriber Groups](#) for details.

Admin Portal

An Administrator can expose a Class of Service drop-down on the QAS page on the Admin Portal by editing or cloning the Field Display Policy. See [Expose Device Pools and Class of Service in Quick Add Subscriber](#). 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 is done to make sure 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)

22.5.4. Expose Device Pools and Class of Service in Quick Add Subscriber

Administrators with access to Field Display Policies (FDP) can expose the **Device Pools** field and **Class of Service (CoS)** field on the Quick Add Subscriber (QAS) interface at a specific hierarchy.

1. As an administrator with access to Field Display Policies (FDP), choose **Customizations > Field Display Policies**.
2. Filter the **Target Model Type** on **view/QuickSubscriber**.
3. Depending on which hierarchy or hierarchies the **Device Pools** or **Class of Service** field should be exposed in QAS:
 - a. If the FDP exists at the correct hierarchy, open it.
 - b. If the FDP does not exist at the required hierarchy, clone one of the available FDP's on a higher hierarchy to the required hierarchy (use **Actions > Clone**).
4. Open the FDP and go to the first group's **Available** list in the **Fields** block. Select **device_pool** or **class_of_service**.
5. Click on the **Select** button to move the **device_pool** or **class_of_service** label from the **Available** list to the **Selected** list.
6. Use the **Move up** and **Move down** buttons to move the label to the desired position relative the the other field labels.
7. Ensure that the cloned FDP name is "default", and click **Save**.

If an administrator is at the hierarchy where the cloned FDP is created or at a lower hierarchy, and then navigates to **Subscriber Management > Quick Add Subscriber**, a drop-down field with the title: **Device Pools** or **Class of Service** is exposed.

22.5.5. Configuration

To create or configure users, enable users with services, or associate users with devices, configure the following items on the system.

1. Server Configurations

Configure the following servers in VOSS Automate:

- Cisco Unified Communications Manager (Unified CM) Server - Adding a Unified CM server. This server is required to:
 - Sync manually provisioned users or LDAP-integrated users in Unified CM to VOSS Automate.
 - Sync any of these users' existing associated Phones, Directory Numbers, Extension Mobility Profiles in Unified CM to VOSS Automate.
 - Create Subscribers (push users to Unified CM)
 - Push users' associated Phones, Directory Numbers, Extension Mobility Profiles, to Unified CM.

- LDAP Server. This server is required if you want to configure LDAP-synced users in VOSS Automate. If you do not want to configure LDAP-synced users, this server is optional.
- Cisco Unity Connection Server. This server is only required if you want to add Cisco Unity Connection voicemail users that are configured in VOSS Automate.

2. Voicemail Service

Deploy Voicemail Service with a pilot number created and associated to a site under **Services > Voicemail** in VOSS Automate. This item is required to create a “Default CUC Subscriber Template” under **Site Defaults > CUC Defaults**. The template is required to create Cisco Unity Connection Voicemail users.

3. WebEx Service

Configure a WebxEx Server in VOSS Automate to deploy any WebEx users provisioned through QAS. Set a password for WebEx users in Site Defaults.

22.5.6. Quick Add Subscriber Conditions

For details to provision services to users, follow these instructions:

- [Provision the Voice Service](#)
- [Provision the Extension Mobility Service](#)
- [Provision the Voicemail Service](#)
- [Provisioning Subscribers with Webex App](#)
- [Provision the Pexip Conference Service](#)
- [Provision the Single Number Reach Service](#)
- [Provision the Jabber or Dual Mode Device Service](#)
- [Provision the Contact Center Agent](#)
- [Enable Self Provisioning](#)

When creating users with the Quick Add Subscriber function, consider these conditions:

- A check box called **Send welcome email** is displayed when you type in a user email address *only if* the following configuration has been made and is enabled:
 - An SMTP server has been set up ([Add a SMTP Server](#))
 - The **Allow email to be sent to user after Quick Add Subscriber** on **Email** tab of the **Global Settings** is set to **Yes** for the relevant hierarchy ([Global Settings](#))

A welcome email is then sent to the subscriber email address using the configured “Quick Add Subscriber” HTML email template that applies to the hierarchy ([Email](#))

- From the Quick Add Subscriber Group menu, create a custom group or use the default group.
- You can edit existing users on Cisco Unified Communications Manager (CUCM) through Quick Add Subscriber only if the users exist at the Site level.

A check box called **Include users at higher hierarchy** can be displayed by means of a custom Field Display Policy (field name: `lookUpForUser`, hidden by default), so that the **User** drop-down list will also show users above the current site hierarchy. This setting is also available for bulk load sheets and API calls.

- A check box called **Fail Transaction if user not found** can be displayed by means of a custom Field Display Policy (field name: `failIfNotFound`, hidden by default) to prevent adding users not on Cisco Unified Communications Manager. By default, the transaction will not fail. The option is used for the case where users have not been synced from LDAP to Cisco Unified Communications Manager. This setting is also available for bulk load sheets and API calls.
- LDAP synced or LDAP integrated at Cisco Unified Communications Manager user fields are always read-only and cannot be edited.
- You can associate a Line with multiple phones.
- You can associate a Phone with multiple Lines.
- If you choose to add a Phone for the user, the **Phone Name** drop-down list will show available phones at the user's site, according to the Phone Type as specified in the Site Defaults for the site.

The phones available from the drop-down list are those in the associated Quick Add Subscriber Group at the Customer level, which have synced from Unified CM, as well as the phones that are available at the specific site level.

You can also add a new phone if required by entering a valid name in the **Phone Name** field. The Phone Name must consist of a prefix, for instance SEP, followed by a MAC address, which is 12 hexadecimal characters. If you enter the Phone Name incorrectly, for example too few or too many characters, then subsequent associated transactions will fail.

- Associate an Entitlement Profile with the Subscriber.
- You can create multiple devices for a user. Therefore, the **Voice** check box is always visible. When the **Voice** check box is selected, four optional fields are exposed: **Phone Type**, **Phone Protocol**, **Phone Button Template**, and **Phone Security Profile**.
- Values set in the **Phone Type**, **Phone Protocol**, **Phone Button Template**, and **Phone Security Profile** fields will override any existing values in QAG or CFT, as well as the SDD or any other backend CFTs (CFTs that can not be edited).

If a specific phone type is not allowed in an entitlement profile, that phone type will not be displayed in the Phone Type drop-down list for a Subscriber associated to that entitlement profile.

If a field is blank, the existing values in QAG, CFT, SDD or other backend CFTs will be used.

If a Phone Template is not specified in QAG, or if the specified Phone Template has blank values for the phone fields, then the phone field values are pulled from the SDD.

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 Unified CM if the Unified CM allows it for that phone type.

Note: To reduce the likelihood of conflicting QAS settings when completing the optional fields mentioned above, we strongly recommend setting the required fields in the order as displayed on the Quick Add Subscriber screen:

1. Entitlement Profile
 2. Quick Add Group
 3. Voice (Phone Type, Phone Protocol, Phone Button Template and Phone Security Profile).
-

- You can set only one Extension Mobility profile for a user. Therefore, the **Extension Mobility** check box is not visible after you create an Extension Mobility profile.
- You can set only one WebEx account for a user.

- See [Contact Center Agent Quick Add](#).
- You can associate multiple Jabber and Dual Mode devices to a user.
- Jabber and Dual Mode devices get the first line assigned to them that is specified in the QAS form.
- You can create a Directory Number in Unified Communications Manager in two ways:
 - By creating a Voicemail Line in QAS.
 - By creating a Line in QAS.

When you create a Voicemail or Voicemail Line using Quick Add Subscriber, the Directory Number Used field is set to “true” under **Subscriber Management > Directory Number Inventory**.

- A Directory Number created without any device associations (for example, a Voicemail Line) is tagged under **Subscriber Management > Lines** as ‘DN created without device from QAS.’
- When the **Enable Self Provisioning** check box is selected, phone lines are added using the Universal Line Template (ULT) referenced in the Self Provisioning User Profile chosen from the **Self Provisioning User Profile** drop-down list which is exposed upon selecting the check box.

If a User is added with lines but no devices, then selecting the **Enable Self Provisioning** check box automatically sets the **CUCM User Primary Extension** to the QAS line pattern and ULT route partition. If a user is added with devices and lines, then selecting this check box also automatically sets the CUCM User Primary Extension to the QAS line pattern and ULT route partition.

Choose the required User Profile from the **Self Provisioning User Profile** drop-down list. The available User Profiles are those under **User Management > Self Provisioning > User Profile**. A User Profile must be selected when a user is enabled for Self Provisioning. A default User Profile (as shown under **Site Management > Site-Defaults**) is selected. Change this default if required.

Contact Center Agent Quick Add

Contact Center

The Quick Add Subscriber feature supports the easy creation of an UCCX agent.

The **Contact Center Agent** check box becomes visible if:

- the associated Entitlement Profile has Contact Center enabled
- a Contact Center Server is available at the hierarchy - [Configure Contact Center Express \(UCCX\) Server](#)
- the selected user is not already associated with an Agent

If the check box 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 Subscriber 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 Unified CM user associated with the Contact Center Agent.

Related Topics

- Introduction to Entitlement in the Core Feature Guide

22.6. Line Reports

22.6.1. 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
- 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.

22.6.2. 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:

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.

22.7. Customization Reports

22.7.1. Audit Template Customizations

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.

Procedure

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**.

What to Do Next

View the audit report. See “View Template Customization Audit Reports”.

22.7.2. View Template Customization Audit Reports

Procedure

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.

22.7.3. 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:

```
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.

22.8. Conferencing

22.8.1. Introduction to Conferencing

VOSS 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 input form that provides the interface to Conferencing users displays the minimum of Conferencing user properties that are mandatory. The Field Display Policies and Configuration Templates for this Conferencing input form can be modified according to the suggested customization procedure for Policies and Templates.

For Conference Workflows to function, make sure that the following is done at the Customer:

- A Conferencing server is added.
- The Conferencing server is added to a Network Device List (NDL).
- The required site references the relevant NDL.

WebEx Conferencing for Subscribers

If conferencing was added for a Subscriber user when the Subscriber was added, the WebExId is defaulted to the userid. Note that the WebEx user properties that are shown on the Subscriber form may not correspond with those shown on the Conferencing input form. If the Conferencing feature is to be added for an existing subscriber, make sure that the WebExId is the same as the userid.

22.8.2. Conference Workflows

User details can be added if a valid server is available.

When adding Conferencing from this input form, the mandatory fields are entered on the Conferencing server.

Conferencing details can also be added as part of Subscriber Management.

- For WebEx:

If the WebEx Id is a VOSS Automate 10.6(x) or later version, and Unified CM username of a Subscriber, the WebEx details are displayed on its Subscriber Management screen WebEx tab.

Modify Conferencing details on the selected item, or also add and delete details from the Subscriber Management form.

Deleting a Conference item will remove the details from the Conferencing tab of Subscriber Management if the user is a Subscriber.

22.8.3. Pexip Server

For an overview, see: [Pexip Conference Users](#).

1. Log in as provider or reseller administrator.
2. Choose **Apps Management > Pexip Conferencing > 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*

22.9. Webex App Users

22.9.1. Webex App

Overview

Webex App is a cloud-based business collaboration service that allows employees to message, meet, and call instantly in order to strengthen relationships and increase productivity.

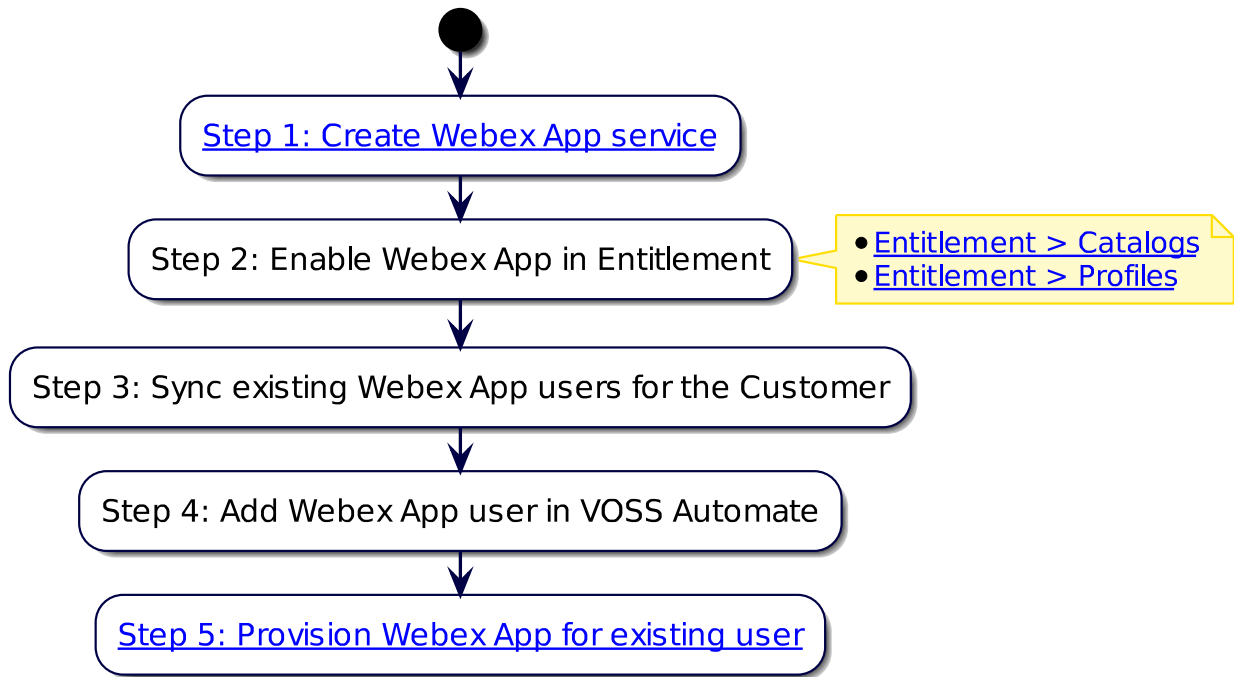
Webex App combines mobile devices and other communications tools to provide instant communications and live meetings to ensure a professional and effective collaboration experience.

The table describes the main Webex App features:

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 Webex App 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.

Note: Configure a specific Subscription for organizations with multiple License Subscriptions, in other words where there is a single organization with more than one entitlement for a specific license, such as “Messaging”.

Webex App Flowchart



Note: Only steps 1 and 2 are mandatory for Webex App to function in VOSS Automate. The other steps are dependent on your particular requirements.

The table describes the high-level Webex App workflow steps outlined in the flowchart above:

Steps	Description
1. Create Webex App service	
2. Enable Webex App in Entitlement	Select the Webex App checkbox (at the appropriate hierarchy level, in the entitlement catalog and entitlement profile): <ul style="list-style-type: none"> • Entitlement > Catalogs • Entitlement > Profiles
3. Sync existing Webex App users for the customer	Two methods for syncs: <ul style="list-style-type: none"> • On the Customer Access page, click Action > Sync Webex App Users • Run a sync by executing SyncSpark[Customer] (via Administration Tools > Data Sync).
4. Add a Webex App user in VOSS Automate	Two methods to add Webex users: <ul style="list-style-type: none"> • Via Subscriber Management > Subscribers • Via Subscriber Management > Quick Add Subscriber <p>To add a Webex App user using Quick Add Subscriber (QAS), choose the <i>Webex Teams User Template</i> to use for the user. This selection overrides the default user template referenced in the <i>Quick Add Subscriber Groups*</i> associated with the user.</p> <p>If a <i>Webex Teams User Template</i> is not selected from the dropdown, selection falls back to the <i>Webex Teams User Template</i> referenced in the associated <i>Quick Add Subscriber Groups</i>. If you want customized values, clone the <i>Webex Teams User Template</i> (via Customizations > Configuration Templates), and edit as required.</p>
5. Provision Webex App for an existing user	

Related Topics

- Webex App Server
 - [Webex Servers](#)
- Webex App Services:
 - [Create Webex App Service](#)
- Webex App Users:
 - [Generate Webex App User CSV Import File](#)
 - [Bulk Update Webex App Users](#)
 - [Webex App Licenses](#)
 - [Add a Subscriber \(Webex App tab\)](#)
- Webex App Workspaces:
 - [Webex App Workspaces](#)

– *Webex App Manual Steps*

Add a Webex App User

This procedure adds a new Webex App user in VOSS Automate.

1. Log in to the Admin Portal as a Provider, Reseller, Customer, or Site administrator.
2. Go to (default menus) **Subscriber Management > Webex App > Users**.
3. View existing Webex App users (synced, or added in VOSS Automate).
4. Click **Add**.
5. Choose the hierarchy where you want to add the Webex App user.
6. Fill out fields on the **Account Details** tab:
 - First Name and Last Name
 - (Mandatory). Email Address

Note: Email address is mandatory. It is used to match users when they're moved during an overbuild.

- **Login Enabled**

This read-only field displays only when a user is enabled for Webex App, and when selected, indicates that the user has activated their Webex App account (by accepting an email invitation to join Webex App).

- **Invite Pending**

This read-only field displays only once you've saved the form to add the user, which sends the invitation to join Webex App. The checkbox is selected if the user has not yet accepted their invitation.

- **Status**

A read-only field that displays only once the Webex App user exists (once you've saved the form), and indicates the user status, based on the Login Enabled and Invite Pending fields, for example, "The user has never logged in; a status cannot be determined".

- **Line**

Webex App services (other than Message only) must have a line specified that can be associated with a Jabber device for calling:

- New users must have an input line specified.
- Existing users must have either a primary extension, or an input line must be specified.

7. On the **Services** tab, select relevant services:

- **Message:** Webex App Messaging. Allows a user to exchange messages and share files with another person or a group of people.
- **Meeting:**
 - Webex App 25 Party Meetings. Allows a user to host up to 25-party meetings in Webex App cloud spaces.
 - Webex Enterprise Edition 200. Webex Enterprise Edition.

- Webex Collaboration Meeting Rooms. Allows users to come together for one meeting experience irrespective of the devices and software they're using, whether video conferencing services such as Webex, or other systems such as Polycom.
- **Hybrid Calendar Services:**
 - Microsoft Exchange/Office 365. Select for users who have mailboxes in on-premises Exchange or Office 365.
 - Google Calendar. Enable for users using Google Calendar.
- **Hybrid Call Services:**
 - Aware. Makes Webex App “aware” of all calls across your existing unified communications system. Hybrid Call Services Connect (see field below) is dependent on Hybrid Call Services Aware.
 - Connect. Deployed on top of Hybrid Call Services Aware (see above field) and amongst other things, connects Webex App with VOSS Automate so that they work together. Enabled = Remote Device created.

Note: With Hybrid Call Service Aware and Hybrid Call Service Connect together, users can make the same calls from either their desk phones or Webex App, and hear incoming calls ring both their desk phones and Webex App, and answer calls on either.

If the user has calling enabled, the **Services** tab displays Calling settings.

8. On the **Roles** tab, select relevant roles:

- No administrator privileges
- Full administrator privileges. Access to all of the portal's features, including: assign roles, company policy and templates, device management licenses and upgrades, etc.
- Read-only administrator privileges. Can view only whatever privileges are available to the full administrator.
- Support Administrator privileges. Access to user information and support logs.
- User and Device Administrator
- Device Administrator

9. Click **Save**. The Webex App user is added.

Delete a Webex App User

This procedure deletes an existing Webex App user (synced, or added via VOSS 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 (default menus) **Subscriber Management > Webex App Users**.
4. Choose the Webex users you wish to delete (one or more).
5. Click **Delete**.
6. Click **Yes** to confirm.

Provisioning Subscribers with Webex App

This section describes how to provision Webex App for a subscriber, either via the Subscriber list view, or via Quick Add Subscriber (QAS).

Related Topics

- [Add a Webex App User](#)
- [Webex App Quick Add](#)

Provision Webex App via Subscriber list view

This procedure provisions a subscriber with Webex App, via the Subscriber list view.

Prerequisite:

- The users entitlement profile must have Webex App enabled (**Webex App** checkbox must be selected).
- Unless WebexApp 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 [Add a Webex App User](#)

Perform these steps:

1. In the Admin Portal, go to (default menus) **Subscriber Management > Subscribers**.
2. From the Subscribers list, click on a subscriber you wish to provision with Webex App.
3. On the subscriber configuration screen, select the **Webex App** tab.
4. In the **Webex App User** field, click the Plus icon (+) to display the **Webex App User configuration** fields.

Note: The following checkboxes are read-only, indicating the user's status (whether their Webex account is active): **Login Enabled, Invite Pending**

Options in the **Services** and **Roles** sections depend on the Webex App Server to which the Webex App Service is synced.

5. In the **Services** section, select the required check boxes:

Message	Webex App Messaging. Allows a user to exchange messages and share files with another person or a group of people.
Meeting	<ul style="list-style-type: none"> • Webex App 25 Party Meetings. Allows a user to host up to 25-party meetings in Webex App cloud spaces. • Webex Enterprise Edition 200. Webex Enterprise Edition. • Webex Collaboration Meeting Rooms. Allows users to come together for one meeting experience irrespective of the devices and software they use, whether video conferencing services like Webex, or other systems, such as Polycom.
Hybrid Calendar Services	<ul style="list-style-type: none"> • Microsoft Exchange/Office 365. Enable for users who have mailboxes in on-premises Exchange or Office 365. • Google Calendar. Enable for users using Google Calendar.
Hybrid Call Services	<ul style="list-style-type: none"> • Aware. Makes Webex App aware of all calls across your existing UC system. Hybrid Call Services Connect depends on Hybrid Call Services Aware. • Connect. Deployed on top of Hybrid Call Services Aware and amongst other things, connects Webex App with VOSS Automate so that they work together. Enabled = Remote Device created. Note that with Hybrid Call Service Aware and Hybrid Call Service Connect together, users can make the same calls from either their desk phones or the Webex App app as well as hear incoming calls ring both their desk phones and the Webex App app and answer the call on either.

6. In the **Roles** section, select the relevant checkboxes to configure the required roles:

No administrator privileges	.
Full administrator privileges	Access to all of Portal features, including: <ul style="list-style-type: none"> • 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	.

7. Click **OK**. Webex App is provisioned for the subscriber.

To verify that Webex App is enabled for the subscriber, ensure the **Webex App** column in the Subscribers list view displays the text, *Enabled*.

Provision Webex App via Quick Add Subscriber

This procedure enables Webex App for a subscriber via Quick Add Subscriber (QAS).

Prerequisite:

- The user's entitlement profile must have Webex App enabled (**Webex App** checkbox must be selected).
- Unless WebexApp 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 [Add a Webex App User](#) and [Webex App Quick Add](#)

Perform these steps:

1. Go to (default menus) **Subscriber Management > Quick Add Subscriber**.
2. From the **Username** drop-down list, choose the name of the subscriber to be provisioned with Webex App.
3. Select the **Webex App** checkbox to enable Webex App for the subscriber.
4. From the **Webex Teams User Template** drop-down list, choose the template you want to assign to the user.
5. Click **Save**. Webex App is provisioned for the subscriber.

To verify that Webex App is enabled for the subscriber, ensure the **Webex App** column in the Subscribers list view displays the text, *Enabled*.

22.9.2. Generate Webex App User CSV Import File

Provided the following setting is enabled in the Global Settings, when a Webex App user is added or updated, a CSV file is created and attached to an email message, and sent to specified recipients via the Webex App message service: **Generate and send Webex App User CSV file via Webex App message**

The CSV file can be imported into Webex App Control Hub to update the users.

Formatted example of CSV file:

User ID/Email (Required)	Jabber with Webex Teams	Jabber Calling	UC Manager Profile	Contact Migration Required	Calling Behavior	Cal
mvs_user20@aaaglobal.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	
testext1@test.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	
adent@marclight.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	
lwilson01@aaaglobal.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	
kevin.green@marclight.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	
jmeyers01@aaaglobal.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	
email.bumar@marclight.com	FALSE	FALSE		FALSE	USE_ORG_SETTINGS	

Note: This task can also be carried out in bulk.

Generate and Send Webex App User CSV file

Prerequisite:

- Enable the following setting in Global Settings: **Generate and send Webex App User CSV file via Webex App message**

Perform these steps:

1. In the Admin Portal, go to (default menus) **Subscriber Management > Webex App > Generate User CSV Import File**.
2. Choose the relevant hierarchy (the hierarchy of your Webex App users).
3. Fill out a **Recipient Email Address**
4. Click **Save**

An email message with a CSV attachment is sent. The CSV file contains the data of all the Webex App users.

See: [Global Settings](#) for an email message example.

22.9.3. Bulk Update Webex App Users

This procedure generates CSV files to perform bulk actions on import into Webex App Control Hub.

1. In the Admin Portal, go to (default menus) **Subscriber Management > Webex App > 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. Choose whether to generate a combined CSV file for the hierarchy or individual files for each user, or both (generates multiple files).
6. Fill out the **CSV Recipient Email Address**. This defaults to the VOSS Automate administrator email address.
7. If necessary, you can select more users (move users from the **Available** field to the **Selected** field. Else move all users.
8. Click **Save**. The message is sent with the CSV file attachment.

22.9.4. Webex App Workspaces

Overview

You can define Webex App workspaces of various types in VOSS Automate. For example, meeting rooms or open spaces.

When adding or updating a workspace, the details you add to the Workspaces page in the Admin Portal is formatted as a sequence of manual steps, in an email message. The manual steps are to be performed in the Webex App Control Hub.

See: [Global Settings](#) for an email message example.

The content of the manual steps for a workspace configuration display in the **Steps** content via the (default menus) **Subscriber Management > Webex App > Manual Steps**.

Add a Webex App Workspace

This procedure adds a Webex App workspace.

1. In the Admin Portal, go to (default menus) **Subscriber Management > Webex App > Workspaces**.
2. Choose the relevant hierarchy.
3. Provide a workspace name, and capacity, and from the **Type** field, choose the workspace type.
4. In the **Send Device Activation Code To** field, fill out the email address(es) where the device type code is sent.

Note: This code is unique to this created 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**.

A VOSS Automate schedule checks the expiration date and generates a new code. The **SIP Address** of the workspace is also shown.

5. In the **Calling** section, choose the calling behavior (free or hybrid).

Note: The hybrid calling option displays additional fields where you need to choose a site and an available directory number, which then generates a mail ID is generated from CUCM. The auto-generated value in the **Mail ID from Unified CM** field uses the following:

wt_ + <random-number> + the email hostname set up for the Webex App service

For example, wt_886821663180@myhost.com.

A subscriber user for the device is then added at the selected site, with the following:

- **User Id** and **Last Name**: wt_886821663180
- **First Name**: workspace **Name**
- **Primary Extension**: **Directory Number**
- **Phone**: Spark Remote device with workspace specific settings

Once the device code is entered, the page displays details of the device associated with the workspace in the **Devices** group, for example: **Product**, **Connection Status** and **IP Address**. A link to the device is then also available, to show details (read only) as listed under the **Devices** menu for Webex App.

The new workspace is listed on the **Workspaces** list view.

22.9.5. Webex App Manual Steps

When workspaces are created or updated in VOSS Automate from the **Workspaces** menu, the data entered on this input form 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 App Workspaces](#)
- [Global Settings](#) for an email message example.
- [Webex App](#)

22.9.6. Webex App Licenses

Webex App license usage counts aren't automatically updated in VOSS Automate after licenses are assigned (that is, after assigning a subscriber with Webex App services). For this reason, it is recommended that you create a schedule to periodically sync Webex App user licenses.

Webex App License Syncs

Webex App user license syncs may be actioned 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.
Business Admin Portal	On the Webex App Quick Actions card at the customer hierarchy, select Sync Licenses .

Important: Webex App Licenses need to be synced after upgrading to release 21.1:

1. Execute the Data Sync named 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: [Create Webex App Service](#).
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: [Create Webex App Service](#).

Only licenses synced and managed by VOSS 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.

View Webex App Licenses

This procedure provides a condensed view of the Webex App licenses consumed and available at the selected hierarchy level.

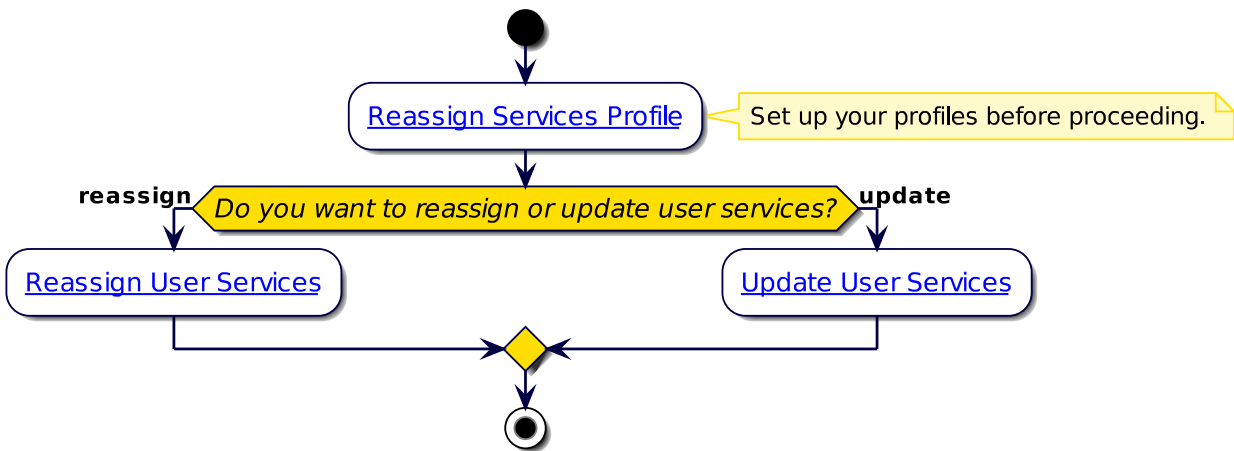
1. Go to (default menus) **Subscriber Management > Webex App > Licenses**.
2. View Webex App license details in the License list view:
 - Name (of the license)
 - Total Units (total number of licenses available)
 - Consumed Units (the number of licenses still available)
 - Location (where the licenses are available and used)

22.10. Reassign Services

22.10.1. Introduction to Reassign Services

Reassign Services simplifies and automates the transfer of existing Subscriber services from a Source User to a Target User.

Reassign Services high level workflow



This utility is for example useful when an employee left the company and a new employee now starts the same role. Therefore, instead removing the old subscriber and configuring a new subscriber with the same settings and standards, the services and settings can be moved from the old subscriber to the new subscriber.

These services can include:

- Phone(s), which can be dual-mode with associated Remote Destination and/or Mobile Identity
- Device Profile(s)
- Remote Destination Profile(s) with associated Remote Destinations
- Voicemail User with related services including Alternate Extension and Message Handler (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 subscribers. 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.

An option is also available 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:

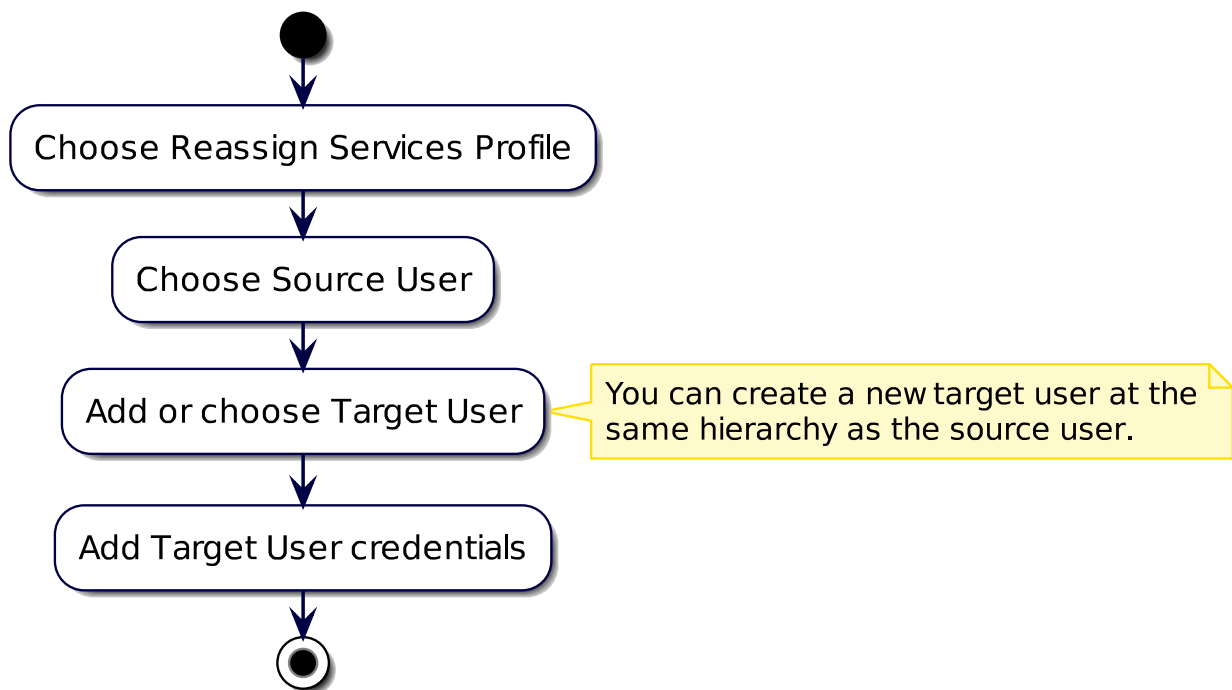
- Change User Details (modified Reassign Services) that updates the services of an existing subscriber using custom templates referenced in a Reassign Services Profile.

Related Topics

- [Reassign Services](#)
- [Update User Details](#)
- [Reassign Services Profile](#)

22.10.2. Reassign Services

The Reassign Service feature directs you to the Customer hierarchy (if you are not already there) because it supports target users that are on a different site as the source user.



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 subscriber to be reassigned. This provides a list of usernames of Subscribers in the system. It will list local or CUCM-LDAP Synced Subscribers only (not VOSS-LDAP Synced). Once a subscriber 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 subscriber 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.

Note: It is not possible to reassign services to a user who is on a different Unified CM Cluster than the source user. The target user dropdown 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.

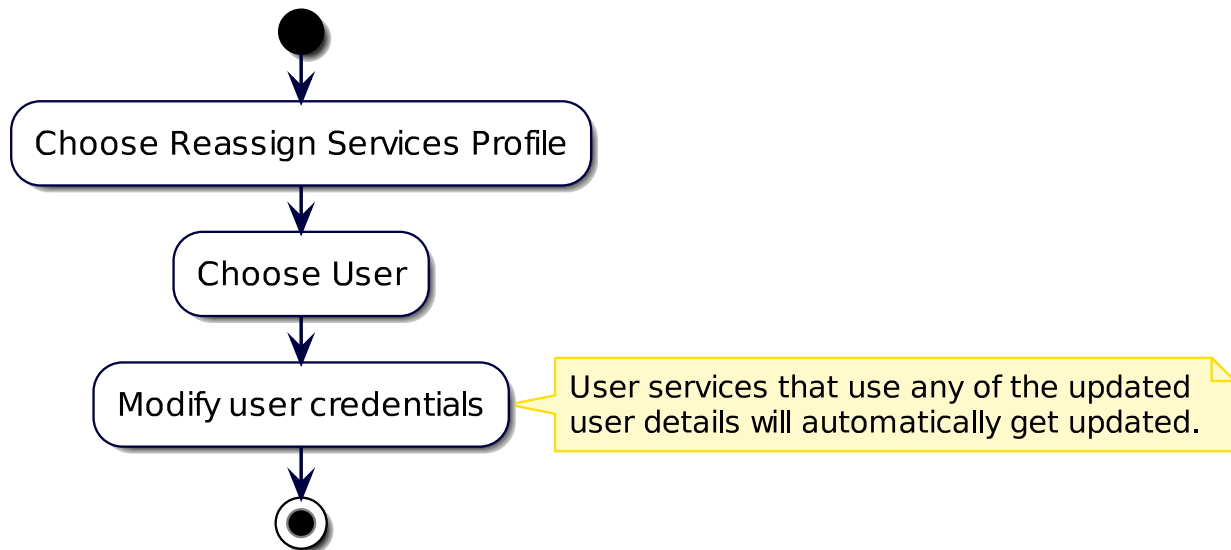
22.10.3. Update User Details

The **Update User Details** menu shows 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 shows which services will be updated.

Reassign User Services (Update user services workflow)

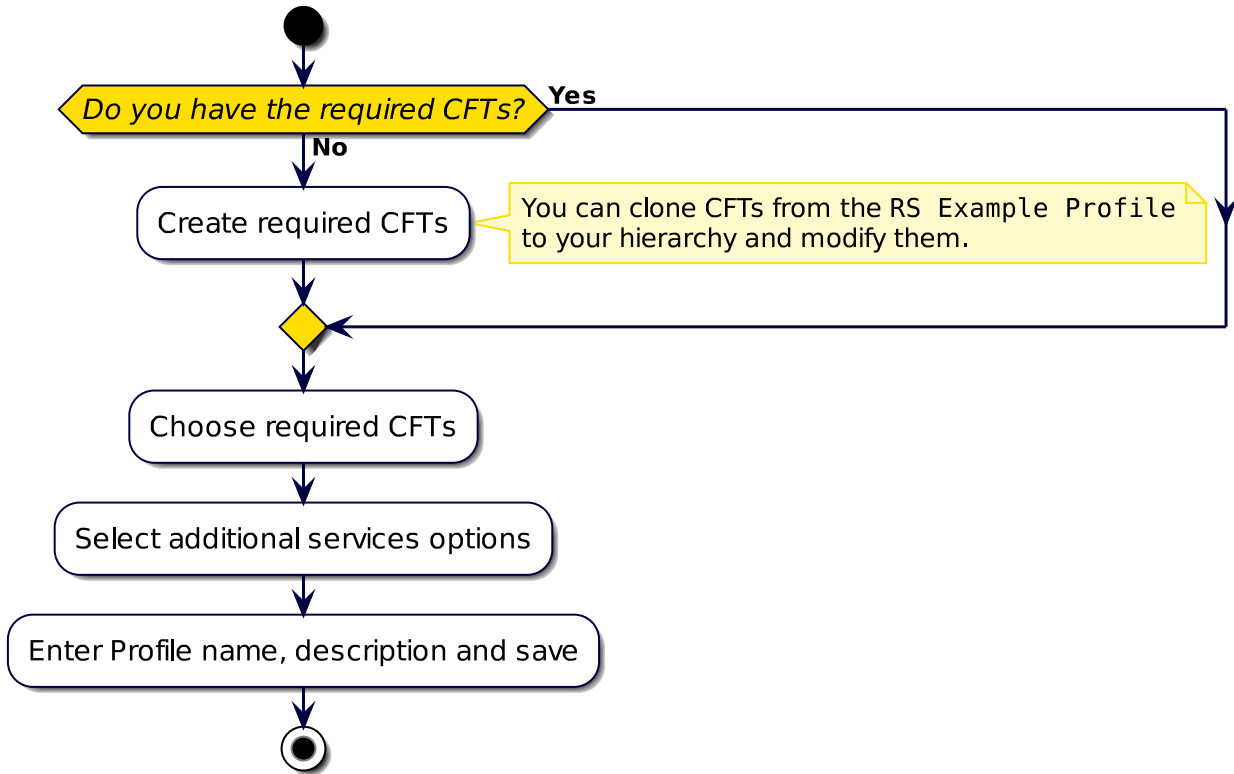


22.10.4. Reassign Services Profile

The **Reassign Services Profile** page allows for a set of configuration settings and additional settings to apply when the Reassign Services functionality is used.

Reassign services profile workflow

The flowchart describes the configuration settings to apply. If no CFT is defined for a service, it is still moved to the new user. However, existing settings will be left in place.



Configuration templates and profiles

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 is essentially to 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.

There is a set of example CFTs in the system by default - prefixed RS - that provides some examples of common settings and logic that might be used.

This profile and templates for configuration settings can be maintained per hierarchy as needed. The context for the reassign services feature is fairly similar to Quick Add Subscriber and this is to allow the reuse 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 created in order to use the feature.

Reassign Services Profile field reference

To access this page, to to (default menus) **Subscriber Management > Reassign User Services > Reassign Services Profile**, then choose an existing profile to view settings, or 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 subscriber will be left when the feature completes however no services will be enabled.
User CFT	This CFT defines VOSS 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.

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 Subscriber 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**

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 CUCAAlternateExtension 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: **RelayAddress**

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.

23. Services

23.1. Webex App

23.1.1. Create Webex App Service

This procedure adds a Webex App service.

Prerequisites:

To allow VOSS Automate to connect to the Webex App Cloud API, obtain the following from the Cisco Webex page:

- a Webex App Organization Account Number
- an Access and Refresh token

Perform these steps:

1. Log in to the Admin GUI as a provider or reseller administrator.
2. Select the hierarchy path to the correct customer node.
3. Select **Services > Webex App > Access Token** to display **Webex App Account**.
The form opens on a separate tab, at the following URL: `https://us-central1-webex-teams-auth-token.cloudfunctions.net/webex_teams_oauth`
4. Click the **GET TOKENS** link.
5. In the **Email address** field on the **Cisco Webex** page, enter a valid email address; then, click **Next**.
An email address and password are only required the first time you log in to the Cisco Webex site.
6. In the **Password** field on the **Cisco Webex** page, enter a valid password; then, click **Sign In**.
7. View the codes/tokens generated and displayed on the form:
 - **Organization ID**
 - **Access Token** (14 days)
 - **Refresh Access Token** (90 days)

Note:

- VOSS Automate automatically refreshes the access tokens every 7 days. To manually refresh the access tokens, click **GET TOKENS** on the **Webex App Account** form or **Action > Refresh Access Token** on the **Customer Access** form.

- The Refresh Token is valid for 90 days. The number of valid days remaining for the access token is displayed in the **Refresh Token Expires in** counter on the **Webex App Access Token Management for VOSS4UC** page.
- See <https://developer.webex.com/docs/integrations> for more details on access token management.

- Click on each **Copy** button in turn to copy the item, return to the VOSS Automate tab, and paste in the appropriate field on the **Customer Access** form. Note that the access tokens must also be pasted into the 'Repeat' fields.
- Fill out, at minimum, the other mandatory fields on the **Customer Access** form under **Account Details**:

Field	Description
Webex App Customer Name	Populated automatically, using the customer name.
Default Calling Behavior	Can be applied to synced in users, if also set in Global Settings (Automatically apply default calling behavior on Webex App user data sync)
Use Organization's Domain	Can be enabled if you select option Calling in Webex Teams (Unified CM) (same as Webex App Control Hub behavior) When selected, you may also enable Default UC Manager Profile
Email Domain for Hybrid Calling in Workspaces	When hybrid calling is enabled for a workspace, a dummy subscriber email domain can be added.
Subscription ID	Fill out the subscription ID (as seen on the Control Hub portal) to selectively manage multiple subscriptions in multiple sites. If required, fill out the newly managed subscription ID here.
Site URL	The site URL for Webex Enterprise Edition meeting services. When syncing licenses and subscriptions, VOSS Automate only syncs in subscriptions matching the ID and services from the site.
Enterprise Content Management Enabled and Jabber Team Messaging Mode Enabled	These settings match the configuration setting on the user user feature of the Webex App Control Hub, and apply to the corresponding Default Calling Behavior selection: Calling in Webex App (Unified CM) and Cisco Jabber app. Note that with these calling behavior options, Quick Add Group Templates for Jabber devices under the Webex App group are applied.
UC Manager Profiles	Added for use when managing users.
HTTP Proxy String	Required only if a proxy server is required to connect to the Webex App cloud, for example: <code>http://[ip address]:port</code>
HTTPS Proxy String	Required only if a proxy server is required to connect to the Webex App cloud, for example: <code>https://[ip address]:port</code>

- Click **Save**. The Webex App Service is added.
- Sync the Webex App Users for the customer. To do this, click **Action > Sync Webex App Users** on the **Customer Access** form.

Note: Webex App Users can also be synced from **Administration Tools > Data Sync**, and then running the SyncSpark[Customer] data.

Related Topics

- [Quick Add Subscriber Groups Default Model](#)
- [Webex App Licenses](#)

Workflow Animation

The animation demonstrates how to create a Webex App service.

23.2. Auto Attendant (Call Handler)

23.2.1. Auto-Attendant Call Handler

Overview

An Auto-Attendant Call Handler transfers telephone 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 Unified Communications Manager (CUCM).

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 VOSS Automate:

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

- [Add, Update, or Delete a Call Handler in the Core Feature Guide](#)
- [Manage Greeting Files in the Core Feature Guide](#)
- [Call Handler \(Auto Attendant\) Schedule in the Core Feature Guide](#)
- [Create a Call Handler \(Auto Attendant\) Schedule in the Core Feature Guide](#)
- [Modify a Call Handler \(Auto Attendant\) Schedule in the Core Feature Guide](#)
- [Add a Language Filter in the Core Feature Guide](#)
- [Add a TimeZone Filter in the Core Feature Guide](#)

- *Number Status and Usage*

Call Handlers and Shared Numbers

VOSS 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

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 that already has a Call Handler*
- *Add a Call Handler to a number that already has devices*
- *Remove Call Handler from a number that was shared between Call Handler and devices*
- *Remove devices from a number that was 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 *Add, Update, or Delete a Call Handler (Auto Attendant)*

Internal Number	Status	Usage	E164Number	Release Date	Tag
2126693916	Used-Utility	Call_Handler_Pilot, Device			

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:

Status	Usage
Used	Device

Add devices to a number that already has a Call Handler

In this scenario, Call Handler is added first and is assigned to a number. Then you can add additional devices (e.g. deskphone, BOT, EM, SNR) with the same number.

Scenario	Before adding devices	After adding devices
Add devices to a number already assigned to Call Handler	<ul style="list-style-type: none"> • Status: "Used-Utility" • Usage: <ul style="list-style-type: none"> – "Call_Handler_Pilot", or – "Call_Handler_Pilot, Device" 	<ul style="list-style-type: none"> • Status: "Used" • Usage: "Call_Handler_Pilot, Device"

Add a Call Handler to a number that already has 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.	<ul style="list-style-type: none"> • Status: "Used" • Usage: "Device" 	<ul style="list-style-type: none"> • Status: "Used-Utility" • Usage: "Call_Handler_Pilot, Device"

Remove Call Handler from a number that was 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.

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.	<ul style="list-style-type: none"> Status: "Used" Usage: "Call_Handler_Pilot,Device" 	<ul style="list-style-type: none"> Status: "Used" Usage: "De-"
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.	<ul style="list-style-type: none"> Status: "Used-Utility" Usage: "Call_Handler_Pilot,Device" 	<ul style="list-style-type: none"> Status: "Used" Usage: "De-"

Remove devices from a number that was 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).	<ul style="list-style-type: none"> Status: "Used" Usage: "Call_Handler_Pilot,Device" 	<ul style="list-style-type: none"> 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).	<ul style="list-style-type: none"> Status: "Used" Usage: "Call_Handler_Pilot,Device" 	<ul style="list-style-type: none"> Status: "Used" Usage: "Call_Handler_Pilot,Device"

23.2.2. Add, Update, or Delete a Call Handler (Auto Attendant)

This procedure adds, modifies, or deletes an Auto-Attendant Call Handler to VOSS Automate and to Cisco Unity Connection (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 **Customizations > Configuration Templates**) 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 Cisco Unity Connection (CUC) Auto-Attendant Call Handler template must have been synced from CUC.

To add a Call Handler:

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 (default menus) **Services > Auto Attendant > Call Handler**.
4. Click **Add**.

The **Call Handler/New Record** page opens at the **Call Handler Basics** tab. All other tabs on this page remain read-only until you configure the initial settings on this tab.

Once you've saved the new call handler, you can edit these settings. See [Update a Call Handler](#)

5. Mandatory. At **Network Device List**, choose the required network device list (NDL).

Note: This field is auto-populated and read-only if you're adding the call handler at site level.

6. Mandatory. At **Name**, enter a name for the new Call Handler.
7. At **Call Handler Template**, choose the CUC Call Handler template.

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.

8. Optional. At **Pilot**, choose a directory number to associate with the Call Handler.

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 VOSS Automate allows sharing of numbers between Call Handler and multiple device types. See [Auto-Attendant Call Handler](#)

9. 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) optional.

- When disabled (default), choosing a route list (route pattern) is mandatory.

This setting is relevant when adding or updating a Call Handler.

10. At **Route List**, choose a CUCM route list for the new Call Handler. Optional when **Do not add Route Pattern** is enabled.
-

Note: The NDL determines the route lists available in this drop-down. If the NDL is updated, route list options are updated.

11. Click **Save**.

Adding a Call Handler through VOSS Automate also adds a route pattern on the Cisco Unified Communication Manager (CUCM, or CallManager) 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 Cisco Unity Connection (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 (default menu) **Services > Auto Attendant > Call Handler**.
4. In the list view, click the relevant Call Handler to open the **Call Handler** page.
5. On the **Call Handler** page, update settings on the following tabs, as required:

Tab	Description
Call Handler Basics tab	<p>Only this tab is enabled when adding a Call Handler. All tabs are available when updating a Call Handler.</p> <ul style="list-style-type: none"> • 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). <ul style="list-style-type: none"> – 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	<p>Enables/disables transfer rules.</p> <ul style="list-style-type: none"> • 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 <i>Release to Switch</i> or <i>Supervise Transfer</i>)
Caller Input tab	<p>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.</p>
Greetings tab	<p>Configures greeting settings.</p>
Record/Playback tab	<p>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</p> <ul style="list-style-type: none"> • 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 Action > Record Greeting, or to Action > Playback Greeting (as applicable) to record or playback the greeting you wish to use.
Upload Greeting tab	<p>At Greeting File, choose the greeting file (.wav) to upload to the Call Handler. Then configure the specific greeting (if required).</p>

6. Click **Save**.

Changes are saved to the Call Handler in VOSS Automate and in Cisco Unity Connection (CUC).

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 [Auto-Attendant Call Handler](#) to understand how the status and usage description of the number may change when you delete the Call Handler.

Call Handler Page

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

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 GUI rules) 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.
Call Handler Template	cuc_template	Select the Unity Template for Call Handler.

Note: If the pilot number is shared between the Call Handler and one or more additional device types, see

Auto-Attendant Call Handler to understand the status of numbers available to assign to the Call Handler.

Transfer Rules Tab

Title	Field Name	Description
Message	callerInput_tab_message	Caller Input
Callhandler Menu Entry	CallhandlerMenuEntry.[n]	
Object Id	ObjectId	The primary key for this table. A globally unique, system-generated identifier for a MenuEntry object.
Call Handler *	CallHandlerObjectId	The unique identifier of the CallHandler object to which this menu entry belongs.
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 Object Id	TargetHandlerObjectId	The unique identifier of the specific object to send along to the target conversation.

Caller Input Tab

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:

Title	Field Name	Description
Message	callerInput_tab_message	
Callhandler Menu Entry	CallhandlerMenuEntry.[n]	
Object Id	ObjectId	The primary key for this table. A globally unique, system-generated identifier for a MenuEntry object.
Call Handler *	CallHandlerObjectId	The unique identifier of the Call Handler object to which this menu entry belongs.
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 Object Id	TargetHandlerObjectId	The unique identifier of the specific object to send along to the target conversation.

Greetings Tab

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.

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 HandlerObjectld	The unique identifier of the specific object to send along to the target conversation.
Call Handler Object Id	CallHandlerObjectld	The unique identifier of the Call Handler object to which this greeting rule belongs.
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

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	RecordPlayback.call_handler	Call Handler Name.
Extension	RecordPlayback.extension	Extension to Record message on.
Specific Greeting	RecordPlayback.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

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.

Related Topics

- See “System Call Handlers” in the “Cisco Unity Connection System Administration Guide for more information about Call Handlers.
- Call Handler (Auto Attendant) in the Core Feature Guide
- Manage Greeting Files in the Core Feature Guide

23.2.3. Call Handler (Auto Attendant) Schedule

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, VOSS Automate imports two predefined schedules from Cisco Unity Connection. These are accessed via **Services > Auto Attendant > Schedule**:

- **All Hours**
- **Weekdays**

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.

Designating 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.

See also:

- [Create a Call Handler \(Auto Attendant\) Schedule](#)
- [Modify a Call Handler \(Auto Attendant\) Schedule](#)

23.2.4. Create a Call Handler (Auto Attendant) Schedule

You may want to create a new schedule for your organization.

On the **Schedule** form (modify or add), take note of the following field:

Uses Holiday Schedule - If you want your schedule to recognise 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** check box.
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.
 2. Clone it (**Action > Clone**) to the desired hierarchy level.
 3. Edit as required.
 4. Click **Save**.
-

23.2.5. Modify a Call Handler (Auto Attendant) Schedule

To edit a Call Handler schedule:

1. From the **Schedule** list view, click on the schedule that you want to edit.
2. Select the **Schedule Details** link name and edit the required fields (as described under [Create a Call Handler \(Auto Attendant\) Schedule](#)).
3. Click **Save** when complete.

To delete a Call Handler schedule:

1. From the **Schedule** list view, select the check box next to the schedule you want to delete. If you want to delete more than one schedule, select multiple check boxes.
2. Click **Delete** on the button bar.
3. Click **Yes** on the dialog box to delete.

23.2.6. Manage Greeting Files

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 [Cisco Unity Connection \(CUC\) Servers](#).

1. Click **Auto Attendant > Manage 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](#).

23.3. Cisco Unity Connection (CUC) Localization

23.3.1. Cisco Unity Connection Localization

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 Subscriber), to set this information on a per-site level.

Timezones and languages in VOSS Automate are populated with the required 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 VOSS Automate that match the installed timezones and languages on the associated CUC Server. The names entered must uniquely describe the timezone and code.

See also:

- [Add a TimeZone Filter](#)
- [Add a Language Filter](#)

23.3.2. Add a TimeZone Filter

To add a custom Cisco Unity Connection timezone filter:

1. Log in as provider administrator or higher.
2. Choose **Services > Cisco Unity Connection Localization > TimeZone Filters** to see a list of timezone filters currently in VOSS Automate.
3. Click **Add**.
4. Enter the following:
 - a. **TimeZone Code** - this is a mandatory field, and must match a timezone code installed on the associated Cisco Unity Connection Server.
 - b. **TimeZone Name** - this is a mandatory field, and must be a unique description for the timezone code above.
5. Click **Save**.

23.3.3. Add a Language Filter

To add a custom Cisco Unity Connection language filter:

1. Log in as provider administrator or higher.
2. Choose **Services > Cisco Unity Connection Localization > Language Filters** to see a list of language filters currently in VOSS Automate.
3. Click **Add**.
4. Enter the following:
 - a. **Installed Language Code** - this is a mandatory field, and must match a language code installed on the associated Cisco Unity Connection Server.
 - b. **Language Name** - this is a mandatory field, and must be a unique description for the language code above.
5. Click **Save**.

24. Overbuild

24.1. Overbuild Introduction

24.1.1. Overbuild Overview

Important: It is recommended that VOSS Automate training and/or VOSS Services are engaged during the initial use of the feature to help ensure optimized processes and guidance.

Note: References to HCM-F and Shared Data Repository (SDR) are only relevant if installed.

The Overbuild feature enables Provider and Reseller Administrators to integrate an existing, deployed Unified Communications (UC) system into VOSS Automate without reprovisioning, unless required. This option is available for single-cluster dedicated deployments only. Overbuild provides tools to help the administrator manage the data synced from existing configurations in Cisco Unified Communications Manager and Cisco Unity Connection.

Although a deployed Unified CM system does not contain such VOSS Automate components as a hierarchy or a subscriber, the relationship between Unified CM components makes it possible to, for example, create a VOSS Automate subscriber 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** menu interface.

The Overbuild logic can be summarized as follows:

- **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
- **Users** - If the user has an associated phone then the user is moved to the same site as the phone.

If the user does not have an associated phone then the user must be manually moved to the relevant site using the Move Users menu option under either **User Management** or **Overbuild**.

It is recommended this happens prior to the Overbuild process so that all their related services are moved during overbuild; otherwise the Overbuild will need to be run again after moving the user to handle their related services.

- **Device Profiles** - this will move the device profile to the same site as the user associated to the device profile.

- **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.
- **Remote Destinations** - this will move the RD to the same site as the associated RDP
- **Lines** - this will move the line to the same site as the phone/device profile/RDP it is associated to.
- **CUC 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 VOSS Automate to the same site as the base user (if it finds a matching email address).
- **Contact Center Agents** - this will move contact center agents to the same site as the base user (if it finds a matching Unified CM user ID).

The Overbuild process involves five broad steps:

- Perform initial manual setup and configuration on VOSS Automate.
 - The business information of the existing, deployed system is identified and entered into VOSS Automate, optionally by the bulk load process. This means hierarchy information is created with customers, sites and site codes. Some configuration data is initially generated, for example Site Defaults data. This data should be modified if required according to Unified CM data, so that Overbuild processing can move data to required sites.

For example, the default, generated VOSS Automate Site Defaults for a site have the Site name as the Device Pool name. Since the Site Defaults are used in the Overbuild process, this name should be modified to match the Device Pool name on the imported Phones before the Overbuild process is run. VOSS Automate allows Provider and Reseller Administrators to modify Site Defaults in order to modify the configuration of an Overbuild process.

Note:

While Customers and Sites have access to the Site Defaults under the **Site Management** menu, the **Overbuild Defaults** tab is only visible to Provider and Reseller Administrators.

- Network device connections are identified, created, associated with a Network Device List, and imported. This includes Unified CM and CUCX clusters.

Caution:

Whenever this data is synced in, it becomes managed by VOSS Automate and, as a result, would be deleted by any hierarchy delete. See [Delete Issues and Purges](#) for information on managing these issues.

One Unified CM 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 Network Device List on VOSS Automate that is mapped to a created hierarchy.

- If the **Users** check box is selected on the **Run Overbuild** tool, users exposed under the **User Management** menu are moved to the site of their associated phones as specified in the Site Defaults Doc Device Pools.

Users without phones will not be moved and can be moved separately - see [Move Users](#).

The following model instances are moved from customer level to the site level:

- data/User
- data/HCSHcmfUserDAT
- device/cucm/User
- device/hcmf/User (only if HCM-F is installed)

- If the **Lines** check box is selected on the **Run Overbuild** tool, 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** check box is selected on the Site Defaults Doc **Overbuild Defaults** tab.
- 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.

Note:

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.

The 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.

- Manually validate and modify the overbuild run by reviewing the moved items using **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.
- Perform post-move operations:
 - Perform Self Care authentication provisioning steps for non-LDAP, LDAP, and SSO-enabled scenarios - see [User Authentication](#).

24.1.2. Overbuild Steps

Important: System Integrator Support Recommended - For all Managed Services: Day 2 Overbuild Projects, we recommend support from a System Integrator.

Provider and Reseller Administrators can follow these general steps to use the Overbuild tool:

1. Provision the business hierarchy. This can be done manually in VOSS Automate or by bulk load (see "Bulk Administration" topics and [Bulk Loading a File](#)).
2. Provision Cisco UC Applications, network device lists, and network device list references. Once UC Applications are configured, the sync from Cisco Unified Communications Manager will be scheduled and executed. See "Data Sync" topics.
3. Choose the device pool and devices for the site on both the **Site Defaults > General** and **Overbuild Defaults** tabs. See [Overbuild Site Defaults: Overview](#).
4. Choose **Run Overbuild** to move the imported UC Applications data into the site hierarchy that corresponds with the existing deployed site. See [Run Overbuild: Overview](#).
 - Users exposed under the **User Management** menu are moved to their associated phones if the **Users** check box is selected on the **Run Overbuild** tool.

Users are moved to their phones if the phones have the user set as the OwnerUserID, if the **Users** check box is selected on the **Run Overbuild** tool.

Note: The User's role is not changed when moving to Site.
 - Lines are moved and marked as in use in the Directory Number (DN) inventory if the **Lines** check box is selected on the **Run Overbuild** tool. A Site DN inventory is created.

If the DN instance already exists, it is updated as in use. The DN inventory instance is created at the site level by default. This can be set to Customer in the SiteDefaultDoc before running OverBuild.

Note: Adding Directory Number inventory at Customer level is only possible if the DialPlan in use is non SLC(Site Location) Based, or if no DialPlan is in use.

5. Choose **Overview Tool** to verify the number of Unified Communications elements at the selected hierarchy and below. See [Summary of the Overview Tool](#).
6. Optionally, review the device model types listed with hierarchy in the Device Models or **Subscriber Management** menu. See [Device Models: Overview](#).

24.2. Moving Model Instances

24.2.1. Moving Model Instances: Overview

If the Move operation is enabled for a model, instances can be moved from its current hierarchy level to another level. Data models, Device models and Relations can be enabled for the Move operation. For lists of objects moved during a move operation, see [Objects Moved During the Overbuild](#) for data and device models, and [Subscriber Management Models](#) for Subscriber 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).

24.2.2. 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, 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.

24.2.3. Subscriber Management Models

Administrators have privileges to manually move these Subscriber Management Menu models:

- Lines
- Voicemail
- WebEx
- Webex App
- Hunt Groups
- Call Pickup Groups

It is recommended to use the dedicated tools to move subscribers and phones between customer and site hierarchy levels.

24.2.4. Move Subscriber Management List View Items

Perform these steps:

1. Log in as a Customer Administrator or higher.
2. Choose the hierarchy level of the **Subscriber Management** menu item from which you want to move the items.
3. From the list view, choose the items to be moved by selecting the check boxes next to the items.
4. Click **Action > Move**. A form prompts you to choose the target hierarchy from a drop-down list.
5. Choose the target hierarchy and click **OK**.

The items are moved to the selected hierarchy, and will then be shown in their new hierarchy.

24.3. Overbuild Site Defaults

24.3.1. Overbuild Site Defaults: Overview

Important: System Integrator Support Recommended - For all Managed Services: Day 2 Overbuild Projects, we recommend support from a System Integrator.

While Customers and Sites have access to Site Defaults under the Site Management menu, the Overbuild Defaults tab is only visible to Provider and Reseller Administrators.

The settings on the Overbuild Defaults tab of Site Defaults determine if and how imported objects are moved to the site hierarchy during an Overbuild process.

The settings on this tab work as follows:

- **Include Site for Overbuild:** If selected, the site is included in the Overbuild and all the settings on the Site Defaults tabs apply.

The list of defaults when the menu **Site Management > Defaults** is selected, show “true” in the Include Site for Overbuild column.

- **Create Internal Number Inventory at Customer:** If clear, the internal number inventory is created at site level only. If selected, the internal number inventory is created at customer level only, and will be used by all sites belonging to that customer, default = cleared.

Caution: If Overbuild has already been run for a site and the Internal Number Inventory has been created for the Site, if the option ‘Create Internal Number Inventory at Customer’ is enabled and Overbuild is run for the same Site, then a duplicate set of Internal Number Inventory will be created at the Customer. The same applies if the ‘Create Internal Number Inventory at Customer’ is enabled when Overbuild is run for the Site, if it is then disabled and Overbuild is run again, a duplicate set of Internal Number Inventory will be created at the Site.

- **Additional Device Pools:** By default, if a site is included for the Overbuild process, the Default CUCM Device Pool on the General Defaults tab has to match the Device Pool of the 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 in order to determine which devices and models are to be moved to the site where the site defaults are defined.

However, additional Device Pools can be added, 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 list 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 entered on the General Defaults tab if the Replace with Default Device Pool box is selected.

- **Overbuild Device Control:**
 - **Move All Devices:** If selected, all matching and related imported devices are moved to the site.
 - **Limit Moved Devices:** If selected, check boxes appear for selecting devices to import to the site. This corresponds with the controls and logic on the Run Overbuild interface. For details on the interdependency and available options when check boxes are selected, see [Run Overbuild: Overview](#).

24.4. Run Overbuild

24.4.1. Run Overbuild: Overview

Run Overbuild processes Unified CM imported objects for all sites in the current customer. It 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 conditions for creating or updating the INI (Internal Number Inventory) during Overbuild are listed in the table below:

Given	Then
<ul style="list-style-type: none"> • INI exists at Site. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear. 	The lines in the INI at the Site are updated to “Used”.
<ul style="list-style-type: none"> • INI exists at Customer. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear. 	The lines in the INI at the Customer are updated to “Used”.
<ul style="list-style-type: none"> • No INI exists. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear. 	The INI is created at the Site.
<ul style="list-style-type: none"> • INI exists at Customer. • Site Defaults “Create Internal Number Inventory at Customer” check box is selected. 	The lines in the INI at the Customer are updated to “Used”.
<ul style="list-style-type: none"> • INI exists at Site. • Site Defaults “Create Internal Number Inventory at Customer” check box is selected. 	The lines in the INI at the Site are updated to “Used”.
<ul style="list-style-type: none"> • No INI exists. • Site Defaults “Create Internal Number Inventory at Customer” check box is selected. 	The INI is created at the Customer.

The options available in the **Overbuild Action** drop-down are:

- **All Enabled Sites Using Settings Below**

- All selected devices on the **Run Overbuild** form are included.
- The Site Defaults Doc for each site contains an **Overbuild Defaults** tab. If the **Include Site for Overbuild** check box is selected, the site is included.
- An internal number inventory is created at customer level if the **Create Internal Number Inventory at Customer** check box is selected or at site level if the check box is cleared (if **Lines** are included).
- The Device Pools are from the **General Defaults** tab of the Site Defaults Doc and the Additional Device Pools from the **Overbuild Defaults** tab.
- The devices displayed when the **Limit Move Devices** option is selected on the **Overbuild Defaults** tab are ignored. Runs Overbuild for all sites, and uses the devices selected on the **Run Overbuild** form.

When the Run Overbuild tool executes with this option, it will apply to all sites and use the devices selected on the **Run Overbuild** form. Run Overbuild devices supersede the devices selected in **Limit Move Devices**.

- **All Enabled Sites Using Site Defaults Doc Overbuild Settings**

- Selected devices on the **Run Overbuild** form are hidden and ignored. All selected devices when **Limit Moved Devices** is chosen on the **Overbuild Defaults** tab of Site Defaults are moved.
- The site is included only if the **Include Site for Overbuild** check box is selected.
- An internal number inventory is created at customer level if the **Create Internal Number Inventory at Customer** check box is selected or at site level if the check box is clear (if **Lines** are included).
- The Device Pools are from the **General Defaults** tab of Site Defaults and the Additional Device Pools from the **Overbuild Defaults** tab will be used.

- **Single Enabled Site Using Settings Below**

- Overbuild is applied to the single site specified in the **Select Site** drop-down, which is exposed when this Overbuild option is selected.

Only sites that have the **Include Site for Overbuild** check box selected in the Site Defaults Doc are available in the drop-down.

- All selected devices on the **Run Overbuild** form are included.
- An internal number inventory is created at customer level if the **Create Internal Number Inventory at Customer** check box is selected or at site level if the check box is clear (if **Lines** are included).
- The Device Pools are from the **General Defaults** tab of the Site Defaults Doc and the Additional Device Pools from the **Overbuild Defaults** tab.
- The 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** form.

When the Run Overbuild tool executes with this option, it applies to the selected site only, and uses the devices selected on the **Run Overbuild** form. Run Overbuild devices supersede the devices selected in **Limit Move Devices**.

Available device types include:

- Phones
- Phone Remote Destinations
- Users:
 - device/cucm/User
 - device/hcmf/User (only if HCM-F is installed)
- Device Profiles
- Remote Destination Profiles (RDP)
- RDP Remote Destinations
- 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

The specific device models that are affected by the Overbuild move, are:

- device/cuc/User
- device/cuc/UserPassword
- device/cuc/UserPin
- device/cuc/AlternateExtension
- device/cuc/ExternalServiceAccount
- device/cuc/SntpDevice
- 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/hcmf/User (only if HCM-F is installed)
- device/pexip/Conference
- device/spark/User
- device/uccx/Team
- device/uccx/Skill
- device/uccx/ResourceGroup
- device/uccx/Agent

Data models affected when the user is moved during Overbuild:

- data/User
- data/HCSHcmfUserDAT

The availability of certain device type check boxes depends on the status of other device type check boxes. For example, the **Dual-Mode Remote Destinations**, **Users**, and **Lines** check boxes are only available if the **Phones** check box is selected. The **Device Profiles**, **Remote Destination Profiles**, and **CUC Users** check boxes are only available if the **Users** check box is selected.

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, subtransactions of a successful overbuild workflow show their Status as “Fail” if a model (such as a User) already exists. The subtransaction logs also show details of the duplicate model and an “ignore error code” information message.

24.4.2. Objects Moved During the Overbuild

The overbuild processes the imported Unified CM 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.

Objects Moved to the Site Hierarchy

The table describes objects moved to the site during the overbuild:

Object	Description
Unified CM models	device/cucm/Line device/cucm/Phone device/cucm/RemoteDestinationProfile device/cucm/RemoteDestination device/cucm/DeviceProfile device/cucm/User
HCMF (if installed)	device/hcmf/User
Cisco Unity Connection models	device/cuc/User device/cuc/UserPassword device/cuc/UserPin device/cuc/AlternateExtension device/cuc/SmtDevice 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/SmtDevice 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 Unified CM users. This matching is done according to the Unified CM 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:

- data/User
- data/HCSHcmfUserDAT

Objects Remaining at the Customer Hierarchy

The table describes objects that remain at the Customer hierarchy during the overbuild:

Object	Description
Unified CM 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

24.5. Overbuild Tool

24.5.1. Summary of the Overview Tool

Use the Overview Tool to validate your Run Overbuild process. Overbuild users can use individual device models to make sure that the required Unified CM elements have been moved to the right hierarchy.

Choose the **Overbuild > Overview Tool** menu option. It can be used at the Customer or Site hierarchy. The report shows the numbers of each Unified CM 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 you run the Overview Tool at Site level, the number on the right will always show as 0, since Site is the lowest VOSS Automate hierarchy level.

To verify the individual device models after running Overbuild, choose **Overbuild > Device Model > (desired model name)**. The hierarchy where each device model instance exists will be listed in the right-most column in the list view of the device model.

24.6. User Phone Association

24.6.1. User Phone Associate Tool

VOSS Automate uses the associated or controlled devices value on the Unified CM user (Subscriber in VOSS Automate) to determine which phones are associated to that Subscriber.

This User Phone Associate tool will ensure that Unified CM phones in the system with the ownerID value set, are correctly associated to the Unified CM user (Subscriber) for correct association in VOSS Automate.

A common situation where this might be the case is in the event of phones synced in from an existing environment for Overbuild - where the ownerID on the phones were set, but were not associated from the Unified CM User perspective. The symptom to look for is when you do not see the phones under the Subscriber view, but that you think they are owned by the user - an indication that this tool needs to be run to correct the association.

Note: When adding phones and subscribers from *within* VOSS Automate, the phone-user relationship is bi-directional.

Perform these steps:

1. Navigate to the hierarchy of the Unified CM and choose it from the **CUCM** dropdown list.

The **Number of Phones that will be checked** value that is displayed is the number of phones on the Unified CM at the hierarchy that have been synced in to VOSS Automate and have an ownerID set, but cannot be found to be an associated device of any subscriber at the hierarchy or lower.

2. Click **Save** to run the tool. Subscribers will be searched on VOSS Automate that match the ownerID and if found, their associated devices will be updated with the phone.

If the tool is now re-run for the selected Unified CM and any of the checked phones were set as associated devices, the **Number of Phones that will be checked** value will decrease accordingly.

Note: If a subscriber already has other associated devices, any new associated devices will be appended to the existing list.

24.7. Overbuild Analog Gateway

24.7.1. 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.

How Does this Feature Work?

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.

24.8. Device Models

24.8.1. Device Models: Overview

With the Device Models menu item, you can view details about the devices by model in the selected hierarchy. Like the Overview Tool, this can be useful to help you see where devices have moved as a result of the Overbuild process. When you select a device model type in the menu, a table presents you data about the devices of that model type in the hierarchy: the device names or identifiers, their device pools, their hierarchies at and below the one currently selected, and other data that varies with the device model selected.

Within a device model, you can modify, delete, and export the individual devices by selecting them. Additionally, you can change settings all at once for all the devices in a device model by selecting the **Select All** check box, located at the top-left on the table header, and choosing **Action > Bulk Modify**.

Caution: We do NOT recommend that you directly edit the device models in this menu, but use the other menus in VOSS 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 cannot move or that need additional manual moves after Run Overbuild is executed.

For CUC models, there are two system users, operator and undeliverablemessagesmailbox, which will remain at 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. Note that adding device instances here in the Overbuild menu is not recommended.

- CUCM CtiRoutePoint
- CUCM DirectedCallPark
- CUCM Phone
- WebEx User

24.8.2. Find a User Associated with a CUC Device Model

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 to which the device model is associated. The VOSS Automate search function can be used to find this associated user information.

Perform these steps:

1. Choose **Overbuild > Device Models**.
2. Click the desired CUC device model in the menu. A list of the CUC device models appears.
3. Click the desired device model instance.
4. In the CUC device model output, find the field Subscriber Object ID.
5. In the search box at the top right of the Admin Portal, type this string:

```
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 VOSS Automate API request would be:

```
https://<host-or-proxy>/api/tool/Search/?  
format=json&  
device%2Fuc%2Fuser%20  
with%20object_id%20like%20  
9b16c8ce-edd9-43c4-9262-c25296d3560b
```

25. Administration Tools

25.1. Import

25.1.1. 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 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).

25.1.2. Import a File

1. Choose the hierarchy level for the import (not applicable to packages - see [Import: Overview](#) for more details).
2. Access the **Import** form (default menu **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.
4. Click **Import** to import the file to the hierarchy.

25.2. Bulk Administration

25.2.1. Bulk Load Overview

The bulk loader tools enable the quick and easy management of system data using pre-populated MS Excel formatted spreadsheets.

A spreadsheet template can be generated by the system for any of the resources in the system - either from the Admin Portal or the API.

The 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 will 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.

25.2.2. Data Export

Data can be exported in JSON format and as MS Excel spreadsheets.

The system JSON file format is used to Export and Import various operations on model instances. The operations available via JSON files are: Add, Modify, Delete. This Import and Export task is carried out from the Admin Portal or API using the file Export and Import functionality.

The JSON file format for the different operations is available when you **Export** a specific model and choose **JSON** as the export format. The API provides a request URL and parameter for this task - refer to the API documentation. The export file format is a compressed JSON file. The import filename and format can be <filename>.JSON, <filename>.JSON.zip or <filename>.JSON.gz.

The Excel file format for data export of selected items can be carried out in the list or instance view of a model.

Commands can be exported from the Admin Portal by choosing **Export** and then selecting either **Excel** or **Excel (formatted)** as the export format. The API provides a request URL and parameter for this task - refer to the API documentation. The export file format is a MS Excel XLSX file.

The Field Display Policy that applies to a menu item from which an Excel (formatted) export of data is carried out, is reflected in the Excel (formatted) exported sheet as follows:

- Titles of attributes
- Sequence of the attributes
- Group names
- Hidden fields, with the exception of mandatory fields.

25.2.3. 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:
 - 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.

25.2.4. Bulk Load Template Export

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 VOSS 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 administration 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](#).

25.2.5. Carry out a 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 administration tool to upload the bulk load template sheet.

25.2.6. Bulk Load Sheets

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 VOSS 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

VOSS Automate 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 Bulkload 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 table describes the general bulk load limitations:

Limitation	Description
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 fields are currently exposed as mandatory fields. The fields and the specific conventions that are 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.
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.	<p>Examples - GUI rules may:</p> <ul style="list-style-type: none"> • 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 following 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.

	Y	Z	AA	BB
1				
2	forwardHuntNoAnswer.destination	forwardHuntNoAnswer.usePersonalPreferences	forwardHuntNoAnswer.callingSearchSpaceName	forwardHuntBusy.destination
3				
4	# Destination	# Use Personal Preferences	# Calling Search Space Name	# Destination
5		TRUE		

Sample Bulk Load Sheets

To overcome the complexities introduced by the bulk load limitations, a set of sample bulk load sheets have been generated that enable users to get started quickly and to leverage the best practices developed by VOSS.

The latest sample bulk loaders can be obtained from your account team.

Bulk Loading a File

This procedure uploads a bulk load .xlsx worksheet.

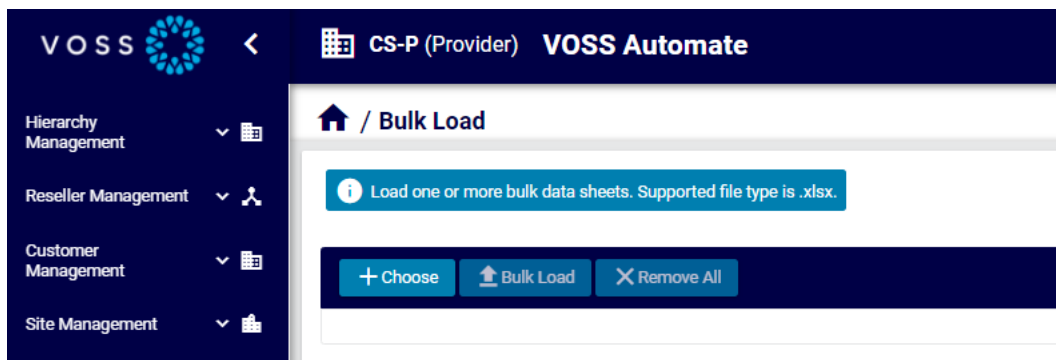
Prerequisites

- File format must be .xlsx.
- Ensure any referenced configuration templates are available.
- Verify the information in the file, and ensure it contains all required details.
- 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, either type a space in the cell, or type <NULL> (in that cell).

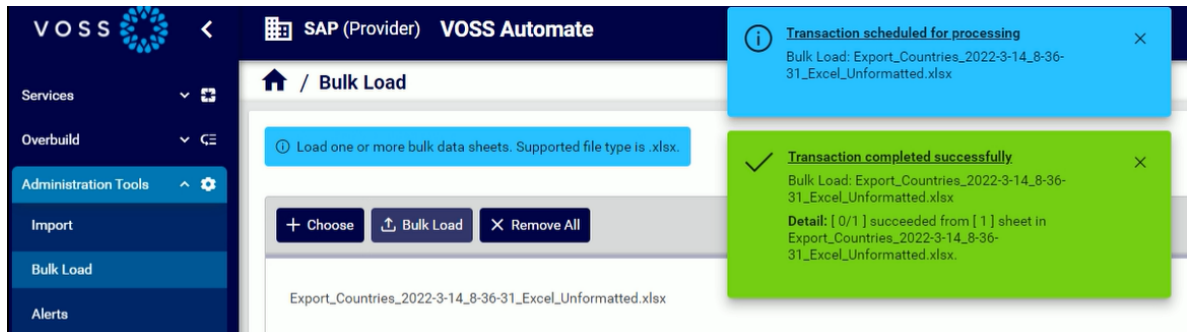
Note: Spreadsheet formulas in data are ignored, for example: '=7+2'

Perform these steps:

1. Set the hierarchy to the level where you want to add bulk data.
2. Choose an option (default menus):
 - In the Admin Portal, go to (default menus) **Administration > Bulk Upload**.
 - In the Business Admin Portal, select the **Tools** menu; then, click **Bulk Upload**.
3. On the **Bulk Load** page, click **Choose**; then, browse to the file/s.



4. Click **Bulk Load**.
5. View transaction result.

**Note:**

- You can click on the transaction result to inspect the bulk load in the transaction log, if necessary.
- In the legacy Admin GUI only:
 - The **Execute Bulk Load** sub-transaction list shows the transaction for each row of the sheet.
 - To schedule the bulk load, clear the **Execute Immediately** checkbox and add scheduled date and time values in the mandatory **Execution Date**, **Execution Time** and **Execution Timezone** fields. A scheduled bulk load is shown on the list view of the Schedule and has the name and upload load date of the sheet.

25.2.7. Sample Bulk Loaders

Sample loaders enable a quick start by providing working examples of the most frequently used loaders. These can be customized according to user requirements and data.

Furthermore, sample bulk load sheets incorporate best practices for using bulk loaders; ensuring rapid customer and subscriber 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.

25.2.8. Bulk Load Template Sheet Layout

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:

- 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.
 - 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.
-

entity: relation/HuntGroupRelation; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template: ; meta_pre																	
\$hierarchy	\$action	\$search_fields	\$device	\$template	\$nd1	\$pkid	pattern	name									
# Base							# Hunt Pilot Pattern										
Comment	Hierarchy	Nod	Action	Search	Field	# Device	FT	Templa	Network	Device	Li	Unique	Identifie	# Hunt	Pilot	Pattern	# Name

Refer to the example sheet snippet. A bulk load sheet contains the following information:

Sheet name (tab on spreadsheet workbook)

Any name can be provided on the tab or sheet. If the name is prefixed with a # 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 {}:

```
entity: {entity name}; \
hierarchy: {hierarchy}; \
parallel: {True | False}; \
parallel_transaction_limit: {n}; \
template: {config_template}; \
meta_prefix: {c}; \
evaluate_macros: {True | False}
```

- `entity: {entity name}`: the name of the model, in the format `{modeltype}/{model name}`, for example `data/User`
- `{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: 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 \(grouped by # Base in Row 3\)](#).

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 # character is used as prefix. An error message will be shown in the transaction log.

- *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.

– For examples, see [Bulk Load Sheet Macro Evaluation](#).

Note: `fn.bulkload_evaluate` is not available via the Macro Evaluator. For testing purpose using the Macro Evaluator, please use the `fn.evaluate` function prefix.

Row 2 - Base columns (grouped by # Base in Row 3)

The list below describes the column values with the default value of `meta_prefix`, in other words, column names by default prefixed by \$.

The purpose of the columns is to provide more detailed instructions or overriding data for a row.

- Comments: Any row that contains a # character in column A is considered a comment row and will be 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** 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.
- **\$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 out 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`.

- `$template` (Configuration Template): If a row that contains a Configuration Template name that applies to the model, this template is applied to the row when it is loaded. Upon bulk loading, values in this column will override any value for `template` in the sheet header.
- `$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.

entity: relation/HuntGroupRelation; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template: ; meta_pref												
Hierarchy	Section	Search_fields	Device	Template	ndl	pkid	pattern	name				
# Base					# Hunt Pilot Pattern							
# Comment	Hierarchy	Nod#	ActionSearch	Fiel	# Device_FT	Templa	Network	Device	Li#	Unique Identifier	# Hunt Pilot Pattern	# Name
	sys.Provider1Customer52										33121	
#	svs.Provider1Customer52										33122	

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.

25.2.9. Export Data Sheet Layout

This topic describes an exported sheet, either formatted or not formatted.

For both exported sheet formats, the header and column layout shows correspondences with the Bulk Load Template sheet.

The following items apply to sheets containing data exports:

- The # Comment column shows the text “Exported data” in green for each row of data.
- The # Hierarchy Node column shows the source hierarchy of the exported row. The hierarchy: value in the sheet header shows the hierarchy from which the data export was run.
- If device instances were exported, the # Device columns shows the business key of the device (for example, comma-separated: host, port, hierarchy).
- If a Configuration Template was applied during the export - for example if it applied to the Admin Portal form - # CFT Template column will show this name for each row, as well as the template value in the sheet header. If a sheet is used for loading, the row value overrides the sheet header value.
- The # Unique Identifier contains the pkid that is used to identify the exported resource represented in the row data. On modify, delete, execute, and custom action operations, this pkid is used to identify the resource instance on the database represented in the row data.

The pkid field:

- takes precedence over the search fields criteria when locating a resource

- 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
- For a formatted Excel export, the columns in the sheet correspond with an exported Bulk Load Template sheet.
- For a non-formatted Excel exported sheet, the columns correspond with the properties of an exported JSON file. For example, only properties where strings are not empty and boolean values are set, are exported.
- A formatted, exported sheet of data can be used just as a Bulk Load Template sheet to bulk load data. For other Actions, the # Search Fields column needs to be completed. Refer to [Bulk Load Template Sheet Layout](#).
- “Default” values of attributes in any Not Grouped Fields group need to be removed from a sheet before it is used to bulk load rows.
- The rows and data in the columns of an exported sheet are bound by the limitations of the MS Excel format. For example, model data with property values longer than 32,767 characters (maximum length of MS Excel cell contents) will be truncated in the exported sheet.

25.2.10. 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.
 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.

25.2.11. Bulk Load Transactions

The transaction log is available on the user interface after a bulk load transaction has been run. Refer to the topics on transactions and viewing transactions in the documentation.

Go to the **Transaction** menu. Bulk load transactions show in the log:

- 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 section will hold the name of the file that is bulk loaded as well 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 box shows the number of successful and failed rows loaded.

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 more 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.

25.3. Alerts

25.3.1. Alerts

Administrators can view alerts at the hierarchy level at which they are logged in, and the levels below that hierarchy. For example, if an alert is raised at the customer level, for example *sys.hcs.provider.reseller.customer*, then the provider, reseller, and customer administrators can see that alert but not site administrator. A Site administrator doesn't have access to view the alert. All administrators have read and delete permissions to the alerts.

When an alert is raised, the messages or notifications indicator on the **Messages** button will show this. Clicking the button will show a message that alerts have been raised: "There are one or more alerts. Click here to view them." When clicking on this message, the user is directed to the list of alert messages.

The Alerts list can be viewed and managed on the Admin Portal from the **Alerts** list view (default menu **Administration Tools > Alerts**) or by clicking **Messages** on the top menu bar.

The Alert list is summarized by:

- **Category:** A specific category to which the alert belongs, for example: "Device Change Notification Collector/CallManager".
- **Code:** an error or warning code associated with the alert.
- **ID:** A reference to the source of the alert. Alerts with the same ID and code will update 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.

Administrators can also filter alerts by any of these fields.

When features are enabled to send alert messages, these are recorded in the list. Each alert also has such properties as a 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.

Alert messages can be inspected and then acted upon by the administrator. If an issue that raised the alert has been resolved, the administrator can delete the alert from the list. If no alerts are present in the list, no notification is shown.

25.3.2. Alert Types and Alert Field Reference

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>

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

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

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

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 [Scheduling](#).

Alert 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.

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

25.4. Transactions

25.4.1. Transaction Logging and Audit

Activity on the VOSS Automate system results in transactions that are recorded. The **Transaction** list view provides auditing information for each transaction.

View specific transaction details by clicking on a transaction. The **Back** button on the button bar (or the **See all transactions** link on the transaction details screen) can be used to navigate to the previous screen, for

example from the parent transaction screen to the list view of all transactions.

Details

Information recorded includes data such as:

Info	Details
Transaction ID	Identifier of 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.

On the Admin Portal, details of a specific transaction are displayed when the transaction is selected from the list view. Refer to [Bulk Load Transactions](#).

When a transaction is selected, the **Base** tab shows details of the columns of the transaction list view. The button bar on the detail list view shows **Help** and **Refresh** buttons if the transaction is still running.

If the transaction is running, click the **Refresh** button to update the Progress field. On the Admin Portal, a **Auto-refresh** check box is also available to automatically update the progress every 5 seconds.

Lists of transactions and sub-transactions can also be filtered. Refer to "Filtering Lists" and "Filtering Transactions" for details.

Note: If the transaction queue service stops and is restarted, any queued transactions will resume processing, while processing transactions will fail and show a message: Transaction aborted due to queue service restart.

Cancel

If you want to cancel a transaction while it is still running, click the **Cancel** button. If a transaction is cancelled, its **Status** is marked as **Fail** and the **Message** field shows **Transaction canceled**.

If a transaction, with sub-transactions, is canceled, the sub-transaction currently in progress will complete. This sub-transaction as well as all preceding sub-transactions will then roll back to their previous states. Note that bulk load transactions do not follow this behavior. Each bulk load sub-transaction is seen as a main transaction, and only the 'in progress' sub-transaction will roll back to its previous state.

Replay

A **Replay** button is available if the transaction is complete. A transaction can be replayed if required, for example if a transaction failed because a target system service was not running. The replay of the transaction can then be used instead of re-entering data on an Admin Portal form.

Edit and Replay

An **Edit and Replay** button is also available for completed transactions. This is similar to the **Replay** button, but allows you to first make changes to the previously submitted form before the transaction is resubmitted.

The button is available for transactions that did not originate from bulk loads, or pop-up forms.

Edit and Replay opens the original input form that resulted in the transaction. The form also contains the original data that was posted. This data can be edited and the form can be submitted to replay the transaction. This functionality can therefore be used to for example edit a failed transaction or to modify data of a successful transaction.

Since GUI Rules apply to a form from a specific hierarchy, the Edit and Replay functionality should only be used from the same hierarchy as the original transaction was executed.

Note:

- Replay and Edit and Replay functionality 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(s). The only time a bulk load file is 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 Subscriber transaction, the following user information fields will not automatically update when changing the Username field:
 - Entitlement Profile
 - Firstname
 - LastName
 - Email

These need to be edited manually.

Sub-transactions

If a transaction has sub-transactions, a sub-transaction list is available.

- On the Admin Portal, the sub-transaction list will show below the transaction details if there are 10 or less sub-transactions. Otherwise, a **Sub Transactions** tab is available on the form to list sub-transactions. A navigator bar and list page show at the bottom of the list.
- On the Legacy Admin GUI, the sub-transaction list will show below the transaction details and if there are more than 10 sub-transactions, a list length (**Items/page**) and pager (**Page n of m (k items)**) is available.

Sub-transactions also 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 “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 section 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.

Resource or Record

Depending on the transaction type, an option is available to navigate to the original record where a resource changed.

25.4.2. 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

25.4.3. View a Transaction

You can only view transactions that are relevant to your specific hierarchy level. For instance, if you are logged into the system as a Customer Administrator you will be able to view all transactions that were performed at the customer for which you are the administrator. This includes transactions that were performed at any of the sites that belong to the customer. If you are logged in as a Site Administrator you will be able to view only the transactions that were performed at your specific site. Refer to the topic on Data Partitioning in the Core Feature Guide and to the API Guide to view transactions by means of the API. The steps below can be followed on the Admin Portal.

1. Choose **Administration Tools > Transaction**.

By default, the **Transaction** list view shows all parent transactions in progress or executed. This is indicated in the **Status** column of the list.

If you also want to see the child transactions (sub-transactions) in the list view, select the parent transaction. The list view shows both parent and sub-transactions.

For completed transactions, the **Status** column displays either **Success**, **Success With Async Failures**, or **Fail**. Failed transactions are highlighted in red by default, but this can be overridden in the Theme if required. An exclamation icon is also displayed next to the word **Fail**.

The **Detail** column provides additional details on the transaction if available. See “Transaction Details” for more information.

2. Click an individual transaction or sub-transaction (if required) to show a detailed view. If the top-level transaction has the status **Success With Async Failures**, the list of failed async transactions show below the list of sub-transactions. The 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.

25.4.4. Transaction Log Levels

For users that have access to the data/Settings model or view/DataSettings, the global levels of logging can be managed.

This level will affect the Log block of messages at the bottom of a selected transaction on the Transaction interface and does not for example affect the transaction or sub transaction Action and Detail information.

Log levels are *cumulative*, in other words, more detailed levels include all details from less detailed levels. The levels includes messages and have severity values as follows:

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

- The 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: [Manage System Settings](#).
- If a transaction fails, the Log block will include 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.

25.4.5. 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:

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	<ul style="list-style-type: none"> • 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.

25.4.6. Filtering Transactions

Overview

A transaction filter is a logical AND operation based on column values in the Transactions list, defined as search criteria on the **Transaction Search Filter** dialog.

Using Filters to Search for Transactions

1. Log in to the VOSS Automate Admin Portal.
2. Go to (default menu) **Administration Tools > Transaction** to open the **Transaction** log.

Note:

- In the classic Admin GUI, you can also open the **Transaction** log via the toolbar **Notifications** icon.
 - In the Admin Portal, you can also open the **Transaction** log via the toolbar **Transaction Log** icon.
-

3. On the **Transactions** 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. Open the search filter:

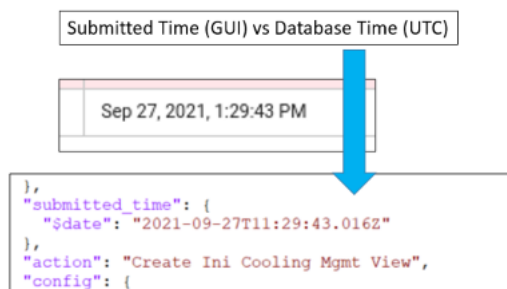
- In the classic Admin GUI, to open the **Transaction Search Filter** dialog, either click the filter icon in the header row of the **Id** column, or click **Filter** at the bottom of the list.
- In the Admin Portal, to open the **Filter** dialog, click the toolbar **Filter** icon.

5. In the Filter dialog, specify search criteria for the transaction/s you wish to view:

Field	Description
Transaction ID	Options depend on whether you're using the Admin Portal or the classic Admin GUI <ul style="list-style-type: none"> • Admin Portal: Enter a specific transaction ID, else, leave the field clear to search on alternate criteria. • Legacy Admin GUI: <ul style="list-style-type: none"> – 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.
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, Queued, Processing, Success, Success with Async Failures, or Fail.

Field	Description
Date Range	<p>Predefined options are Last Day, Last Week, Last Month, or All. Alternatively, you can specify a custom date range.</p> <p>When selecting a quick filter (Last Day, Last Week, Last Month), the next time the filter is opened, the date selection displays as a Custom date range, since the range is then less than the selected interval.</p> <p>When choosing a Custom date range:</p> <ul style="list-style-type: none"> • In the Admin Portal, choose a start and end date from a date picker. • In the legacy Admin GUI, choose a start date and time, and an end date and time. <p>When specifying a start date, end date, and time, use a transaction date and time range in the format of the system locale. For example, for language code en-us, the typed format is mm/dd/yyyy. The number format “9” instead of “09” is also valid.</p> <p>You can select a date range, or type in values. Time values can be selected for 15 minute intervals, or type in values (the system locale format is default).</p> <p>Note that when adding filter criteria for Username, Detail, or Message (legacy Admin GUI), filtering may be slower when the date range is greater than 7 days.</p> <p>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)</p>
Action	Select an action to filter on, for example, Create Subscriber, or start typing to filter values in the drop-down.
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	<p>Case-insensitive field to filter by text values in the Message column (legacy Admin GUI).</p> <ul style="list-style-type: none"> • For <i>failed transactions</i>, hover over the Status column to view a message, or inspect it in the transaction detail view. • Some <i>successful transactions</i> also show messages when viewing its details, for example, data import and bulk load.

(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.

25.4.7. Filtering 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".

25.4.8. 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:

- 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.

25.4.9. 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.

25.4.10. 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 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.

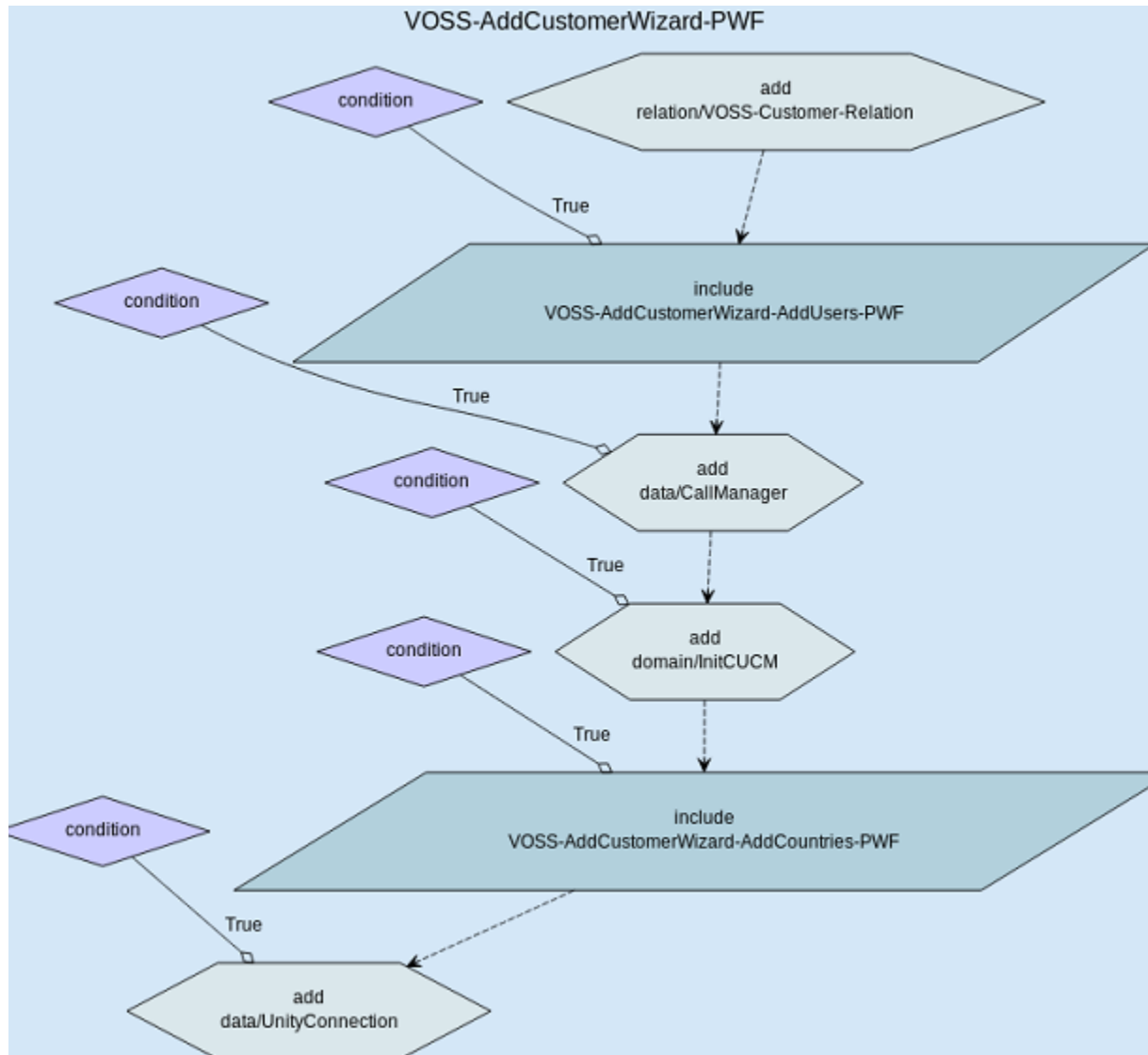
After the wizard is run, the sub-transactions show the actions of the workflow. In the example, only the Unified CM is selected. The first action in the wizard is to execute a workflow, that results in three sub-transactions. The first sub-transaction is itself a workflow that carries out three actions:





























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.



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 15:26:1 SAST	info	Step 3 - End 
Mar 27, 2014 15:26:1 SAST	info	Step 3 - Template (AddCustomerWizard_CUCM_CFT) aft 
Mar 27, 2014 15:26:1 SAST	info	Step 3 - Template (AddCustomerWizard_CUCM_CFT) be 
Mar 27, 2014 15:26:1 SAST	info	Step 3 - Template after merging AddCustomerWizard_Cl 
Mar 27, 2014 15:26:1 SAST	info	Step 3 - Start add data/CallManager 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - End 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - End 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Template (AddCustomerWizard_User_CFT) after 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Template (AddCustomerWizard_User_CFT) befo 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Template after merging AddCustomerWizard_U: 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Start add data/User 
Mar 27, 2014 15:26:1 SAST	info	Step 0 - Executing workflow (dynamic_workflow) with thi 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Executing workflow for each [1] 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Start add data/User 
Mar 27, 2014 15:26:1 SAST	info	Step 0 - Executing workflow (VOSS-AddCustomerWizard: 
Mar 27, 2014 15:26:1 SAST	info	Step 2 - Including_workflow, name: VOSS-AddCustomer) 
Mar 27, 2014 15:26:1 SAST	info	Step 2 - Start include VOSS-AddCustomerWizard-AddUs 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - End 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Template (AddCustomerWizard_VOSS-Custome) 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Template (AddCustomerWizard_VOSS-Custome) 
Mar 27, 2014 15:26:1 SAST	info	Step 1 - Template after merging AddCustomerWizard_W 
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

25.4.11. Device Data Sync Errors in Transactions

The DataSync 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 Phone.
2. Requests for detailed information of each resource of the specific type.

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.
- CUCM AXL handled by VOSS 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
DirNumberAliasLookupan dSync	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.

- HCMF handled by VOSS Automate (DataSync transaction final status is not failed)

Model	Operation	Device Error Message Match	VOSS Automate DataSync Action and/or error log
TransportModeSettings	GET	API Call Error [404]	Ignored known error
SmartAccountsAccessCredententials	GET	API Call Error [404]	Ignored known error

- CUCM Device errors not handled by VOSS 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.

- CUC Device errors not handled by VOSS 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	<ol style="list-style-type: none"> 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 be 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.

25.4.12. Export a Transaction

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 (default menu **Administration Tools > Transaction**), select a parent transaction.

- From the transaction details view, choose **Export** from the button bar. 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
- 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",
  "transaction_id": "d7aa7333-f692-40b4-a637-80cf456c1f70"
},
```

25.5. Northbound Notifications

25.5.1. Northbound Notification

The VOSS Automate Northbound Notification (NBN) provides a mechanism to notify an Operations Support System (OSS) or Business Support System (BSS) when user data in VOSS Automate is created, updated, or deleted. The 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 VOSS Automate.

relation/Subscriber Subscriber information, such as assigned devices and services. Only changes made in VOSS Automate via Subscriber Management generate notifications. Changes to subscribers made in VOSS Automate do not generate notifications.

All NBN events are post-execution so the notification is sent immediately after the data is changed in VOSS 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.

25.5.2. 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.

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'
  }
}
```

25.5.3. 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.

25.5.4. 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.

25.5.5. 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**.

25.5.6. Configure Northbound Notification Event Attributes

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. Choose **Administration Tools > Northbound Notifications > Attributes**.
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**.

Apply the event attributes to an event by adding or updating the event and choosing the desired attribute selector.

25.5.7. Configure Northbound Notification Event

You must set the Northbound Notification Destination before you can configure events.

Use this procedure to specify an event to trigger Northbound Notifications.

1. Log in as provider administrator.
2. Choose **Administration Tools > Northbound Notifications > Events**.
3. Click **Add**.
4. Provide the following information for the triggering event:

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**.

25.6. Schedules

25.6.1. Scheduling

Single or Multiple actions can be executed on one or more resources. The actions can be scheduled to take place at a specified time or to repeat.

Currently, the action is to *execute*.

The resources that can be executed are:

- **Data Sync**
- **Script**
- **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 synchronization 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.

25.6.2. Create or Update a Schedule

This procedure displays existing, configured schedules, adds a new schedule, or edits an existing schedule.

1. Log in to the Admin Portal and select the hierarchy where you want to add or update a schedule.
2. Go to (default menus) **Administration Tools > Scheduling** to open the **Scheduling** list, where you can view existing schedules (if configured), including a number of attributes for each schedule.

Note: Resource attributes are used for filtering when you want to choose a resource.

3. Choose an option:
 - To edit an existing schedule, click on a schedule in the list to open its configuration page. Edit the schedule, and save your changes.

Note: See the field descriptions below to find out more about field values you may want to update.

- To add a new schedule, click the Plus icon (+) to open the **Scheduling / New Record** page. Go to the next step in this procedure.

4. On the **Details** tab, complete the following:

Note: In the classic Admin GUI, this tab is called the Base tab.

- a. Mandatory. At **Schedule Name**, fill out a name for the schedule.
- b. At **Owner**, fill out the name of the user who created the schedule.
- c. Mandatory. At **Schedule Type**, choose an option, either **Multi Execution** or **Single Execution**.

Note: Choosing an option launches the display of an additional tab on this page. The tab name depends on the option you select at **Schedule Type**, either **Multiple Executions** or **Single Execution**.

- d. Select or clear the **Active** checkbox to define whether the enable or disable the entire schedule.
- e. Optional. At **Scheduled resources**, click the Plus icon (+) to configure an action to execute on a resource.

Note: You can schedule one or more actions or one or more resource types, and choose resource attributes for each.

- a. At **Action**, choose an action (e.g. Execute).
- b. Choose a **Resource Type** (resources that can be executed, for example, data/DataSync).
- c. For the selected resource type, at **Resource Attribute**, choose a unique identifier (the resource attribute, which is used for filtering when choosing the resource type, which is typically name).

- d. At **Resource**, select the value of the resource attribute. For example, if the attribute is name, then the name of the resource.
 - e. At **Perform Action**, select or clear the checkbox to enable or disable the resource scheduled action.
 - f. Repeat this step to add additional scheduled resources.
5. On either the **Multiple Executions** or **Single Execution** tab, fill out the scheduling time information according to the selected schedule type.
- Date format: *YYYY-MM-DD* in Local time - an **Execution Timezone** is selected
 - Time format: *HH:MM:SS* in Local time - an **Execution Timezone** is selected
- a. On the **Multiple Executions** tab, choose options for execution:
 - **Use Specific Executions** - Allows one or more specific schedule times. An **Execution Date**, **Execution Time** and **Execution Timezone** is added for each specific schedule.
 - **Use Calender Executions** - Allows one or more calendar times (**Calendar Hour** and **Calendar Minute**) and dates (**Calendar Month** and **Calendar Day**). If no time is entered, the current time is used.
 - **Use Timed Executions** - Allows one or more specified number of repetitions (**Number of Repeats**) at intervals (**Repeat after (x) Days**, **Repeat after (x) Hours**, **Repeat after (x) Minutes**) from a specified start time (**First Execution Date**, **First Execution Time**, **First Execution Timezone**).

If more than one of these options is selected, the first scheduled time takes priority.
 - b. On the **Single Execution** tab, fill out **Execution Date**, **Execution Time**, and **Execution Timezone**.
6. Click **Save** to create (or update) the schedule.
- You schedule you added (or updated) displays in the **Scheduling** list view.

25.7. System Settings

25.7.1. Manage System Settings

Administrators at provider level as well as `hcsadmin` administrators have access to a **System Settings** menu under **Administration Tools**.

Transaction Log Level

Provider level and `hcsadmin` administrators can modify the Transaction Log Level - the level of verbosity of transaction logs.

The setting is available as a global setting to high level administrators who have access to the `data/Settings` model. When an administrator first opens **System Settings**, the displayed value (default: Info) for the **Transaction Log Level** is the default in the global setting.

For a description of the available log levels, see: [Transaction Log Levels](#)

The settings are:

- Disabled
- Error
- Warning
- Info
- Verbose
- Debug

The purpose of the setting is so that the log level can be changed according to need, for example to Verbose so that more details are available for immediate troubleshooting and customization work.

Note: A **Notes** section and warning is shown if the level is set to Verbose or Debug, reminding administrators that the retention period of such logs is shorter due to their increased size, which consequently reduces the date range of available logs for troubleshooting.

A typical use of this setting would be for troubleshooting: when a problem is encountered on a system and detailed logs need to be obtained. The steps could then be:

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.

26. Single Sign On (SSO)

26.1. 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 Single Sign-On for VOSS Automate](#).

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 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.
-

26.2. SSO Certificate Management

Use this procedure to create a self-signed or third-party-signed system certificate to use when setting up Single Sign-On (SSO) on the web proxy node on VOSS Automate.

Note:

- Web server certificate management is carried out on the VOSS Automate command line. Refer to the CLI documentation for details.
 - During customer onboarding, SSO certificate creation is customer specific.
-

Procedure

1. Log in as system administrator.
2. Choose **Single Sign On > Certificate Management**.
3. Click **Add**.
4. On the **Base** tab, enter a **Name** and **Description** for the certificate.
 - For a self-signed certificate, leave the **Generate Certificate Signing Request** check box clear.
 - For a third-party-signed certificate, select the **Generate Certificate Signing Request** check box.
5. For a self-signed certificate, control when the certificate is valid by changing the Valid From and Valid To fields. These are measured in seconds and default to 0 (now) and 315360000 (10 years), respectively.
6. (Optional) Change the **Key Length** from the default of 1024.
7. Click the **Certificate Information** tab, and complete all mandatory fields (see **Certificate Management** fields).
8. Click **Save**.
9. If you created a self-signed certificate you are done. If you requested a third-party-signed certificate, continue to the next step.
10. Click the certificate you just created.
11. Choose **Action > Export Certificate Request**.
12. Follow your organization's procedures to obtain the third-party signature for the certificate.
13. Click the certificate.
14. Choose **Action > Upload Signed Certificate**.
15. Browse to the signed certificate and click **OK**.

26.2.1. Certificate Management Fields

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

26.3. Configure Single Sign-On for VOSS Automate

This procedure configures self-service Single Sign-On (SSO) for VOSS Automate.

The configuration applies to customers and customer administrators associated with the identify provider (IdP).

Note:

- Administrators are configured for SSO use via the **Users** form (default menu **User Management > Users**).
- Administrators can also be configured with multiple user roles, i.e. have a user type “End User + Admin” (see: [Add an Admin User](#)). While the role of such an administrator user is “selfservice”, the user’s association with a Authorized Hierarchy model instance redirects such an administrator to the *same* interface as a single role administrator when using the SSO URLs for login - as indicated under *Integrating with an SSO Identity Provider* below.

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/#/
```

Prerequisites

- Create a self-signed or third-party-signed system certificate. For more information, see [SSO Certificate Management](#).
- The VOSS Automate server and the IdP server must be configured so that their clocks are synchronized.

26.3.1. SSO Service Provider Configuration

1. Log in to VOSS Automate as system administrator.
2. Choose **Single Sign On > SSO SP Settings**.

Note: This screen is only available to you if you've logged in as a higher-level administrator.

3. Click **Add**.

Note: Configure only one instance of SSO SP Settings.

4. On the **Base** tab:
 - (Mandatory). From the **System Certificate** drop-down, choose the System Certificate to use. See [SSO Certificate Management](#).
 - To allow the SSO SP Setting to expire, enter a number of hours in the **Validity (Hours)** field.

Note:

- Specifying an unsigned third-party-signed certificate results in an error.
 - To renew an expired certificate, see [Renew Single Sign-On Certificate for VOSS Automate](#).
-

5. On the **SAML SP Settings** tab:
 - Enter the mandatory **FQDN of the Server**.
 - Select the **Sign Authn Requests** and **Want Assertions Signed** check boxes as required by your security environment.

Note:

- Only select **Want Reponse Signed** if you're sure that all IdPs sign responses.
 - 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`.
-

6. Click **Save**.
7. To view the location of the VOSS Automate SP metadata that you will upload to the IdP:
 - Choose **Single Sign On > SSO SP Metadata**.
 - Point your browser to the URL shown here, and then save a copy of the SP metadata.
8. Upload the SP metadata to the IdP.

Refer to your IdP documentation for details on adding VOSS Automate as a service provider.

Note: 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.

- Download the IdP metadata from the IdP server.

Refer to your IDP documentation for details on downloading IDP metadata.

Note: If an expired SSO certificate is being renewed and the IdP metadata has *not* changed, the download, configure and upload of the IdP metadata is not required.

26.3.2. Integrating with an SSO Identity Provider

- Log in as provider, reseller, or customer administrator (depending on your IdP configuration level).
- Choose **Administration Tools > File Management** and upload the IdP metadata.
- Choose **Single Sign On > SSO Identity Provider**.
- Click **Add** to add the SSO Identity Provider configuration.

Note: Only one instance of an SSO Identity Provider can be configured for a hierarchy node.

- On the **SSO Identity Provider** screen, complete at least the mandatory fields (Entity ID, Login URI, Local Metadata File, User lookup field at minimum, the mandatory **SSO Identity Provider** fields (see **SSO Identity Provider** fields):

If a customer is using a *custom domain*, the **Service Provider Domain Name** is filled in 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``
Business Admin Portal: ``https://<Service Provider Domain Name>/business-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 VOSS-4UC 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 and re-upload the metadata so that it contains this field.

6. Click **Save** to save the SSO Identity Provider Configuration and enable SSO if selected.
7. Choose **User Management > Users** and filter on **Auth Method** equals SSO to display enabled SSO users.

When the **Service Provider Domain Name** is not specified for a given IDP, these URLs 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``
Business Admin Portal:	``https://<FQDN of the Service Provider>/business-admin/sso/ ↪<Login URI>/login``

See **SAML SP Settings FQDN** in *SSO Service Provider Configuration*.

The IdP redirects to this FQDN on login.

Note: While an IdP may exist at more than one hierarchy in VOSS Automate, a user will only be permitted to log in if the user exists at or below the hierarchy of a single IdP.

26.3.3. SSO Identity Provider: Field Reference

Field	Description
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.
Local Metadata File	Mandatory. Choose the IdP metadata file. This field must be unique across the system.
SSO Enabled	Select the check box to enable SSO for users synced in or created at the current hierarchy level. Clear this check box to disable SSO for the users associated with the defined IDP.
Note	Reminder to upload the IdP metadata file
SSO Login URL	Read-only field displays the SSO Login URL to use. Users with <code>selfservice</code> role and no Authorized Admin Hierarchy will be redirected to Self-service.
Business Admin Portal Login URL	Read-only. Displays the Business Admin Portal SSO Login URL to use.
Admin Portal Login URL	Read-only. Displays the new Admin Portal SSO Login URL to use.
User lookup field	Mandatory. Select the field to bind the VOSS and SSO user - typically <code>username</code> .
Authentication Scope	Hierarchical scope this server applies to. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Synced users only: Only users synced in from LDAP can authenticate against this server. • All users

For Authentication Scope, also see [User Login Options by Authentication Method and Server Authentication Scope](#).

26.3.4. SSO Scenarios for User Roles

The table below shows the interface a user will be directed to when using a specific SSO URL, according to the user's role: either single role or multiple role (includes Authorized Admin Hierarchy).

User Role	Auth Admin?	URL used	UI (Session Limiting)	Expected Behavior
selfservice	Yes	<a href="https://<hostname>/sso/<login-uri>/login">https://<hostname>/sso/<login-uri>/login	administrator	Redirect to Classic Admin
selfservice	Yes	<a href="https://<hostname>/business-admin/sso/<login-uri>/login">https://<hostname>/business-admin/sso/<login-uri>/login	administrator	Redirect to Business Admin
selfservice	Yes	<a href="https://<hostname>/admin/sso/<login-uri>/login">https://<hostname>/admin/sso/<login-uri>/login	administrator	Redirect to Admin
selfservice	No	<a href="https://<hostname>/sso/<login-uri>/login">https://<hostname>/sso/<login-uri>/login	selfservice	Redirect to Self-service
administration	Yes	<a href="https://<hostname>/sso/<login-uri>/login">https://<hostname>/sso/<login-uri>/login	administrator	Redirect to Classic Admin
administration	Yes	<a href="https://<hostname>/business-admin/sso/<login-uri>/login">https://<hostname>/business-admin/sso/<login-uri>/login	administrator	Redirect to Business Admin
administration	Yes	<a href="https://<hostname>/admin/sso/<login-uri>/login">https://<hostname>/admin/sso/<login-uri>/login	administrator	Redirect to Admin
administration	No	<a href="https://<hostname>/sso/<login-uri>/login">https://<hostname>/sso/<login-uri>/login	administrator	Redirect to Classic Admin
administration	No	<a href="https://<hostname>/business-admin/sso/<login-uri>/login">https://<hostname>/business-admin/sso/<login-uri>/login	administrator	Redirect to Business Admin
administration	No	<a href="https://<hostname>/admin/sso/<login-uri>/login">https://<hostname>/admin/sso/<login-uri>/login	administrator	Redirect to Admin

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/#/
```

26.4. Configure the System as a SSO Service Provider

The configuration below is available to high level administrators *above* the provider administrator from a menu called **SSO SP Settings**.

1. On the **Base** tab, enter the Entity ID is required and is used to identify VOSS Automate as service provider. The URL points to the metadata, for example `http://mydomain/sso/metadata/`.
2. Choose the Public key and Private key that were uploaded using the data/File model and that will be used to communicate with identity providers. Alternatively, if you want to use a system generated certificate, select the check box and choose the required certificate from the drop-down list. These certificates were added typically using **System Configuration > Certificates** or a similar menu that creates data/certificate instances.
3. Enter the Validity period (in hours) that the metadata is valid for.
4. Enter the number of seconds of the permitted clock drift between VOSS Automate and the Identity Provider. The number of seconds for tolerance is customizable, and this value must be set in accordance with the deployment's security policy. By default, VOSS Automate will use a value of 0 for the clock drift, in other words, assume clocks are exactly in sync.
5. Enter the details of the Contact Person responsible for the metadata.
6. If required, select the **Block unencrypted assertions** check box to raise an error if SAML assertions are not encrypted. If the check box is selected, and there is no encryption in the assertion, then an error message: "Unencrypted assertions are not allowed" is shown.
7. On the **Service Provider Settings** tab, enter a friendly name that will be the ServiceName of the AttributeConsumingService in the metadata.
8. If the **Sign Authn Requests** check box is selected, outgoing messages are signed and the specified private key is used. Drop-down lists are also displayed to select the SignatureMethod (default is `rsa-sha1`) and DigestMethod (default is `sha1`) corresponding with those used by the Identity Provider.
9. If an Identity Provider has `WantAuthnRequestsSigned` set in its metadata, select the check box. The check box is cleared by default.
10. The **Want Assertions Signed** check box determines if assertions should be signed. Do not clear this check box unless the integrity check of assertions is not needed in your environment.
11. The **End Points** section provides an external interface to the service provider in VOSS Automate. The binding determines how SAML requests and responses map onto standard messaging or communications protocols. The Assertion Consumer Service (ACS) receives assertions, while the Single Logout Service is used to log out a user when instructed by an Identity Provider.
 - a. Choose Binding and URL for the Assertion Consumer Service.
 - b. Choose the Binding and URL for the Single Logout Service.

The Saved SSO settings are published by the VOSS 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.

26.5. Renew Single Sign-On Certificate for VOSS Automate

If a customer's Single Sign-on certificate expires, then to renew the certificate for VOSS Automate:

1. Follow the steps to regenerate the certificate (either self-signed or CA signed) as described in *SSO Certificate Management*.
2. Follow the steps to regenerate and upload SP metadata to the IdP described in *Configure Single Sign-On for VOSS Automate*.

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.

26.6. 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.

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>
```


27. Data Sync

27.1. Introduction to Data Sync

27.1.1. Overview

You can perform data syncs from within VOSS Automate or directly on a device. For this reason, cached VOSS Automate data should be periodically synced with data on devices.

Examples:

- When an instance of a Unified CM is added to the system, its data is imported and cached.
- When instances are added, updated, or deleted from the Unified CM, the cached data in VOSS Automate becomes out of sync with data on the device.
- When deleting data from Unified CM before deleting it from VOSS Automate, the system displays the following error: “The specified resource could not be found”

This means the resource is out of sync, and VOSS Automate may need to re-sync with Unified CM in order to delete it or update it.

VOSS Automate data syncs allow you to dynamically synchronize cached VOSS Automate data with data on devices. The data sync instance is associated with the connection parameters of a device type in VOSS Automate.

Supported devices include:

- HCM-F (if installed)
- Cisco Unified CM
- Cisco Unity Connection
- LDAP
- WebEx

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.

To view configured data syncs in a list view in the VOSS Automate Admin Portal, go to (default menus) **Administration Tools > Data Sync**.

The screenshot shows the Voss Automate interface for Data Sync configuration. The table displays the following data:

Name	Description	Device Type	Sync Type	Model Type List	Synchronization Order	Model Instance Filter	Force Refresh On
CMCCS-10.120.9.245-MohFile	Perform a sync of Call Manager Control C...	data/CmCcs	pull	CMCCS_MohFile			true
CMCCS-192.168.100.15-Mo...	Perform a sync of Call Manager Control C...	data/CmCcs	pull	CMCCS_MohFile			true
CMCCS-192.168.100.16-Mo...	Perform a sync of Call Manager Control C...	data/CmCcs	pull	CMCCS_MohFile			true
CMCCS-192.168.100.17-Mo...	Perform a sync of Call Manager Control C...	data/CmCcs	pull	CMCCS_MohFile			true
HcsLdapSchemalImport-1		data/Ldap	pull				
HcsLdapSchemalImport-7		data/Ldap	pull				
HcsLdapSchemalImport-8		data/Ldap	pull				
HcsLdapSchemalImport-9		data/Ldap	pull				
HcsLdapUserPurge-1		data/Ldap	purge_local	HcsSyncldapUserMTL-1			
HcsLdapUserPurge-7		data/Ldap	purge_local	HcsSyncldapUserMTL-7			
HcsLdapUserPurge-8		data/Ldap	purge_local	HcsSyncldapUserMTL-8			

Note: 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.

Related Topics

- Sync Overview in the Best Practices Guide
- Data Sync Types in the Core Feature Guide

27.1.2. Data Sync Settings

The table describes a number of key settings that are available for data sync:

Model Type lists	<p>Define the entities to pull in a given sync. For example:</p> <ul style="list-style-type: none"> • Only pull in <code>device/cucm/User</code> records from Cisco Unified CM.
Model Instance filters	<p>Limit a sync to a subset of entities in a sync. For example:</p> <ul style="list-style-type: none"> • Pull in users with a primary extension starting with <code>1</code>. <p>A system-level administrator will need to expose this setting on the Admin Portal.</p>
Actions	<p>Select which actions are active for a sync (Add/Update/Delete).</p> <ul style="list-style-type: none"> • Update requires more effort to run because this typically involves a GET API call for each record, which must then be compared to VOSS Automate data. • Add/Delete can be determined from the initial list API calls. <p>To save time on the sync, you may wish to disable Update if you only require Add/Delete.</p>
Quick Import	<p>Uses the list API responses to update the VOSS Automate cache, and won't perform individual GET calls for each entity for the update.</p> <p>Recommended when the list response contains all values for the entity, or where only the key settings must be updated.</p> <p>Removing individual GETs speeds up the sync, since VOSS Automate is not waiting for the API responses when there are a many entities to update.</p> <p>This is useful if the list and GET responses are required, or if you only need the summary data from the list view.</p>

Note: Quick Import is generally not recommended, and should be used only for syncing `device/cuc/ImportUser`.

However, *initially* there is an exception to the performance improvement of a Quick Import sync with `device/cuc/User`:

- When quick import is turned on a sync that has previously run without it, dependent, non-Import User model types use the LIST response data to compare with the resource data that was originally saved using the GET response data.
- The data sync detects a change, and initiates a resource save for each instance.
- For `device/cuc/User`, dependent import API calls are made, resulting in a long sync time.
- Once it completes, *subsequent* quick import syncs should show an improvement over non-quick import syncs. When changing back to a non-quick import sync, the same effect would likely be observed.

27.1.3. 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.

27.2. 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 overrides:
 - Model Type: device/notification_service/*
 - * Cache Policy for Reads: Cache

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.

27.3. Data Sync Types

VOSS Automate provides the following data sync types:

Data sync type	Description
Pull from Device	Available to all device types. <ul style="list-style-type: none"> • Pull all data from the device • Pull only the schema from the device (used for LDAP) • Pull data from the Change Notification Feature local data collection
Purge Local Resources	Available to all device types. <ul style="list-style-type: none"> • Purge data from the cache
Push to Device	Available only to Cisco Unified CM devices <ul style="list-style-type: none"> • Push data in the cache to the device
Change Notification Sync	Available only to Cisco Unified CM 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.

Generally, for all sync types, VOSS Automate builds up the lists of entities from both VOSS 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 Unified CM, the ID is the *pkid*, which is the internal Unified CM database ID.

For subscribers, a sync builds up the list of `device/cucm/Users` in VOSS Automate and then requests from the Unified CM the lists of users it currently has for the comparison. Differences in the lists are handled according to each sync type.

Related Topics

- Data Sync Overview in the Core Feature Guide
- Change Notification Feature Overview in the Core Feature Guide

27.3.1. Pull from Device

For sync type *Pull from Device*, the VOSS Automate resource is updated where the same key is present in both lists. In this case, the device data is the master and the VOSS Automate system model data is updated with the device data.

For example, let's say new data is added to the Unified CM, so that the VOSS Automate system data state for a Unified CM `device/cucm/User` does not show instances that are shown on the Unified CM.

In this case, a *pull* data sync synchronizes the system data with the Unified CM data. For example, a user's Department may be updated on the Unified CM, but the update only shows on the system after a *Pull from Device* sync. If a user resource is created in Unified CM but not in VOSS Automate, this adds the `device/cucm/User` instance into VOSS Automate at the level the *pull* sync was run from, for example, at the customer level.

When deleting a VOSS Automate resource from the device, so that the key is in the VOSS Automate list but not in the device list, a *pull* sync removes the resource in VOSS Automate. For example, if the resource is a user in VOSS Automate but not in Unified CM, the *pull* sync removes the `device/cucm/User` record in VOSS Automate.

To restrict the number of records removed in VOSS 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 VOSS 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.

27.3.2. Push to Device

Sync type *Push to Device* is available only to Cisco Unified CM device types.

In a *Push to Device* sync type, devices are synchronized with the VOSS Automate system data state, which is the primary data state.

- When deleting device data from VOSS Automate so that the key is in the *device* list but not in the VOSS Automate list (for example, delete user in VOSS Automate), the user is removed from Unified CM. The user will not exist on the device or on VOSS Automate.
- When adding new device data to VOSS Automate so that the resource shows instances that are not shown on the device, a *push* data sync synchronizes the device data with the VOSS Automate data. For example, adding a `device/cucm/User` instance to VOSS Automate and running a *Push to Device* sync adds the user record to Unified CM.

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 VOSS Automate and on Unified CM, no update occurs in either direction. Detailed settings may still not match after a *Push to Device* sync.

Important: When performing a *push* sync, it is important to consider data dependencies between different models.

For example, data dependencies may exist between users and phones in the Cisco Unified CM. 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 in Cisco Unified CM.

On the other hand, for ownerID on the phone, pushing the phone first will fail since the user isn't in place.

This might mean running the *push* sync multiple times so it loads in the required order, or 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 Unified CM to restores/inactive partitions, the end-state of the relevant pkids may differ to their state the last time VOSS Automate was in sync with Unified CM (before a restore), particularly if testing occurred in between. This means you may, for example, have a user with the same username in both VOSS Automate and Unified CM, but if that user's pkid in Unified CM now differs to the one in VOSS Automate from previous syncs or interactions, they will be seen as different users even though they have the same usernames.

27.3.3. Change Notification Sync

Sync type *Change Notification Sync* is available only to Cisco Unified CM device types.

A *Change Notification Sync* 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.

27.3.4. Purge Local Resources

In a *Purge Local Resources* sync type, 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 CUCM, 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}}

27.4. 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 of the full sync to filter the changes to remove. If a model instance filter is included, no changes are removed.

27.5. Enable a Scheduled Data Sync

This procedure enables the scheduled data sync so that it executes regularly.

Note: Setting up a CUCM or CUC device in VOSS 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](#)
- 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 (default menus) **Administration Tools > Scheduling**.
3. On the **Scheduling** page, 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** check box.
5. Select the **Multiple Executions** tab, and update the interval, as required.
6. Click **Save**.

The full data sync executes immediately, and executes again according to the schedule.

27.6. Manually Run the Default Data Sync

You can always manually run the default data sync when there have been updates to Cisco Unified Communications Manager (CUCM) or Cisco Unity Connection (CUC) devices that need to be synced into VOSS Automate.

Note: Manually running the change notification sync is not supported.

Perform these steps:

1. Log in as provider or reseller administrator.
2. Go to (default menus) **Apps Management > Advanced > Perform Publisher Actions**.
3. From the **Action** drop-down, choose **Import**.
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**.

27.7. Controlling a Data Sync with a Model Type List

Using a Model Type List (MTL), you can control the types of data that are synced into VOSS Automate from devices from vendors, such as:

- Cisco (Unified CM, Unity Connection)
- Microsoft
- Pexip
- Webex

and so on.

Controlling the types of data that are synced can greatly improve sync performance. The MTL is a list of device models associated with the device type, for example, Phone and Line device models that are associated with the Unified CM device.

These are the possible types of Model Type Lists:

- 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 Model Type List attribute results in the subsequent import(s) synchronizing all device models for the corresponding device.

Here is an example of an include MTL:

Model Type List [HCS CUCM Media MTL] Save Delete Help Back Action ▾

Name*

List Type*

Model Types

<input type="checkbox"/>	<input type="text" value="device/cucm/MediaResourceGroup"/>
<input type="checkbox"/>	<input type="text" value="device/cucm/MediaResourceList"/>
<input type="checkbox"/>	<input type="text" value="device/cucm/MohServer"/>
<input type="checkbox"/>	<input type="text" value="device/cucm/MohAudioSource"/>
<input type="checkbox"/>	<input type="text" value="device/cucm/Mtp"/>

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 Unified CM.

It is recommended to define MTLs for sets of data that are being modified on the device directly. An example is Unified CM 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 VOSS Automate can be maintained with better response times and quicker transaction execution.

Note: Some Unified CM device models to avoid unless needed are Users, Phones, and Lines, as there may be large numbers of these in the Unified CM and result in a lengthy data sync operation.

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. This can be done by unchecking the Refresh Existing (Changed) Data check box on the Data Sync configuration page. This check box controls whether existing device model instances are updated in VOSS Automate in addition to importing new instances and removing deleted instances. If checked, all device model instances must be synced and examined. If unchecked, only new and deleted instances need to be imported and the data sync will run considerably faster.

27.8. Create a Targeted Model Type List

If you manage data on vendor devices directly on a regular basis, perhaps for configuration that is not orchestrated from VOSS Automate, such as media resources, it is recommended to create a Model Type List and Data Sync specifically targeting the data items you are managing. This ensures each data sync is highly optimized for the data being changed on the device directly and minimizing the load on VOSS Automate.

To create a targeted Model Type List:

Perform these steps:

1. Log in as Provider level admin or higher.
2. Access the **Model Type List** form (default menu **Administration Tools > Model Type List**) and click **Add**.

3. Specify the name of the Model Type List.

It is recommended to use a naming convention that makes it easy to identify the MTL in a list view, for example “Unified CM 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.

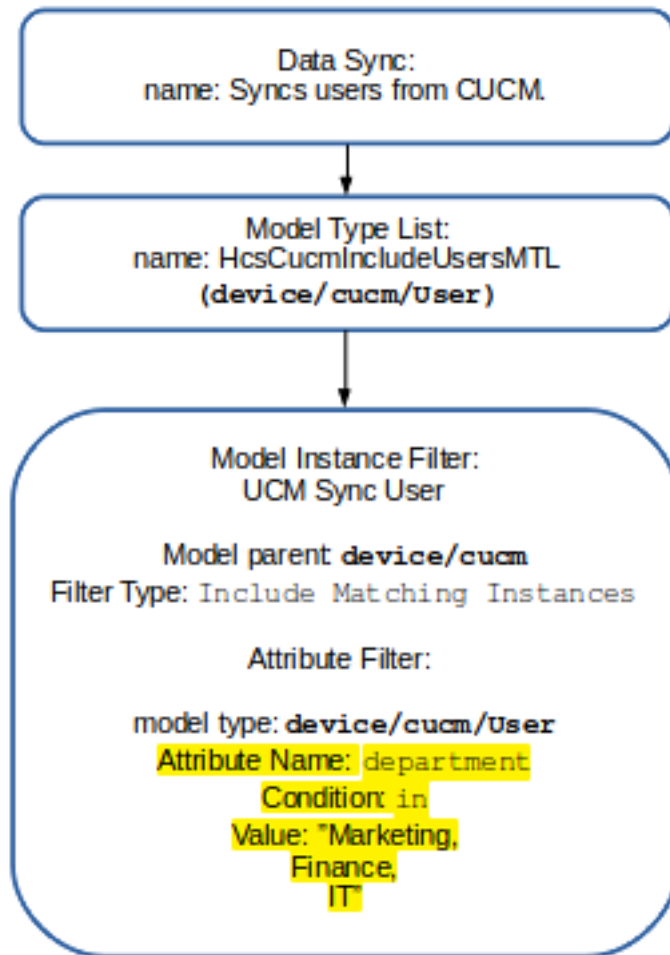
6. Click **Save**.

27.9. Model Instance Filter

The model instance filter (MIF) capability allows 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, that 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



27.9.1. Add a Model Instance Filter

1. Log in as a Provider level administrator and open the **Model Instance Filter** form (default menu **Administration Tools > Model Instance Filter**) to display the list view of existing filters at the corresponding administrator hierarchy.
2. Click **Add** and enter a **Name** for the filter.
3. 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.

4. Choose the type of filter - the inclusion or exclusion of attributes: **Include Matching Instances** or **Exclude Matching Instances**.
5. 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:

- 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”.

- 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.

6. 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

```
</ns0:listUserProfileProvision>
</soapenv:Body>
</soapenv:Envelope>
```

RESPONSE:

(continues on next page)

(continued from previous page)

```
<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>
      </return>
    </ns:listUserProfileProvisionResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

27.9.2. Common Use of Model Instance Filters

While model instance filters can be used on any sync type, their common uses are:

- On add syncs - to retrieve a subset of records from the underlying device into VOSS Automate. For example, to limit the users pulled from LDAP, from UCM, and so on.
- On delete/purge sync - to target specific records for removal in a purge or delete sync. For example, to purge a subset of users from VOSS Automate that were inadvertently pulled in.

Note: Model Instance filters do not work with Cisco UCM Change Notification sync types. If a model instance filter is needed for a UCM element, this model type should be excluded from the change notification sync and a separate sync should be set up for this.

27.9.3. 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}}>
```

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**.

27.10. Model Instance Filter Examples

1. A MIF with multiple Model Filter entries to match criteria on different model types:

The screenshot displays the configuration for a Model Instance Filter (MIF) named "UCM Sync User and Phone Criteria". The configuration is as follows:

- Name*:** UCM Sync User and Phone Criteria
- Model Parent:** device/cucm
- Filter Type*:** Include Matching Instances

The MIF contains two entries in the **Model Filters** list:

- Model Type*:** device/cucm/User
 - Attribute Filters:**
 - Attribute Name*:** department
 - Condition*:** In
 - Values:** Marketing, Finance, IT
- Model Type*:** device/cucm/Phone
 - Attribute Filters:**
 - Attribute Name*:** product
 - Condition*:** Equals
 - Value:** Cisco 7940

This 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”.

2. A MIF with multiple Model Filter entries with the same model type and macros to create a list of records to match

The image displays two screenshots of a Model Instance Filter configuration interface. Both screenshots show the 'Model Type*' dropdown set to 'device/cucm/User' and the 'Attribute Filters' section expanded to show a single filter entry.

Top Screenshot:

- Model Type*: device/cucm/User
- Attribute Name*: telephoneNumber
- Condition*: Equals
- Value: `((fn.containsIgnoreCase +1,input.telephoneNumber == True)) <{{input.tel`

Bottom Screenshot:

- Model Type*: device/cucm/User
- Attribute Name*: telephoneNumber
- Condition*: Equals
- Value: `((fn.containsIgnoreCase +27,input.telephoneNumber == True)) <{{input.tel`

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.

3. A MIF with multiple attribute filters applied to the same model type

Model Type*

Attribute Filters

Attribute Name*

Condition*

Values

Attribute Name*

Condition*

Value

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.

27.11. View List of Device Models

Use this procedure to see the device models available to use in Model Type Lists for custom data syncs from vendor devices.

Perform these steps:

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`

- 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 Model Type List, use the format: `device/<device_type>/<device_model>`, for example, `device/cucm/BillingServer`.

27.12. Create a Custom Data Sync

Create a custom data sync to use a targeted Model Type List.

Perform these steps:

- Log in as provider admin or higher.
- Choose **Administration Tools > Data Sync**.
- Click **Add**.
- Enter the name of 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 Unified Communications Manager, and `DS` stands for Data Sync. You could also include the type of data included in the sync, such as `C1Pull-CUCM01-MediaResources-DS`.

- From the **Device Type** drop-down, choose the Device Type you are syncing from.
- From the **Sync Type** drop-down, choose **Pull from Device**.
- From the **Dependency Resolution** drop-down, choose **Default**.
- Select the **Execute Asynchronously** and **Refresh Existing (Changed) Data** check boxes.
Execute Asynchronously means that the sync request will return a reply before its 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.
- Select the **Force Refresh of Data** check box 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.
- From the **Model Type List** drop-down, choose the targeted Model Type List you defined earlier.
- Leave **Synchronization Order** and **Model Instance Filter** blank.
- Click + next to **Device Filters** to add an entry to the list.
 - From the **Attribute Name** drop-down, choose **host**.
 - From the **Condition** drop-down, choose **Equals**.
 - 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.
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**.

27.13. Unified CM Change Notification Feature Alerts

The Unified CM Change Notification Feature (CNF) is enabled to display alerts. You don't have to configure the change notification feature alerts manually in the VOSS Automate. The administrator gets the alerts when something goes wrong with the collector process.

The administrators can view the alerts at the hierarchy level they log in and all the levels below that hierarchy. For example, if an alert is raised at the customer level (sys.hcs.provider.reseller.customer), then the provider, reseller, and customer administrators can see that alert but not site administrator. A Site administrator doesn't have access to view the alert. All the administrators have read and delete permissions to the alerts.

When a change notification feature alert is raised, the Messages indicator on the VOSS Automate Admin Portal shows the alert. Clicking the **Messages** or **Notifications** button on the toolbar shows a pop-up and a message that alerts have been raised. Clicking on the message, the user is navigated to the list of alert messages on the **Alerts** list view (default menu **Administration Tools > Alerts**).

CNF alerts have the following distinct 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
- Category: The category of the alert - Device Change Notification Collector
- Severity: VOSS 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.

VOSS Automate displays change notification feature 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 {}.
 - 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 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 VOSS Automate. We strongly recommend removing the alert after resolving it.

27.14. Change Notification Sync

27.14.1. Introduction to Change Notification Sync

The VOSS Automate interaction with the UCM Change notification sync has two primary components:

- Data Collector - collects the changes from the Cisco Unified CM and updates the VOSS cache on the configured frequency (defaults to every 300 seconds). This collector must be enabled to collect the changes, otherwise the sync will not process any changes.
- Change Notification Sync - this is a type of sync that processes the changes the collector puts into the VOSS cache. A scheduled sync should be set up and enabled so that the changes are processed within a reasonable period. The sync can also be run adhoc if required around the schedule.

The VOSS Automate data collector retrieves the change records from the Cisco Unified CM on the configured interval. For example, this could be every 300 seconds (5 minutes) which is the default. When a Change Notification Sync type is run, VOSS Automate processes the change records collected. VOSS Automate then processes the records accordingly:

- Add - will do a GET API call to retrieve the full record and add it to VOSS Automate.
- Update - will do a GET API call to retrieve the full record and update the record in VOSS Automate.
- Del - will remove the record from VOSS Automate.

The efficiency on these Update syncs is because there is no need to do a GET API call for every single record in the system - only for those that changed. In large UC application installations, this can make a big difference in Update sync times.

For example, with a data collector polling period of 300 seconds and a CNF sync scheduled for every 24 hours, the process would work as follows:

- Every 300 seconds (5 minutes) the polling collector would get all the current changes from Cisco Unified CM.
- This polling would repeat every 5 minutes - updating the VOSS Automate cache.
- After 24 hours, the CNF sync would run and process all the changes VOSS Automate stored over that 24hr period. The duration of this sync will depend on the number of changes to process, since each requires an AXL GET API request.

This type of sync, especially for updates, is far more efficient, because a GET AXL request for every object in the system is not required - only for those that changed in the time between syncs.

On a system with 10000 users for example, if 100 of the users were changed, then only 100 GET AXL request are needed. By contrast, a normal sync doing an update would require 10000 GET AXL requests to update the same 100 users.

The VOSS Automate data collection can store up to 200,000 changes from a single Cisco Unified CM Cluster. A warning is raised when 75% of the data collection storage capacity is reached. When the 200,000 changes capacity for a cluster is reached, a sync error occurs on the user interface (see [Errors and Troubleshooting Change Notification Processes](#)) To avoid the sync error, we recommend always having a scheduled CNF sync running on a regular basis based on your needs when Change Notification is enabled.

27.14.2. Setup to Enable or Disable CNF for a Cisco Unified CM Cluster

The following steps are a checklist to enable change notification for a Cisco Unified CM cluster in VOSS Automate.

1. Ensure the Service is enabled and configured in Cisco Unified CM. ([Cisco Unified CM Setup to use CNF](#))
2. Enable Change Notification on the Cisco Unified CM cluster in VOSS Automate. ([VOSS Automate Change Notification Functionality](#))
3. Review the detailed Change Notification settings for the cluster. ([VOSS Automate Change Notification Functionality](#))
4. Review or create the required Data Sync instances for change notification for the cluster. Refer to the topics on Data Sync following [Introduction to Data Sync](#).

The 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 above and activate the schedule(s). ([Enable a Scheduled Data Sync](#))

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 setup to be complete.

Follow the steps in reverse in order to disable change notification for the cluster.

27.14.3. Detailed Cisco Unified CM CNF Functionality

The change notification capability supports all the objects that are available via AXL. In general, this means that everything VOSS Automate can manage in Cisco Unified CM will be available via change notification.

Data that VOSS Automate pulls from Cisco Unified CM 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 VOSS 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 Unified CM, 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 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 VOSS Automate when polling is enabled is 300 seconds but it can be modified to be longer (up to 7200 seconds) as desired.

Cisco Unified CM Setup to use CNF

There are two settings in the Cisco Unified CM to check and update to ensure Change Notification 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.

27.14.4. VOSS Automate Change Notification Functionality

This section provides more details on the functionality of the Change Notification Feature (CNF) components in VOSS 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.

- A **Model Type List** (MTL) can be set up and selected to be associated with CUCM 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.

VOSS Automate Setup to enable Change Notification

Enabling the Change Notification capability is completed on a per UCM Cluster basis. This can be done on the 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. The schedule will be 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 UCM Cluster should be executed just before or after enabling Change Notification 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).

27.14.5. Errors and Troubleshooting Change Notification Processes

A number of scenarios may result in error conditions in the change notification process. The VOSS Automate system is enabled to display alerts automatically in this case, so that it is not necessary to configure the change notification feature (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 change notification feature alert is raised, the Notifications indicator on the VOSS Automate Admin Portal shows the alert. Clicking the Notifications button shows a pop-up and a message that alerts have been raised. By clicking on the message, users are directed to the list of alert messages which can also be accessed via the menu under **Administration Tools > Alerts**.

CNF alerts have the following distinct 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: VOSS 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.

VOSS Automate displays change notification feature 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 {}.
 - 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 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 VOSS Automate. We strongly recommend removing the alert after resolving it.

Change Cache Full on Cisco Unified CM

If the Cisco Unified CM maximum number of stored change records is exceeded (see detailed Cisco Unified CM functionality section for more details on the limit and configuration) then the Cisco Unified CM will drop the oldest changes that have not been collected. This can happen if the polling time in VOSS Automate is set up to be too long or the Cisco Unified CM is experiencing a very high level of changes (see the detailed VOSS Automate functionality section for more details on polling configuration). When this situation occurs, VOSS Automate will get an error on polling and will try to recover. This activity is logged as an Alert in the system and provides the outcome - recovery was successful (alert code 40001 or 40002) or recovery was not successful (alert code 40005).

In the event the recovery was successful, you may want to review and consider a full sync as some changes would have been lost (the oldest changes in the Cisco Unified CM cache).

In the event the recovery was not successful, then a full sync is required to update and to get change notification functioning again. The full sync is needed as changes would have been missed from the Cisco Unified CM and we need to be at a clean sync in order to start processes 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 {}"

VOSS Automate Change Collection full for a Cisco Unified CM cluster

If the VOSS Automate change collection for a given Cisco Unified CM 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 Unified CM until some of the pending changes are processed. This can be carried out by an administrator executing a sync for that Cisco Unified CM 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.

Other errors

The other error codes listed for the alerts are more internal in nature and should result in a VOSS support ticket being raised for further investigation.

28. Self Service Administration

28.1. 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.

28.2. Self Service Feature Display Policy

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 Interface. These are typically available on both the Button Bar 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 VOSS 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 **Subscriber Management > Subscribers** 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 check box is no longer applicable.

In a similar way, select the appropriate check boxes 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** check box controls the user self-service user interface. 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.

28.3. 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.

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.

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.

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	cucalttext_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.

28.4. End User Access and Authentication

A user can log into 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. 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 an 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 Unified Communications applications) use the same authentication method.

28.5. Themes and Branding

The Self Service GUI 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”.

28.6. 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”.

28.7. 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".

28.8. 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.

28.9. 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.

28.10. 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".

29. Self Provisioning

29.1. Introduction to Self-Provisioning

The Cisco Unified Communications Manager (CUCM) Self-Provisioning feature allows an end user or administrator to add an un-provisioned phone to a CUCM 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 Cisco Unified Communications Manager 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 VOSS Automate, the user, line, and phone must be at the site level in the VOSS Automate hierarchy.

29.2. Bottom-Up User Management

A bottom-up approach to user management means users are configured on Cisco Unified Communications Manager (Unified CM) and synced into VOSS Automate. Two possible methods for bottom-up user management are:

- Sync LDAP directory into Unified CM. Do not configure the LDAP directory sync in Unified CM 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 VOSS Automate, using a line mask, universal line template, and self-provisioning user profile at the site level.

Note:

During LDAP sync to Unified CM, 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 VOSS Automate to get applied, the User Profile assigned previously must be empty or it must be named the 'Standard (Factory Default) User Profile'.

- Use Unified CM Quick User/Phone Add to create a user and the user's primary extension.

29.3. Top-Down User Management

A top-down approach to user management means users and lines are configured on VOSS Automate and pushed into Cisco Unified Communications Manager (Unified CM). Users may be added via LDAP sync, the Admin Portal, or bulk loading. When users are pushed to Unified CM 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 VOSS 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 Add Subscriber.

Note: You can associate multiple devices (Jabber, iPhone, iPad, 78xx series IP phones, and 88xx series IP phones) to a single subscriber through VOSS Automate (Subscriber Management > Subscribers). This cannot be done through Quick Add Subscriber (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 Add Subscriber 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 Add Subscriber). If a primary extension is already assigned, the line mask is not applied.

29.4. CUCM 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 Unified Communications Manager (CUCM):

- Ensure that the Cisco CallManager, 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 Unified Communications Manager documentation for details.

29.5. Site Configuration for Self-Provisioning

Regardless of whether top-down or bottom-up user management is used, ensure that the following items have been configured in VOSS Automate:

Enterprise deployment:

- Site Defaults: **Site Management > Defaults**
- Internal Number Inventory: **Internal Number Inventory Management > Internal Number Inventory**

Provider deployment:

- Site Dial Plan: **Dial Plan Management > Site > Dial Plan**
- Site Defaults: **Site Management > Defaults**
- Directory Number Inventory: **Dial Plan Management > Customer Management > Add Directory Number Inventory**

29.6. 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 Unified Communications Manager.

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.

Perform these steps:

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 Profiles. 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](#).

29.7. Specify the Primary Line per Subscriber

In the top-down method that uses Quick Add Subscriber, 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 Subscriber, add at least one line, and select the Self-Service ID check box.

29.8. Add a Self-Provisioning Universal Device Template

When the administrator or user self-provisions a phone, Cisco Unified Communications Manager 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.

Perform these steps:

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. Choose **User Management > Self-Provisioning > 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

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 Pre-emption	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**.

29.9. 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. 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.

Perform these steps:

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. Choose **User Management > Self-Provisioning > 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. Enter other optional settings, if applicable.
7. Click **Save**.

29.10. Add a Self-Provisioning User Profile

Perform these steps:

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. Choose **User Management > Self-Provisioning > 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. Click the **Device Template Desk Phone** tab.
 - a. Click '+' 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** check box.
 - e. From the **Calling Search Space** drop-down, choose the appropriate option, for example Cu2Si4-InternalOnly-CSS.
7. Click 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. Enter other optional settings, if applicable.

Next Steps

Set a Default User Profile for a Site.

29.11. 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.

Perform these steps:

1. Choose **Site Management > 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**.

29.12. Add Self-Provisioning Line Mask

Perform these steps:

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. Choose **User Management > Self-Provisioning > Line Mask** (default).
4. Click **Add**.
5. Provide the following information:

Field	Description
Description	A description of the Line Mask.
User Attribute*	Select the user attribute used to generate the user's primary extension. The default is 'telephoneNumber'. This field is mandatory.
Mask*	Provide a mask which gets applied 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. This field is mandatory.

6. Click **Save**.

30. Advanced Tools for System Administrators

30.1. Custom Variables

30.1.1. 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**.

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
```

30.2. Model Report

30.2.1. Create Model Report

System and advanced administrators 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.

Reports for a hierarchy can be created, listed, viewed and deleted. Note that the relation data type is not shown, 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. Choose **Advanced Tools > Model Report > 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
 - HCM-F Models (only if HCM-F is installed)
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, choose **Advanced Tools > Model Report > 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**.

30.2.2. 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**.

31. Appendix: Business Admin Portal Configuration

31.1. Introduction to Business Admin Portal Configuration

In VOSS Automate version 19.1.1 (or higher), a number of mechanisms are introduced to allow the Business Admin Portal (BAP) to be customized for different customers and even different roles within an organization.

The following aspects of the portal can be customized

- Role based access control (see: *Business Admin Portal Profiles*)
 - Access to features (menu items)
 - Access to MACDs / Day 2 functions
 - Access to dashboard widgets (charts etc.)
- Look and feel (see: *Manage Themes (Admin Portal and Business Admin Portal)*)
 - Branding / theming
 - Field visibility, order, title and help text
- Configuration Templates
 - Subscriber Profiles (service profiles) (See Subscriber Profiles in the Core Feature Guide)
 - Available phone types with related configuration (see: *Phone Configuration Mapping*)
 - Line templates
- User level customization
 - Saved searches
 - UI user preferences

For all of the above, default profiles and templates have been created and will be added to the system during an upgrade to 19.1.1 (or higher).

In previous versions of VOSS Automate, BAP was disabled by default and needed to be enabled. In 19.1.1 (or higher) however, BAP will be enabled by default and must specifically be disabled if so required.

It is important that the defaults are reviewed and if required, be cloned (overridden) and amended to fit the requirements of the deployment.

31.2. Custom Icon Names Reference

This reference refers to the icons associated with the **Icon** name drop-downs in the interface.

Go to: <https://fonts.google.com/icons?selected=Material+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.

32. Appendix: Optional Features

32.1. Dial Plan Management

32.1.1. Configure the Dial Plan Management Menu Layout

1. Login as an administrator with sufficient rights to change menu layouts.
2. Click **Role Based Access > Menu Layouts**.
3. Select the required menu.
4. Configure the menu layout as shown below under **Dial Plan Management**.
5. Click **Save**.

Title	Type	Href	Display As
Dial Plan Management			List
Dial Plan Maintenance		/api/view/DP_MaintenanceVIEW/add	Form
Dial Plan Viewer	relation/DP_REL		List
Delete Dial Plan Model		/api/view/DP_DeleteDialPlanModel/add	Form
Dial Plan Input Data			List
• Global Data	data/DP_GlobalDialPlanData		List
• Site Level Data	ata/DP_SiteDialPlanData		List
Dial Plan Models			List
• Dial Plan Models	data/DP_DialPlan		List
• 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

Title	Type	Href	Display As
Dial Plan Models (Continued)			List
• Calling Party Transformations	data/DP_Calling_Party_Transformation		List
• SIP Route Patterns	data/DP_SIPRoutePattern		List
• Calling Space Search	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

See also **Dial Plan Management Menu Layout** illustration:

	Title	Type	Href	Field Display Policy	Configuration Template	Display As	Filter Options	Menu Items
☰ ☱ ⏴	Dial Plan Maintenance		/api/view/DP_Maintenance			Form	More...	More...
☰ ⏴ ⏵	Dial Plan Viewer	relation/DP_REL				List	More...	More...
☰ ⏴ ⏵	Delete Dial Plan Model		/api/view/DP_DeleteDialPl			Form	More...	More...
☰ ⏴ ⏵	Dial Plan Input Data					List	More...	More...
☰ ⏴ ⏵	Dial Plan Models					List	More...	More...
☰ ⏴ ⏵	Dial Plan Log	data/DP_DialPlanLog				List	More...	More...

⊞
↕
Dial Plan Input Data
▼
▼
▼
▼
List
More...
Less...

Menu Items

Menu Items

	Title	Type	Href	Field Display Policy	Configuration Template	Display As	Filter Options
⊞ ⊞ ⊞	Global Data	data/DP_GlobalDialPlanDa	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Site level Data	data/DP_SiteDialPlanData	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...

⊞
↕
Dial Plan Models
▼
▼
▼
List
More...
Less...

Menu Items

Menu Items

	Title	Type	Href	Field Display Policy	Configuration Template	Display As	Filter Options
⊞ ⊞ ⊞	Dial Plan Models	data/DP_DialPlan	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Device Pool - Region - Locatio	data/DP_DP-Reg-Loc	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Conference Bridge	data/DP_ConfBridge	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Media Resource Group List	data/DP_MediaResourceG	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	SIP Trunks	data/DP_SIPTrunk	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	CTI Route Points	data/DP_CTIRoutePoint	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Route Groups	data/DP_RouteGroup	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Route Lists	data/DP_RouteList	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Route Patterns	data/DP_RoutePattern	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Translation Patterns	data/DP_TransPattern	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Called Party Transformations	data/DP_CalledParty_Tran	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Calling Party Transformations	data/DP_CallingParty_Tran	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	SIP Route Patterns	data/DP_SIPRoutePattern	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Calling Search Space	data/DP_Css	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Transcoders	data/DP_Transcoder	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Time Periods	data/DP_TimePeriod	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Time Schedules	data/DP_TimeSchedule	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Media Resource Group	data/DP_MediaResourceG	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...
⊞ ⊞	Partitions	data/DP_Partition	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	List	More...

32.1.2. Access Profile Changes

1. Login as an administrator with sufficient rights to change access profiles.
2. Click **Role Based Access > 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
- 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**.

32.2. Unity SIP Integration

32.2.1. Configure the Unity SIP Integration Menu Layout

1. Login as an administrator with sufficient rights to change menu layouts.
2. Click **Role Based Access > Menu Layouts**.
3. Select the required menu.
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/GlobalSIPVMDPPProfile		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:

Title	Type	Href	Field Display Policy	Configuration Template	Display As	Filter Options	Menu Items
Integrate Unity-CallManag		/api/view/GlobalSIPVMInte			Form	More...	More...
Remove Integrate Unity-Ci		/api/view/GlobalSIPVMInte			Form	More...	More...
Dial Plan Profile	data/GlobalSIPVMDPPri				List	More...	More...
Integration Log	data/GlobalSIPVMLog				List	More...	More...
Unity Tenant Management					List	More...	Less...

Title	Type	Href	Field Display Policy	Configuration Template	Display As	Filter Options
Unity Tenant Add		/api/View/UnityTenantAdd/ad			Form	More...
Unity Tenant Delete		/api/View/UnityTenantDelete/			Form	More...

32.2.2. Access Profile Changes

1. Login as an administrator with sufficient rights to change access profiles.
2. Click **Role Based Access > 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/GlobalSIPVMDPPProfile
 - Permitted Operations: Create, Delete, Read, Tag, Update
 - Permitted Type: data/GlobalSIPVMLog
 - Permitted Operations: Read, Tag
6. Click **Save**.

32.3. Phone Based Registration

32.3.1. Introduction to Phone Based Registration

This section describes the installation, configuration, operation, and troubleshooting procedures for VOSS Automate's Phone Based Registration (PBR) feature.

Phone Based Registration 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.

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.

Related Topics

- [Add Phone Based Registration to Menus](#)
- [Create a restricted API Role and Admin user](#)
- [Install the Phone Based Registration Web Service](#)
- [Configure Phone Based Registration](#)
- [Configure a Cisco Unified CM for Phone Based Registration](#)
- [Phone Based Provisioning](#)

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 follows:

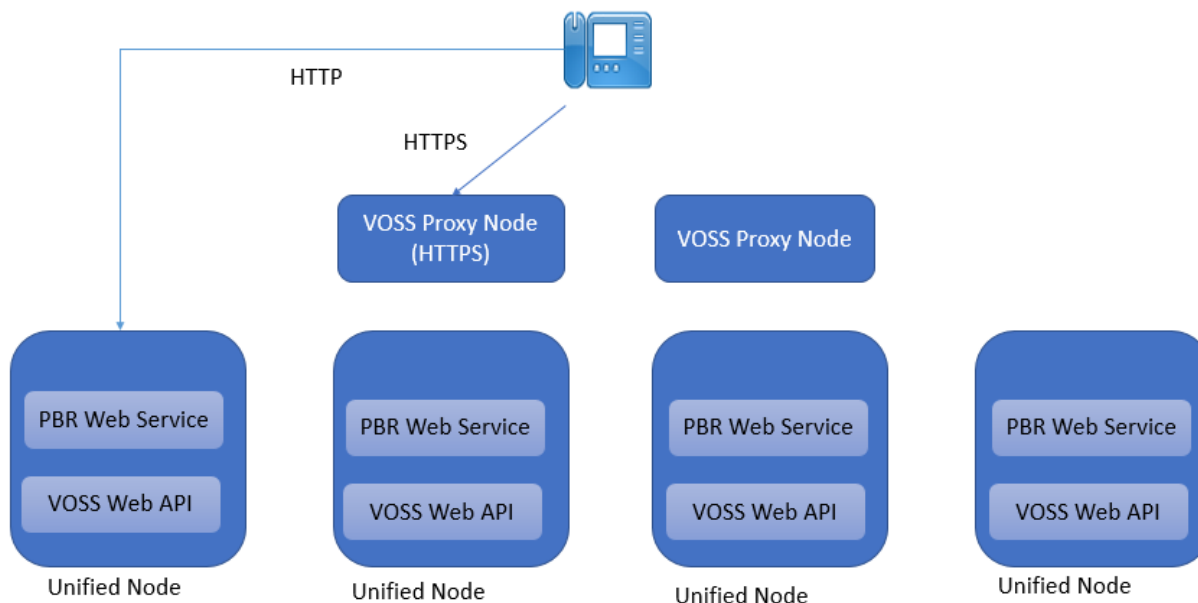


Figure 1: Phone Based Registration Network Connectivity

Prepare to Install and Operate PBR

You will need to prepare the following to install and operate the Phone Based Registration:

- 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: Phone Based Registration Network ports

Note that either HTTP or HTTPS is used on a per customer basis. The choice depends on:

- Security requirements, e.g. 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 Cisco Call Managers that make use of the Phone Based Registration service.

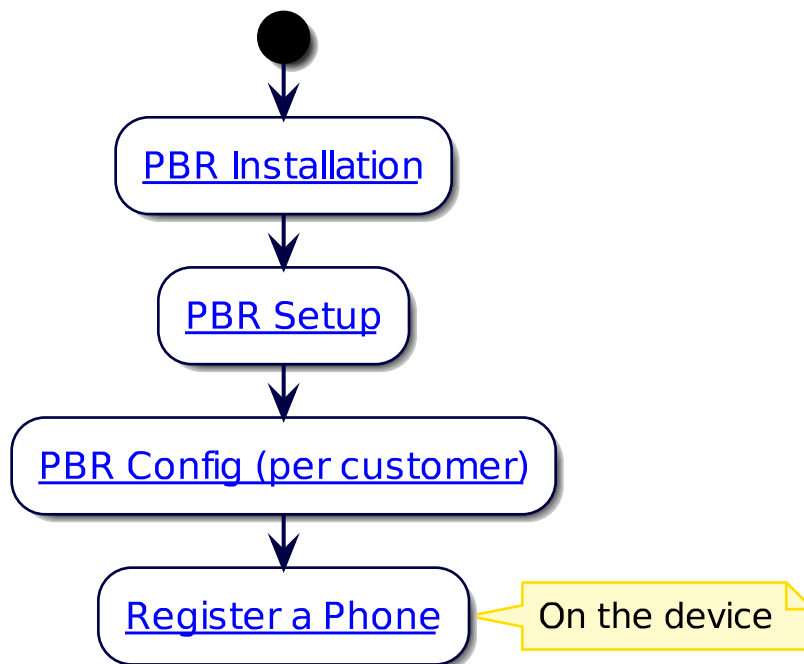
The VOSS Automate Platform certificate needs to be copied from the VOSS Automate server and uploaded to CUCM.

1. Log in to VOSS Automate using Firefox or Chrome. In the URL click on the 'Lock' symbol and choose to view the Certificate. Find the 'Copy To' or 'Export' option depending on your browser and save the certificate file to your PC.
2. Log in to VOSS Automate using the "Cisco Unified OS Administration" login. Browse to **Security > Certificate Management** and upload the Certificate with the Certificate Purpose set to 'tomcat-trust'. Restart the Cisco service as per the instructions.

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.

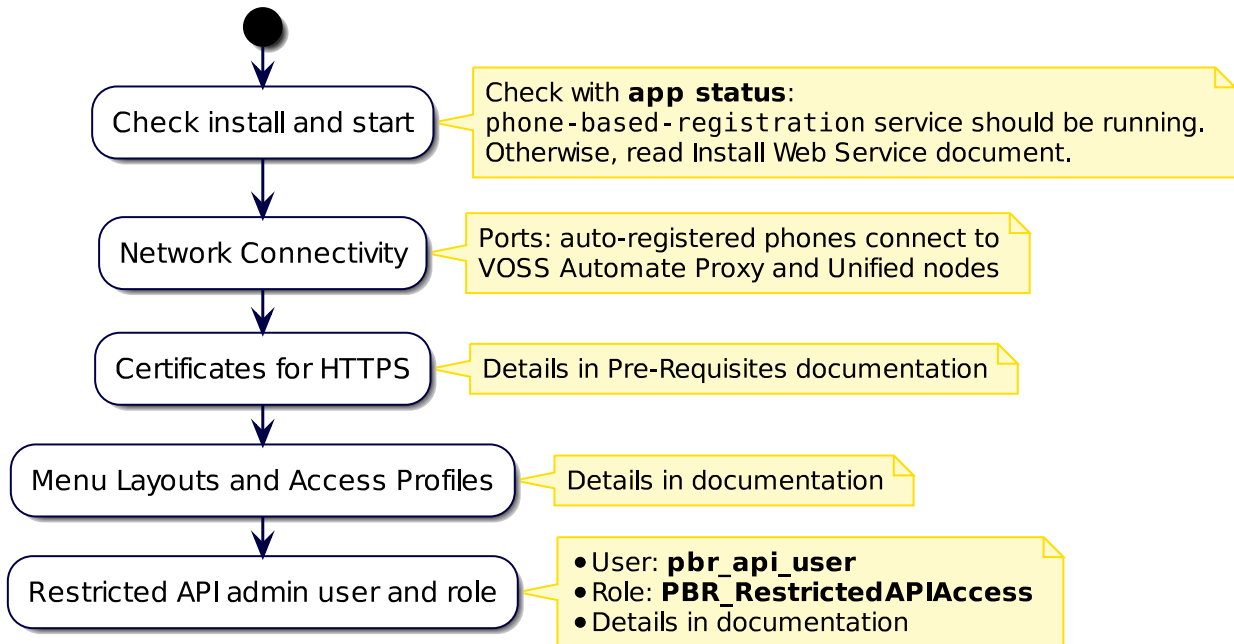
Phone Based Registration Workflows

High-level workflow



Documentation: *Introduction to Phone Based Registration*

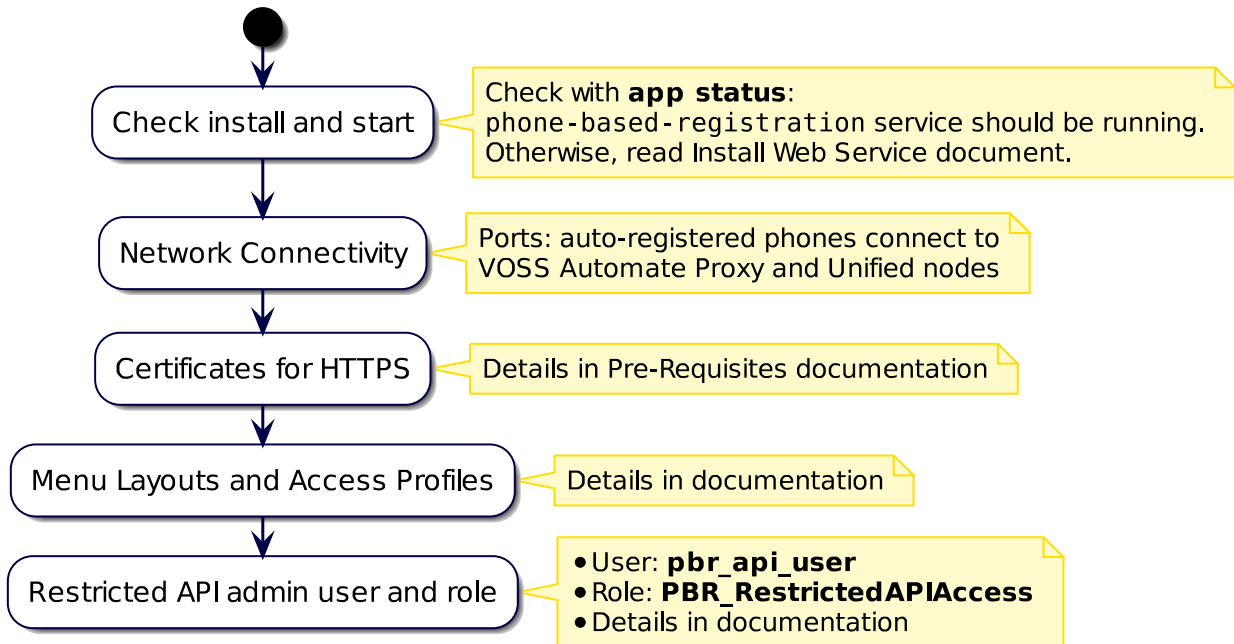
Install PBR



Documentation:

- *Prepare to Install and Operate PBR*
- *Install the Phone Based Registration Web Service*
- *Add Phone Based Registration to Menus*
- *Create a restricted API Role and Admin user*
- *Menu Layout and Access Profiles*

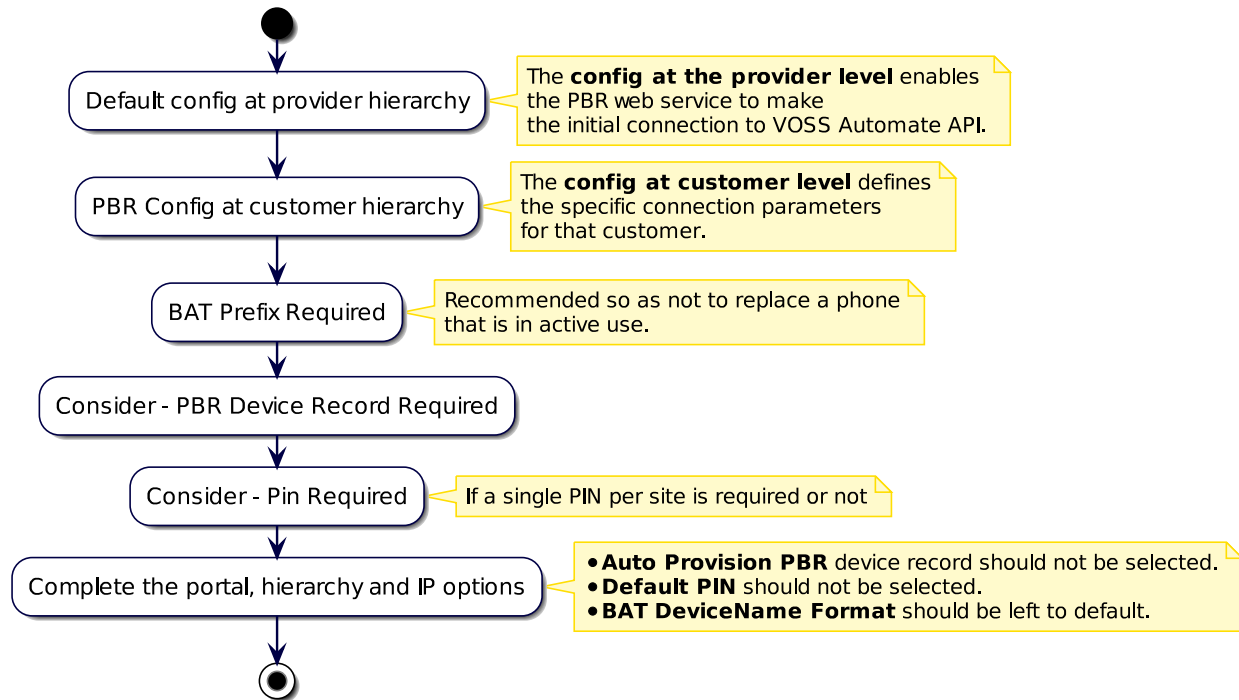
Set up PBR



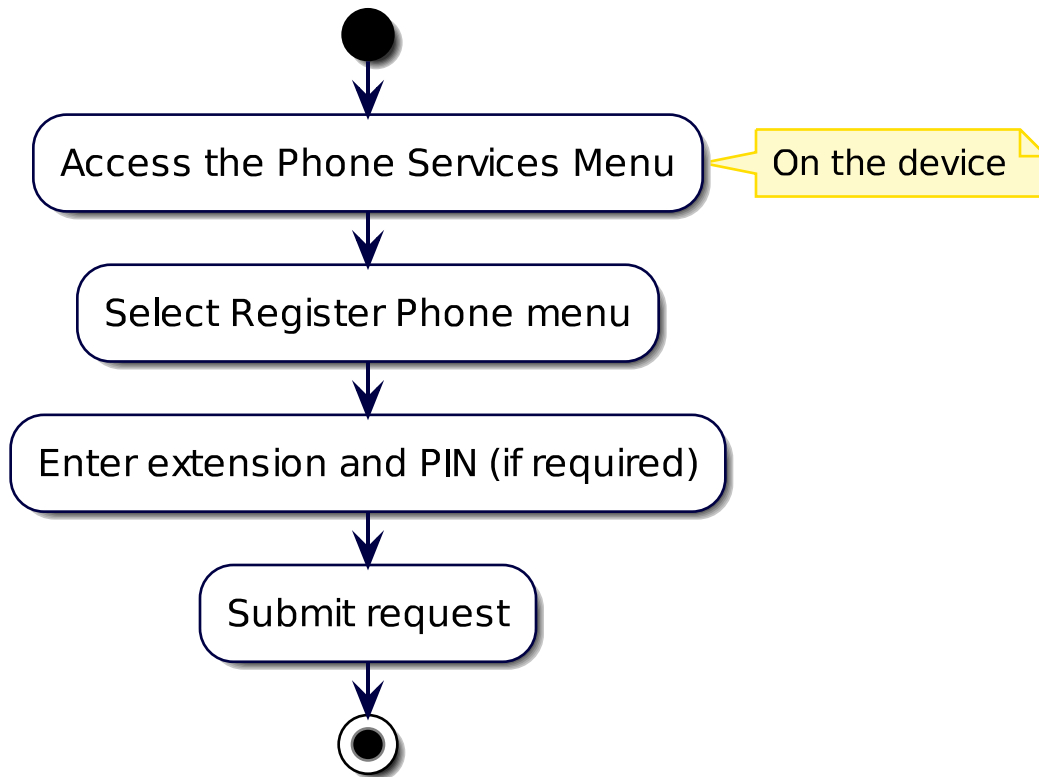
Documentation:

- [Configure a Cisco Unified CM for Phone Based Registration](#)
- When customizing Auto Registration on CUCM, see also [Configure a Cisco Unified CM for Phone Based Registration](#)

PBR configuration (per customer)



Documentation: [Configure Phone Based Registration](#)

Register a phone

Documentation: [Detail Phone Based Provisioning Steps](#)

32.3.2. Add Phone Based Registration to Menus

Phone Based Registration (PBR) must be added to the menu layouts for Provider and Customer administrators that require access to the feature.

The simplest mechanism 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 VOSS GS team to create a customized version that includes current modifications.

A detailed description of the items to expose can be found in [Menu Layout and Access Profiles](#). 1.

▶ Subscriber Management	
--- Lines	
--- Agent Lines	
--- Phones	
--- Subscribers	▶ Phone-Based Registration*
--- Quick Add Subscriber	
--- Quick Add Subscriber Groups	--- PBR Set-Up
--- Smart Add Phone	--- PBR Config
--- Reset UC Passwords	--- PBR phonereg IP Phone Service
--- Voicemail	--- PBR UDT Templates
--- WebEx	--- PBR ULT Templates
--- PLAR (Hotdial)	--- CUCM CallManagers
--- Hunt Groups	--- CUCM CallManager Groups
--- Call Pickup Groups	--- AutoRegistration Phone Protocol
--- PBR Phones & PINs*	
--- PBR Register Phone**	--- Auto Reg Phones

Figure 2: Sample Menu layouts for Phone Based Registration Add-On

Related Topics

- [Introduction to Phone Based Registration](#)

32.3.3. Create a restricted API Role and Admin user

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.

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

The screenshot shows a web interface for managing user roles. The title is "User Roles [PBR_RestrictedAPIAccess]". There are navigation buttons: "Save", "Delete", "Help", "Back", and "Action". Below the title, there are two tabs: "Base" and "Rules", with "Rules" selected. The main form contains the following fields:

Name*	PBR_RestrictedAPIAccess
Description	
Menu Layout	RS_PBR_Restricted_Menu
Theme	default
Access Profile*	RS_PBR_RestrictedAPIAccess
Interface*	Administration
Landing Page	
Self Service Links	

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.

Administration Users [pbr_api_user]		Save	Delete	Help	Back	Action ▾
Base	Account Information					
User Name*	<input type="text" value="pbr_api_user"/>					
Email Address	<input type="text" value="pbr_api_user@cc-p.com"/>					
First Name	<input type="text"/>					
Last Name	<input type="text"/>					
Password	<input type="password" value="*****"/>					
Repeat Password	<input type="password" value="*****"/>					
Role*	<input type="text" value="PBR_RestrictedAPIAccess"/>					
Language	<input type="text" value="English"/>					
Set by Default Language	<input checked="" type="checkbox"/>					

Figure 4: Sample Restricted API Access user

Related Topics

- [Introduction to Phone Based Registration](#)

32.3.4. Install the Phone Based Registration Web Service

Note that a full service restart is initiated on initial startup of the phone-based-registration (PBR) web service on each VOSS Automate unified node.

Note: Prior to running the following commands, ensure the last used ISO image is mounted with:

```
system mount
```

- *On a cluster:*

1. On a *standard* topology, log in to *each node* serially and run `app install phone-based-registration`.

On a *scalable 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
```

- *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
```

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
    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
```

Related Topics

- [Introduction to Phone Based Registration](#)

32.3.5. Configure Phone Based Registration

The Phone Based Registration (PBR) feature supports a number of configuration parameters that manage how the service operates in a specific provider or customer environment. This configuration is implemented using the **Services > Phone Based Registration > PBR Config** menu item.

- A single PBR config record **MUST** be created globally at provider level.
- A PBR config record must be created for each customer that will utilize the phone based registration add-on.

- The config at the provider level is there to enable the PBR web service to make initial connection to VOSS Automate API.
- The config at customer level defines the specific connection parameters for that customer and eventually will allow per customer VOSS Automate user to be used.

The screenshot shows the 'PBR Config [Default]' configuration page. The left sidebar contains a navigation menu with options like Role Management, Audit, Customizations, Dial Plan Management, Subscriber Management, and Services. The main content area displays the following configuration fields:

- Name*: Default
- BAT Prefix Required*:
- BAT DeviceName Format: SEP
- Auto Provision PBR*:
- Pin Required*:
- UseSiteWidePin*:
- Default Pin:
- PBR Device Record Required*:
- Phone Registration Portal Address: 172.30.11.126
- Phone Registration Portal Port: 443
- Phone Registration Portal API User*: flexcorp_pbr_api_user@flexcorp.com
- Phone Registration Portal API Password*:
- Repeat Phone Registration Portal API Password*:
- Phone Registration service Hierarchy: sys.hcs.CC-P.FlexCorp
- CUCM IP: 172.30.11.130

Configuration is on VOSS Automate user interface:

The screenshot shows the 'PBR Config' table in the VOSS Automate user interface. The table has the following columns: Name, BAT Prefix Required, Auto Provision PBR, Pin Required, and Hierarchy. The table contains three records:

Name	BAT Prefix Required	Auto Provision PBR	Pin Required	Hierarchy
Default	true		true	sys.hcs.CC-P
Default	true		true	sys.hcs.CC-P.FlexCorp
Default	true		true	sys.hcs.CC-P.AcmeCorp

Figure 5: Sample PBR Config record

When configuring the PBR service for a specific hierarchy the following considerations are important:

1. VOSS recommends 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.

Select the **BAT Prefix Required** check box.
2. Is the use of PBR Device records required in this environment?
 - a. The PBR device record provides a mechanism for administrators to explicitly specify that a device is eligible for phone based registration.

Select the **PBR Device Record Required** check box if this is desired.

- b. The PBR device record allows the administrator to specify a PIN that should be used when performing phone based registration for a specific phone or for all phones at a site.

Select the **Pin Required** check box.

- 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 Unified CM cluster, e.g. multiple Directory numbers are configured with same DN but located in different partitions.

In this case, clear the **UseSiteWidePIN** check box.

Phone Registration Portal Port:

- This should be port 443 for HTTPS based connectivity
- This can be port 80 for HTTP based connectivity

Phone Registration Portal Address:

- When using HTTPS, this is the IP address or hostname of a VOSS Automate proxy node in a cluster.
- When using HTTP, this is the IP address or hostname of the primary VOSS Automate unified node in a cluster.
- This address and the port below must be accessible from the phone network.

Phone Registration Portal API User Credentials:

- Phone Registration Portal API User:
 - This is the user that was configured in the previous section of documentation. Please specify the email address.
- Phone Registration Portal API Password:
 - The password of the PBR API user:

Note that this information is required for both the Provider level config and the config for any customers.

Phone Registration Service Hierarchy:

- If the config record is defined at Provider level, then this should be the Provider hierarchy, e.g. sys.hcs.CC-P.
- If the config record is defined at the customer level, then this should be the customer hierarchy, e.g. sys.hcs.CC-P.FlexCorp)

CUCM IP:

- This should be the IP address of Unified CM that is accessible to VOSS Automate using HTTPS SOAP requests.

By default, VOSS Automate requires a PBR device record per device, but in some cases, it could be sufficient to use a single pin per site:

1. In this case, select the **UseSiteWidePIN** check box.
2. 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.

Additional options:

- Auto Provision PBR device record. This feature is experimental and should **not be selected**.
- Use default PIN. This feature is experimental and should **not be selected**.

- BAT devicename format: This should be left to default.

Important: After saving the above configuration in VOSS Automate, you must restart the services by running the following CLI command on the primary node:

cluster run all app start phone-based-registration

Related Topics

- [Introduction to Phone Based Registration](#)

32.3.6. Configure a Cisco Unified CM for Phone Based Registration

Related Topics

- [Introduction to Phone Based Registration](#)

Using PBR Setup to configure a Cisco Unified CM

The PBR Setup feature automates the configuration of Unified CM for AutoRegistration and Phone Based Registration.

In VOSS Automate, browse to **Services > Phone Based Registration > PBR Setup**. The following input is required:

- **CUCM IP Address:** IP Address of the publisher for the Unified CM Cluster.
- **Call Manager Group for Auto Reg:** Name of Unified CM Group for AutoReg.
- **Call Manager for Auto Reg:** Name of the Call Manager for AutoReg (as specified under **Services > Phone Based Registration > 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 VOSS cluster UN1 .
- **PBR Portal Port:** 8412.

PBR Set-Up	
CUCM IP Address*	172.30.11.130
Call Manager Group for Auto Reg*	Default
Call Manager for Auto Reg*	172.30.11.130
First Directory Number for auto registration*	8012000
Last Directory Number for auto registration*	8012001
Phone Registration Portal Address*	172.30.11.126
Phone Registration Portal Port*	8412

VOSS recommends that initial configuration of the Unified CM is performed using the PBR Setup workflow described above. In cases where there is existing auto registration config on the Unified CM, it may be required to do this manually.

Important: The **Services Provisioning** value under **Enterprise Parameters Configuration - Parameter Name** on the associated Unified CM **must** be set to **Both**.

Configuration on Cisco Unified CM

VOSS Automate Phone Based Registration (PBR) requires the following functionality to be configured on Cisco Unified CMs that manage phones which may be registered by this feature:

1. Configure the Unified CM to allow AutoRegistration of new phones. This is standard auto registration config for Unified CM. The PBR Setup in VOSS 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 subscribes to the `phonereg` phone service.

Screenshots of the relevant configuration on Unified CM 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

IP Phone Services Configuration

Save ✖ Delete Update Subscriptions + Add New

Status

i Status: Ready

Service Information

Service Name*

Service Description

Service URL*

Secure-Service URL

Service Category*

Service Type*

Service Vendor

Service Version

Enable

Service Parameter Information

Parameters

New Parameter
Edit Parameter
Delete Parameter

Save Delete Update Subscriptions Add New

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):

```
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.


Universal Device Template Configuration

 Save
 Delete
Expand All
 Add New

▼ Template Information

Name *

▼ Required and Frequently Entered Settings

Device Description 

Device Pool * [View Details](#)

Device Security Profile *

SIP Profile *

Phone Button Template *

▶ Device Settings

▶ Device Routing



▶ Phone Settings

▶ Protocol Settings

▶ Phone Buttons Configuration

▼ IP Phone Services Subscription

Subscribe

Service	Description	Action
Register Phone	phonereg	 

5. Unified CM for Auto Registration:
 - a. Browse to **System > Cisco Unified CM**.
 - b. Note the phonereg Universal device template.

Cisco Unified CM Configuration

Save Reset Apply Config

Status
Info Status: Ready

Cisco Unified Communications Manager Information
 Cisco Unified Communications Manager: CM_fx-pbr-cucm-01 (used by 17 devices)

Server Information
 CTI ID: 1
 Cisco Unified Communications Manager Server*: fx-pbr-cucm-01
 Cisco Unified Communications Manager Name*:
 Description:
 Location Bandwidth Manager Group:

Auto-registration Information
 Universal Device Template*:
 Universal Line Template*:
 Starting Directory Number*:
 Ending Directory Number*:
 Auto-registration Disabled on this Cisco Unified Communications Manager
 Next Auto-Registration number to be used: 80000001
Note: Ensure there are unused Directory Numbers within the configured range.

32.3.7. Phone Based Provisioning

Related Topics

- [Introduction to Phone Based Registration](#)

Setup a Phone for Phone Based Registration

In this case we provision a phone with a fake MAC address, e.g. BAT000008012005 using bulk loaders or the VOSS Automate Admin portal. An optional Phone Based Registration (PBR) device record can be provisioned that provides the following functionality:

1. Configure a PIN code that can be used to authenticate requests to register phones with Phone Based Registration.
2. Assist with unique identification of device to replace where directory numbers are not unique within a Call Manager Cluster.

Register a Phone with Phone Based Registration

Assuming the Phone is correctly setup the following steps are required to register a phone with Phone Based Registration (PBR).

1. Auto Register a physical phone with Cisco Call Manager.
2. Access the Phone Services Menu on the Auto Registered Phone.
3. Select Register Phone menu option.
4. Enter extension and PIN (if required).
5. Submit request.

This initiates a request to VOSS Automate to replace the configuration of the Auto Registered Phone with the rich settings defined for the pre-provisioned device with fake MAC.

32.3.8. Detail Phone Based Provisioning Steps

1. Provision a phone with a fake MAC Address:

- a. In this case we'll use Quick Add Subscriber, but VOSS Automate Phone Management or Advanced Subscriber features can also be used.
- b. The fake MAC address must have a BAT prefix, e.g. BATABCABCABCABC.

Quick Add Subscriber

Save Help Back Action

Entitlement Profile: [{"BasicUser", "hcs.CC-P"}]

Quick Add Group*: Standard CIPC SIP

User status: Adding services to NEW CUCM user.

Lines

Directory Number*: 1008

Voice:

Phone Type: Cisco IP Communicator

Phone Protocol: SIP

Phones

Phone Name*: BATDONALDS

Extension Mobility:

Single Number Reach:

2. Provision a PBR Device Record for the phone with a PIN:

- a. Browse to **Subscriber Management > PBR Phones and PINS > Add**.
- b. Specify the Device Name of the pre-provisioned device with the fake MAC.
- c. Route Partition is not required unless Site-Wide PIN.

PBR Phones & PINS* [BATDONALDS]

Device Name*: BATDONALDS

Pattern*: 1008

PIN: 12345

Route Partition:

3. Auto Register the Phone on CUCM:



4. Select Phone Services and then Register Phone:
 - a. Enter Extension and PIN.
 - b. Submit.



- 5. The Phone screen should now show Registering Phone.
- 6. The VOSS Automate Transaction log should now show a Register Phone Transaction.

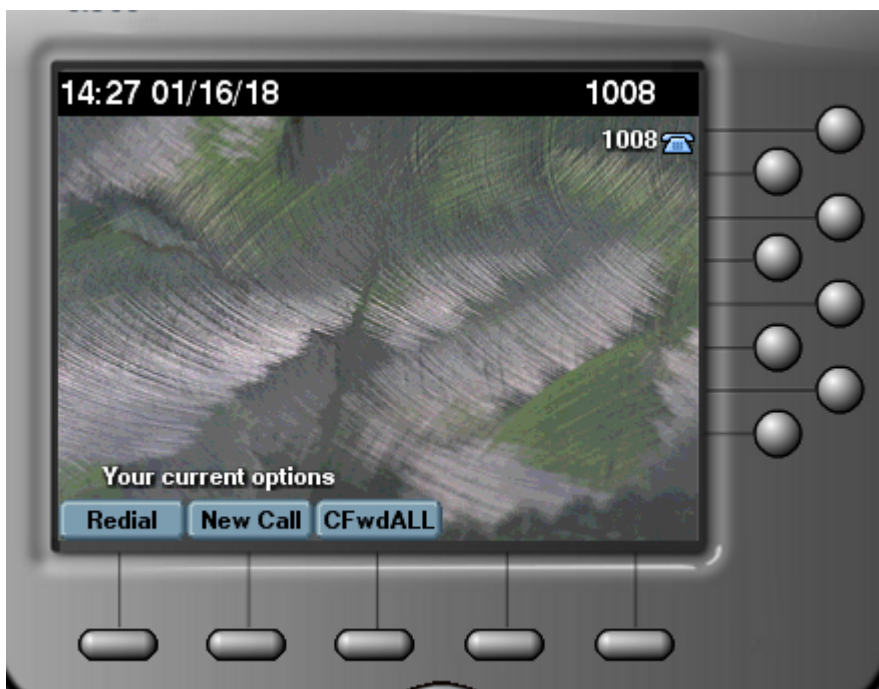
Transaction					
Id	Action	Username	Status	Detail	Submitted Time
27354	Create Rs Reg Phone View	pbr_api_user	Success	RS_RegPhone_VIEW	January 16, 4:12:15 PM

Transaction		Replay	Help	Back
Status	Success			
Submitter Host Name	V4UCUCCEUCDMPRI			
Processor Host Name	V4UCUCCEUCDMPRI			
Message	Refresh device/cucm/User			
Rolled Back	No			
Priority	Normal			
Submitted Time	January 16, 2018 at 4:12:15 PM South Africa Standard Time			
Started Time	January 16, 2018 at 4:12:15 PM South Africa Standard Time			
Completed Time	January 16, 2018 at 4:12:21 PM South Africa Standard Time			
Duration	5.623 seconds			
Sub Transactions				
Action	Status	Transaction	Submitted Time	Detail
Update Cucm Phone	Success	Link	January 16, 4:12:19 PM	SEPDONALDS
Delete RS PBR Device	Success	Link	January 16, 4:12:18 PM	BATDONALDS

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 autoregistered phone.

7. Once the transaction completes, the phone should reboot and show the device configuration of the pre-provisioned phone.



Related Topics

- [Introduction to Phone Based Registration](#)

32.3.9. 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:

PBR Phones & PINs* [SITE]

Device Name*	<input type="text" value="SITE"/>
Pattern*	<input type="text" value="SITE"/>
PIN	<input type="text" value="12345"/>
Route Partition	<input type="text" value="Cu1SI1-Feature-PT"/>

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.

Related Topics

- [Introduction to Phone Based Registration](#)

32.3.10. Menu Layout and Access Profiles

1. Phone-Based Registration Sub-menu under Services:

- Add “PBR Set-Up”
 - Title: PBR Set-Up
 - Type: view/RS_SetupReg_VIEW
 - Display As Form
- Add “PBR Config”
 - Title: PBR Config
 - Type: data/RS_PBR_Config
 - Display as list

- Add “PBR phonereg IP Phone Service”
 - Title: PBR phonereg IP Phone Service
 - Type: device/cucm/IpPhoneServices
- Add “PBR UDT Templates”
 - Title: PBR UDT Templates
 - Type: device/cucm/UniversalDeviceTemplate
- Add “PBR ULT Templates”
 - Title: PBR ULT Templates
 - Type device/cucm/UniversalLineTemplate
- Add “CUCM CallManagers”
 - Title: CUCM CallManagers
 - Type: device/cucm/CallManager
- Add “CUCM CallManager Groups”
 - Title: CUCM CallManager Groups
 - Type: device/cucm/CallManagerGroup
- Add “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
- Add “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

2. Under Subscriber Management Advanced Functions add:

- Add “PBR Phones & PINs”
 - Type: data/RS_PBR_Device
 - Title: PBR Phones & PINs
- Add “PBR Register Phone”

- Title: PBR Register Phone
 - Type: view/RS_RegPhone_VIEW
 - Display As: Form
3. Add the PBR Views to the Access Profile for Provider Admin (expose all operations):
- view/RS_RegPhone_VIEW
 - view/RS_SetupReg_VIEW
 - data/RS_PBR_Config
 - data/RS_PBR_Device

Related Topics

- [Introduction to Phone Based Registration](#)

32.4. Phone Services

32.4.1. Introduction to Phone Services

The Phone Services feature provides a XML-based interface to user settings that can be utilized via the Cisco IP Phones. If the feature is enabled, the following services become available for users to interact with via their IP Phones using the Telephone User Interface (TUI):

- Speed Dials - Provides the user with the ability to manage and use their speed dials for the phones/extension mobility profile.
- Call Forward - Provides the user with the ability to manage call forward destinations per line for key call forward options (all, busy, no answer).
- Corporate Directory - Provides the ability to view, search, and initiate calls from the users within VOSS Automate.

These will appear alongside other Phone Services that are setup in the system.

The Phone Service feature requires network connectivity between the phones and the VOSS Automate Proxy server instance. The feature supports HTTP only from the phones.

The Phone Services feature has been tested to support the following phone types:

- 78XX, 88XX, 89XX, and 99XX
- Other Cisco phone models may work, however these have not been validated and will not be supported if there are issues. So use with any other phone models should be tested carefully in your lab prior to use in production if desired.

See also:

- [Phone Services Feature Setup](#)
- [Manage Phone Services](#)

32.4.2. Phone Services Feature Setup

Introduction to Phone Services

To enable and setup Phone Services, the following steps are required:

1. Pre-requisites

Prior to setting up the Phone Services Feature, make sure that the phone based registration web service has already been installed, see *Install the Phone Based Registration Web Service*.

2. Configure a Local Admin for use by the Feature

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. VOSS suggests this user is used just for phone services and not used to login 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 will be 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 3 for the new password.

3. Enable the PBR instance for UCM Clusters

If you have already configured Phone-based Registration then some of these steps might already be complete. Configuration parameters are accessed from the **Services > Phone Based Registration > PBR Config** menu item.

- Setup the required PBR Configuration instances in VOSS Automate. This may require you 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.
- An instance of the model at the Provider level is required (with the Unified CM IP value blank if you don't have a Unified CM at the Provider level). This instance will enable the basic Phone Services capability on the system.
- An instance of the model at the hierarchy level of the Unified CM Cluster that requires the feature to be supported. **In the case of a multi-cluster setup, multiple instances may be required at the same hierarchy (one instance per Unified CM).**

The following fields and settings are required for Phone Services (see also illustration below - values are examples only). The other settings on the form are not required for Phone Services.

- **Name** - Unique name for this instance.
- **Phone Registration Portal Address** - this is 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 hard coded for Phone Services: `pbr-api-access@[providername].com`.

- **Phone Registration Portal API Password** - The password for the user setup in Step 2.
- **Phone Registration Service Hierarchy** - This field is populated based on the hierarchy breadcrumb when you click the add button. If it is wrong, navigate back 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.

Name*	Default
BAT Prefix Required*	<input checked="" type="checkbox"/>
BAT DeviceName Format	
Auto Provision PBR*	<input type="checkbox"/>
Pin Required*	<input checked="" type="checkbox"/>
UseSiteWidePin*	<input type="checkbox"/>
PBR Device Record Required*	<input checked="" type="checkbox"/>
Phone Registration Portal Address	172.29.232.12
Phone Registration Portal Port	8412
Phone Registration Portal API User	pbr-api-access@csp.com
Phone Registration Portal API Password
Repeat Phone Registration Portal API Password
Phone Registration service Hierarchy	sys.hcs.CS-P.CS-NB.AAAGlobal
CUCM IP	10.120.11.206

To make the setup of multiple instances of this record easier in a system with more than one cluster, you can include a configuration template in your menu layout populated with the values for the shared settings then the form will pre-populate with them, e.g. Portal address, Portal port, API User, and API Password.

Note: Depending on your network setup, in the event of a proxy failure, e.g. a data center DR Failover scenario, the Phone Services hostname/IP address may need to be changed to the proxy in the DR data

center.

Important:

- After saving the above configuration in VOSS Automate, you must restart the services by running the following CLI command on the primary node (if not already done):

cluster run application app start phone-based-registration

If several customers are onboarded and configured at the same time, then the command only needs to be run once after all the configuration is completed. Subsequent single customer onboarding will however require that the command be re-run.

- The **Services Provisioning** value under **Enterprise Parameters Configuration - Parameter Name** on the associated Unified CM **must** be set to **Both**.
-

4. Create Unified CM IP Phone Service for Phones to Access the Feature

There are two ways of setting up the service that controls which devices the service appears on:

- Regular service - the service must be subscribed individually to specific phones on which the service must appear:

Enable check box = Selected

- Enterprise-wide subscription - the service will appear on all phones in the system:

Enterprise Subscription check box = Selected.

Typically an enterprise-wide subscription would be the easiest as it means not managing the service subscriptions by device. However, if more granular control is required then managing it as a normal service and subscribing as needed is possible.

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 setup into the Unified CM for the phones to use it.

Choose **Device > Device Settings > Phone Services**.

The following are the settings for the service. The service can be configured via VOSS 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 Cisco Unified CM:

- **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 follows (see Note below)

Note: 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 '=' sign with the value 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
```

Where <VOSS Automate-Address> - is the address that 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> - is the address of Unified CM as known to VOSS Automate - consider any NAT setup in your network.

- `corp_dir` - this parameter is enabled (true) by default. It can be disabled if necessary by adding it to the URL as “corp_dir=false”. When enabled, the “Corp Dir” menu item is added to the list of services. The corporate directory shows the user with the number of the associated device at the selected hierarchy or lower (see `corp_dir_scope` below), and displays a maximum of 50 numbers only. The users are filtered and formatted according to the `corp_dir_format` parameter.

Note: The corporate directory excludes **End User** type users who have been marked “Exclude from Directory” as well as **Admin** type users (see [Add an Admin User](#)).

- `corp_dir_format` - this parameter determines the format of the corporate directory, and can have one of the following values:
 - “UN-LN-FN” = Username, Lastname, Firstname
 - “LN-FN-UN” = Lastname, Firstname, Username
 - “LN-FN” = Lastname, Firstname
 - “FN-LN” = Firstname, Lastname
 - “UN” = Username

If the parameter is omitted from the URL, the default corporate directory format will be “UN-LN-FN”, i.e. Username, Lastname, Firstname.

- `corp_dir_scope` - this parameter (either Provider, Reseller, Customer, IntermediateNode, Site, or LinkedSite) determines which users and numbers are displayed in the corporate directory. Default = Customer if a value is not specified.

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 will display 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` - this parameter is used to control whether the service will retrieve the latest setting from the underlying Unified CM when the service is used.

For example, when opening the call forward option, it would retrieve the latest call forward all setting from the Unified CM. This can be 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` (which is the default if excluded) can be used to make the service quicker.

Note: To effect a change to any value on the IP Phone Services URL, you must click **Update Subscriptions** on the **IP Phone Services Configuration** page on the Unified CM.

5. Connectivity between Phones and VOSS Automate

For the Phone Services feature to work, the network needs to support connectivity between the Phones and the VOSS Automate Proxy server. This could be across a NAT boundary or a firewall that requires the appropriate configuration to allow the traffic. From a firewall perspective, the connectivity is via HTTP and the port is 8412. As noted above, consider the user/validating of a DNS SRV entry for the VOSS Automate proxy address for redundancy, otherwise if IP address or static hostname is used the service and rules may need updating in the event of a DR scenario or proxy failure.

See also:

- [Manage Phone Services](#)

32.4.3. Manage Phone Services

Note: This feature will only be available once correctly configured in VOSS Automate as well as the associated Unified CM (see [Phone Services Feature Setup](#)).

After initial configuration, an end user will be able to manage the following phone services directly from the phone (if configured in VOSS Automate):

- Speed Dials
- Call Forward - View Call Forward Settings, Set Call Fwd All(CFA), Set Call Fwd Busy(CFB), Set Call Forward NoAnswer(CFNA)
- Corporate Directory



Manage (add, edit or delete) a service directly from the Telephone User Interface (TUI).

The services all work in a similar way as shown in the following example with speed dials:

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**).

See also:

- [Introduction to Phone Services](#)
- [Phone Services Feature Setup](#)

Index

A

app

- app install list, [924](#)
- app install pbr, [924](#)
- app start phone-based-registration, [925](#)

C

- Call Park Management, [209](#)

F

Feature

- Feature Forced Authorization Codes (FAC), [220](#)
- Feature Move Subscriber, [633](#)
- Feature Pexip Conferencing Overview, [674](#)
- Feature Phone Registration Activation Code, [648](#)
- Feature Softkey Templates, [207](#)
- Feature User Management, [360](#)
- Feature Webex App, [754](#)
- Phone Based Registration, [915](#)
- Phone Services, [939](#)

Flowchart

- Audit Number Inventory, [608](#)
- Number Cooling, [604](#)
- Number Inventory (Enterprise), [593](#)

- Forced Authorization Codes (FAC) (Feature), [220](#)

M

- Move Subscriber (Feature), [633](#)

P

- Pexip Conferencing Overview (Feature), [674](#)
- Phone Based Registration (Feature), [915](#)
- Phone Registration Activation Code (Feature), [648](#)
- Phone Services (Feature), [939](#)

Q

- Quick Add Subscriber, [739](#)
- Quick Add Subscriber (Feature), [754](#)
 - Feature Conditions, [745](#)

- Feature Creating Quick Add Subscriber Groups, [669](#)
- Feature Delete a Quick Add Subscriber Group, [670](#)
- Feature Number Management, [602](#)
- Feature Quick Add Subscriber Group Default Model, [671](#)
- Feature Specify the Primary Line per Subscriber, [899](#)

S

- Softkey Templates (Feature), [207](#)

U

- User Management (Feature), [360](#)

W

- Webex App (Feature), [754](#)