



VOSS Automate Provider HCS Dial Plan Management Support Guide

Release 25.3

December 03, 2025

Legal Information

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

DOCUMENT ID: 20251203073141

Contents

1	What's New	1
1.1	Provider HCS Dial Plan Management Support Guide: Release 25.3	1
2	Use the Action search to navigate Automate	3
2.1	Overview	3
2.2	How to use Action search	3
2.3	Result handling	4
2.4	Result formats	4
2.5	Search tips	4
2.6	Example use cases	5
2.7	Best practices for admins	5
3	Overview	6
3.1	Telephony, design, and HCS dial plan overview	6
3.2	Introduction to the dial plan model in Automate	7
4	Manage dial plan	10
4.1	Dial plan roles and privileges	10
4.2	Customer HCS Dial Plan	12
4.3	Site dial plans	14
4.4	Line classes of service	20
4.5	Short codes	22
4.6	Directory number routing	23
4.7	Customers	24
4.8	Introduction to number management in Automate	31
4.9	Number inventory	33
4.10	View number details and usage	43
4.11	E164 numbers in the number inventory	47
4.12	Number status and usage	48
4.13	Number range management	50
4.14	Number cooling	56
4.15	Number reservation	58
4.16	Number inventory alerting	60
4.17	Number inventory audit	61
4.18	E.164 inventory management	64
4.19	Inter-site cross-cluster support	77
4.20	Local breakout support	77
4.21	Voice mail	78
4.22	Adding aggregation trunk and route group and associating to existing route list and SLRG . .	86
4.23	Configure SIP profiles	89
4.24	Configure SIP trunk security profiles	125
4.25	Configure SIP trunks	137
4.26	Configure SIP route patterns	162

4.27	Configure route groups	165
4.28	Configure route lists	168
4.29	Configure date time groups	172
4.30	Configure locations	173
4.31	Configure device pools	176
4.32	Configure Cisco UCM groups	190
4.33	Configure route partitions	193
4.34	Configure calling search spaces	195
4.35	Configure calling party transformation patterns	197
4.36	Configure called party transformation patterns	202
4.37	Configure CTI route points	205
4.38	Configure time periods and schedules	212
4.39	Clone a Cisco UCM device model	216
4.40	Load balancing	217
4.41	Update the USA device-based routing dial plan	219
4.42	Sharing lines across sites	220
5	Advanced management	234
5.1	Macros	234
5.2	Auto-cloning of dial plan schemas and schema groups to the Provider hierarchy node	236
5.3	Create schemas	237
5.4	Clone dial plan schemas	238
5.5	Modify site defaults	239
5.6	Create schema groups	258
5.7	Associate custom schemas to customers	259
5.8	Default dial plan schemas	260
5.9	Emergency and CLI settings	266
5.10	Default dial plan event triggers	268
5.11	Correct calling presentation overwrite on calls forwarded to PSTN	275
5.12	Global settings	276
5.13	Email	296
6	Basic call flow overview	303
6.1	Intra-site extension dialing	303
6.2	Multi-site customer with ISP included in SLC	303
6.3	Multi-site customer with extension prefix and no ISP	304
6.4	Single Site Customer	305
6.5	Customer (single- or multi-site) without PSTN prefix	306
6.6	Multi-site customer with ISP	308
6.7	On-net call flows	308
6.8	Off-net call flows	317
6.9	Emergency call handling	326
7	PSTN call processing and routing	332
7.1	Introduction to PSTN call processing and routing	332
7.2	Dial plan determination	334
7.3	Country dial plan deployment	334
7.4	Dial plans for Caribbean countries	347
7.5	Local breakout (LBO)	352
8	Call search spaces and partitions	356
8.1	Calling search spaces and partitions	356
9	Telephony design and dial plan primer	361
9.1	Architecture primer	361

9.2	Numbering plan design	363
10	Limitations in Cisco UCM	367
10.1	Call limitations	367
	Index	368

1. What's New

1.1. Provider HCS Dial Plan Management Support Guide: Release 25.3

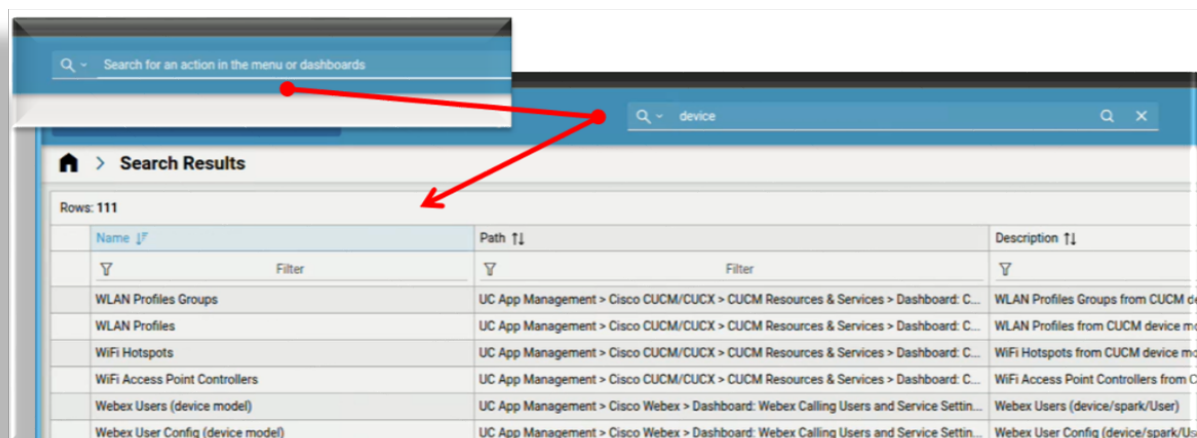
- EKB-24170: Improve Action Search list details. See: [Use the Action search to navigate Automate](#)
Updated Action search topic with improvements, specifically, matching of queries, and ability to sort, filter, and clear results.
- EKB-24268: Change External Breakout field to not required in Customer Dial Plan. See: [Customer HCS Dial Plan](#)
Updated HCS Customer Dial Plan topic to make to note that *Default External Breakout Number* is now optional.
- EKB-25699: Unreserve numbers does not clear Reservation Notes. See: [Number reservation](#)
Docs updated for reservation notes field that is automatically cleared when unreserving a number.
- EKB-25937: Enhance Number Inventory Audit to change numbers from Cooling or Reserved to Used status if they are used. See: [Number inventory audit](#)
Updated topic Number inventory audit to include numbers in Cooling or Reserved status.
- VOSS-1507: (EKB-25879: Create an Overbuild tool for moving Defender device models). See: [Run overbuild](#)
Added details on the new Microsoft Defender for Office & Endpoint functionality.
- VOSS-1507: (EKB-24159: Create new Global settings for enabled services). See: [Global settings](#)
Added details on the new Microsoft Defender for Office & Endpoint functionality.
- VOSS-1545: Configurable Microsoft Sync. See: [Global settings](#)
Added details for the vendor-agnostic Datasync Builder tool, templates, and profiles, which are also integrated with the MS tenant.
- VOSS-1560: Microsoft Tenant App Registration Enhancements. See: [Global settings](#)
Changes when adding and editing a Microsoft tenant.
- VOSS-1575: Role Management System Optimization. See: [Customers](#)
Role Based Access docs updated for deprecation of automatically cloned roles, simpler way of adding and assigning shipped roles directly without cloning across hierarchies, and that roles are now all managed via the data/Role model.
- VOSS-1590: Microsoft: Enhance update sync FTP/Move via Data Sync and Manual Move (Move User). See: [Global settings](#)

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

2. Use the Action search to navigate Automate

2.1. Overview

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



Related topics

- Search in Automate in the Core Feature Guide

2.2. How to use Action search

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

2.3. Result handling

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

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

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

2.4. Result formats

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

2.5. Search tips

To improve your Action search results:

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

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

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

Name ↑	Path ↑	Description ↑
(N to 1) DN to E164 Associations with Update	Number Management > Dashboard: Number Inventory Management	Map range of internal to a single external number if using Cisco with External/Internal
(N to N) DN to E164 Associations	Number Management > Dashboard: Number Inventory Management	Map range of internal to external numbers if using Cisco with External/Internal numbe
Add E164 Inventory	Number Management > Dashboard: Number Inventory Management	Add E164 inventory if using Cisco with External/Internal number mapping
E164 Inventory	Number Management > Dashboard: Number Inventory Management	View and manage E164 inventory if using Cisco with External/Internal number mappin

2.6. Example use cases

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

2.7. Best practices for admins

To ensure meaningful search results with Action search:

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

3. Overview

3.1. Telephony, design, and HCS dial plan overview

The dial plan model is a key component of Automate's architecture and provisioning workflow. This guide describes the relevant architectural elements, the required service configuration, and how the dial plan model may be customized to meet varying infrastructure requirements and customized service types.

Automate provides automation and standardization to Cisco Unified Communications Manager (UCM) and other elements, such as IOS devices, and Cisco Unity Connection (CUC). Additionally, bulk loaders can be used to provision and onboard customers. This routing architecture and the associated element configuration meet Automate's configurable dial plan model.

Note: The dial plan model may be referred to as either *HCS Dial Plan Model*, *HCS Dial Plan*, *Dial Plan Model*, or *Dial Plan*.

HCS dial plan tools are provided only in the Automate Provider deployment.

The dial plan model intends to create a pre-integrated baseline configuration of UCM applications, which can then be integrated into the platform and the service provider infrastructure with minimal effort.

The dial plan model configures both end-customer equipment, such as UCM or on-premise routers, as well as the interaction with aggregation layers, using systems like Cisco Session Management Edition, or Session Border Controller (SBC).

Note: While standard configurations are provided, service providers must customize parts of the dial plan model for a particular environment.

For end-customers, the dial plan model supports many corporate dialing schemes, and includes a standardized model for handling intra-site, inter-site, and PSTN calls, typically using a *site + extension* methodology. Additionally, it covers advanced routing requirements of elements such as central versus local breakout for PSTN calls, and handles different numbering requirements across multiple countries.

Automate's dial plan model provides a definition of standard telephony services that abstract UCM configurations into simpler choices that correspond to the feature plans that service providers want to offer. For example, the partitions, calling search spaces (CSS), and translation patterns are predefined based on a choice of simple outbound, inbound, call forwarding, and time of day settings. These settings are exposed as service types in Automate, and are combined into feature packages and templates that define user or lines telephony services.

3.2. Introduction to the dial plan model in Automate

3.2.1. Overview

The dial plan model was formalized to facilitate a common basis for all translation patterns, partitions, and calling search spaces (CSS). It was also intended to provide consistent naming conventions, and included the following calling patterns:

- G1 (Flat Dial Plan) calling patterns
- G2 (Generic Dial Plan) calling patterns
- G3 (Shared Architecture Dial Plan) inter- and intra-site calling patterns

The dial plan model evolved to provide structure and consistency across deployments, but was inconvenient and clumsy to manage.

The dial plan model in Automate leverages templates and workflows, and JSON files are used to implement it. These features make this dial plan model more flexible and easier to manage.

3.2.2. Dial plan model types in Automate

The Automate dial plan model comprises these four, basic, predefined call types (dial plan model types):

1.	Directory Number = Site Location Code (SLC) + Extension, no Inter Site Prefix (ISP) in SLC
2.	Directory Number = SLC + Extension with ISP as part of SLC
3.	Directory Number = SLC + Extension and without ISP, can be with or without Extension Dialing Prefix (EDP)
4.	Directory Number = Flat Dial Plan (no SLC)

Note: These four dial plan model types comprise all previously available functionality, but gives service providers additional flexibility because they can be extended with custom schemas (additional, standalone elements you can choose in Automate to add to the schema).

3.2.3. Dial plan model features

The dial plan model provides several flexible features, including:

- Dynamic class of service
- Country dial plans
- Blocked / non-blocked numbers
- Call Manager groups
- Flexible routing
- PSTN prefix per country per customer

The first site of the customer's country sets the PSTN prefix for all other sites of the country for that customer.

3.2.4. Using the dial plan model in Automate

An admin user in Automate fills out a template (at either customer or site level), which defines the dial plan model that is delivered to the Cisco UCM and sites.

The dial plan model is based on various configuration elements, depending on the hierarchy level:

Hierarchy	Configuration elements
Customer level	<ul style="list-style-type: none"> • Is SLC-based dial plan required? • Does the customer require inter-site prefix (ISP)? • Is inter-site prefix required as part of SLC? • Is the ISP part of the directory number? • Is the ISP included in the voicemail ID?
Site level	<ul style="list-style-type: none"> • Site name • External breakout number • SLC • Extension length • Extension prefix required • Extension prefix • Published number • Emergency number

High level dial plan workflows manage the following in Automate:

- Locations, region, and device pools per site
- UCM groups at the Provider/Reseller/Customer level
- Local route groups names at the cluster level
- Default and custom, Customer and Site level dial plan schemas
- voicemail

- Routing
- Emergency calling line identification (CLI)
- Inventory management
- Gateway management

4. Manage dial plan

4.1. Dial plan roles and privileges

provider

Administrators can perform all tasks associated with their roles, as well as all dial plan tasks that are lower on the navigation hierarchy.

Hierarchy is shown from left (highest) to right (lowest) in the table below.

The table lists out dial plan privileges for administrators, depending on the role assigned:

Tasks	HCS Admin	Provider / Reseller Admin	Customer Admin	Site Admin
Create a Customer Dial Plan	X (Customer level)	X (Customer level)	X (Customer level)	
Create a Site Dial Plan	X (Site level)	X (Site level)	X (Site level)	
Configure Class of Service	X (Site level)	X (Site level)	X (Site level)	
Configure Short Code	X (Site level)	X (Site level)	X (Site level)	X
Configure Directory Number Routing	X (Site level)	X (Site level)	X (Site level)	X
Add Directory Numbers	X (Customer level)	X (Customer level)	X	
View Directory Number Inventory	X (Site level)	X (Site level)	X (Site level)	
Configure SIP Route Patterns	X (Site level)	X (Site level)	X (Site level)	
Create Voice Mail Service	X (Provider/Reseller level)	X (Provider/Reseller level)		
Associate Voice Mail Services to Customer	X (Customer level)	X (Customer level)		
Define a Voice Mail Pilot Number	X (Customer level)	X (Customer level)	X (Customer level)	
Associate Pilot Numbers to a Site	X (Site level)	X (Site level)	X (Site level)	

continues on next page

Table 1 – continued from previous page

Tasks	HCS Admin	Provider / Reseller Admin	Customer Admin	Site Admin
Configure SIP Trunks	X	X	X	
Reset SIP Trunks	X	X	X	
Restart SIP Trunks	X	X	X	
Configure Route Groups	X	X	X	
Configure Route Lists	X (Customer or Site level)	X (Customer or Site level)	X	
Configure Device Pools	X (Customer or Site level)	X (Customer or Site level)	X	
Provision Emergency Calls	X			
Create Schemas	X	X		
Modify Site Defaults	X (Site level)	X (Site level)	X (Site level)	
Assign Custom Schemas to Customers	X (Customer level)	X (Customer level)		
Configure Unified CM Groups	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Regions	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Route Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Route Partitions	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Calling Search Spaces	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Translation Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Calling Party Transformation Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	
Configure Called Party Transformation Patterns	X (Customer or Site level)	X (Customer or Site level)	X (Customer or Site level)	

Related topics

- For more information on bulk loading, see the topics on Bulk Administration.

4.2. Customer HCS Dial Plan

provider

Cisco

Tip: *Use the Action search to navigate Automate*

4.2.1. Overview

For Cisco HCS dial plans, you must create a customer dial plan before you create the site dial plan.

Cisco HCS dial plan schemas are configured such that the customer-level dial plan elements are not pushed to UCM until the first site for the customer is deployed. Therefore, you won't see any dial plan elements provisioned on the UCM until at least one site is deployed for the customer.

Once you add a customer dial plan, the only change allowed is to enable CSS filtering.

Related topics

- [Site dial plans](#)

4.2.2. Add a Cisco HCS customer dial plan

This procedure adds a new Cisco HCS dial plan for a customer.

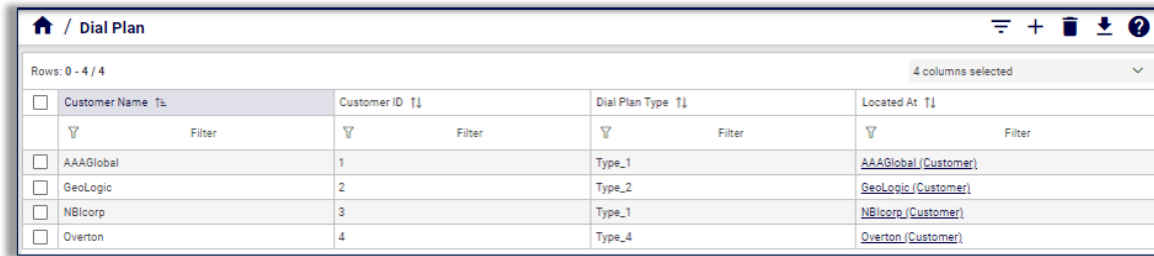
Note:

- You can only add one dial plan per customer.
 - The options you choose define the type of Cisco HCS dial plan schema to be used (Type 1 to 4).
-

1. Log in to the Admin portal as Provider or Customer admin.

Note: For details around tasks that can be performed for each admin level, see [Dial plan roles and privileges](#).

2. Go to **Dialplan Tools > Customer HCS Dial Plan**.



Customer Name	Customer ID	Dial Plan Type	Located At
AAAGlobal	1	Type_1	AAAGlobal/(Customer)
GeoLogic	2	Type_2	GeoLogic/(Customer)
NBicorp	3	Type_1	NBicorp/(Customer)
Overton	4	Type_4	Overton/(Customer)

3. Click the Plus icon (+) to add a new customer dial plan.
4. Select the customer to open the **Customer HCS Dial Plan > New Record** page.

Note: **Customer ID** is a read-only, unique, auto-generated number allocated to the customer. Customer ID is particularly useful in shared deployments (where a cluster may be shared across multiple customers) to correlate specific elements to a customer. Customer ID displays in Cisco UCM as a prefix to elements (for example Cu2Si7 identifies Customer 2, Site 7).

5. Optionally, at **Default External Breakout Number** add a PSTN Access prefix, if required.
6. **Is a site-location (SLC) required?**
 - **No.** Leave **Site-Location Code (SLC) based dial plan** clear (unchecked). Go to Step 7.
 - **Yes.** Select **Site-Location Code (SLC) based dial plan**. Select options for the following additional fields that display. When you're done, go to Step 7:
 - Optionally, select **Use extension prefix**, and fill out an extension prefix, if required.
 - Optionally, select **Inter-Site Prefix required for inter-site dialing**, and fill out the inter-site prefix (ISP), if required. The ISP can be just one digit.
 - If you're applying an inter-site prefix (ISP), define whether the ISP is included in the directory number.
 - If the ISP is to be included in the directory number, define whether the ISP is included in the Voice Mail ID.
7. Define whether to **Enable CSS filtering**.
 - When enabled, CSS filtering filters the Calling Search Spaces (CSSs) when configuring a user, phone, or line, to Site level Class of Service (CoS) CSSs.
 - When disabled (default), all available Cisco UCM CSSs are available when configuring a user, phone, or line.
8. Save the form to add the new customer dial plan.

For add, update, or delete, you can view transaction progress and details in the Transaction Logs.

Note: When adding lines (DNs) at the site level, you must define your DN appropriately (that is, you are responsible for using ISP+SLC+EXT if you deploy a Type 2 dial plan). Otherwise your inter/intra site calls won't route. For details around defining directory numbers, see [Number range management](#).

Related topics

- Transaction logging and audit in the Core Feature Guide

4.3. Site dial plans

provider

Cisco

Tip: *Use the Action search to navigate Automate*

4.3.1. Overview

A site can be associated with only one dial plan.

A Cisco HCS site dial plan is not automatically created for a site when the site is created. Instead, once the first site is deployed for a specified customer, the customer-level dial plan elements are provisioned on Cisco Unified Communications Manager (CUCM), followed by the site-specific, Cisco HCS dial plan elements. Each subsequent site takes less time to create as they have only site-specific dial plan elements to provision.

For customers with two or more sites, the site dial plan must be applied to each site.

Only one site dial plan can be added at a time against a specific CUCM. Parallel transactions are disallowed. When adding a site dial plan, its transaction workflow acquires a lock that prevents a parallel transaction for adding another site dial plan from completing. The lock value is unique per CUCM.

If you try adding another site dial plan while a transaction is in progress for the first one you added, the transaction for the second dial plan starts and is in progress for 3 minutes, trying to acquire the lock. If it cannot acquire the lock, the second transaction fails with this message:

Failed to Add Cisco HCS Site Dial Plan, a Site Dial Plan is currently being added for this Unified CM, please wait for that transaction to complete, or wait 15mins for the lock to auto expire in the case that a failed transaction did not release the lock automatically

If the first transaction fails, the lock is set to auto-expire after 15 minutes.

Related topics

- *Customer HCS Dial Plan*

4.3.2. Add a Cisco HCS site dial plan

This procedure creates a Cisco HCS site dial plan and associates the dial plan with a site.

Pre-requisites:

- Create the customer dial plan. See [Customer HCS Dial Plan](#)

You can only create a site dial plan once the customer dial plan exists because there are attributes defined in the customer dial plan that are required when the site dial plan is created.

1. Log in to the Admin portal as a Provider administrator or Customer administrator.

Note: For details around tasks that can be performed for each admin level, see [Dial plan roles and privileges](#).

2. Go to the **Dialplan Tools > Cisco Site Dialplans**, then view existing site dial plans in the list view.
3. Click the Plus icon (+) to add a new site dial plan; then, select the site.
4. On the **Dial Plan / New Record** page, configure the dial plan. The table describes the configuration options:

Field	Configuration
External Breakout Number	<p>Fill out the one digit external breakout number for the country associated with the site.</p> <p>The external breakout number is the PSTN prefix that is used when deploying a country dial plan. The default is 9. For Cisco HCS Type 1 to 4 dial plan schemas, country dial plans are deployed at the Customer level.</p> <p>The country dial plan is pushed to CUCM once the first site associated with a given country is deployed. For example, if a site is associated with the United States (USA), and it is the first site dial plan being created for the USA, the USA country dial plan is deployed as part of creating the site's dial plan.</p> <p>Automate supports only one external breakout number for each country. For example, all sites within the USA have the same external breakout as the first site within the USA.</p>
Use extension prefix	<p>Defines, for sites without Inter-Site Prefixes (ISPs), whether this dial plan uses the extension prefix from the customer dial plan.</p> <p>Displays only if your customer dial plan does NOT use ISPs, for example, HCS Type 3 dial plans (SLC, no ISP, DN=SLC+EXT).</p> <p>When enabled, this setting is applied ONLY if there is an extension prefix defined in the customer dial plan.</p>
Area Codes	<p>Click the Plus icon (+) to add valid local area codes for the site, if required.</p> <p>For each area code you add:</p> <ul style="list-style-type: none"> • Fill out the area code. • Specify the length of the subscriber part of the PSTN number. <hr/> <p>Note: The area code is used to generate the PSTN local route patterns for the site. For example, in the USA, if area codes are added for Dallas, Texas, the area codes could be specified for local dialing as 214, 469, and 972, with a subscriber length of 7. The Local Number Length field defines the length for the subscriber section of the entire E.164 number.</p> <hr/>

Field	Configuration
Site Location Code	Displays only when the customer dial plan uses site location codes. Fill out the site location code (SLC). The maximum number of digits is 8. The SLC must be unique across sites for a customer.
Extension Length	Fill out the number of digits for the extension (between 1 and 30 digits).
Area Code Used for Local Dialing	Defines whether the area code is required for local dialing from this site. Note: In the USA, this setting defines whether you use 7-digit or 10-digit local dialing.
Published number	Select from the available E.164 inventory numbers, or fill out a custom number. Note: The site published number is the default E.164 mask when a line is associated to a phone at a particular site.

Field	Configuration
Emergency Call Back Number	Select from the available E.164 inventory numbers, or fill out a custom number. Note: Site emergency call-back number is the calling number when initiating an outgoing emergency call. It can be used when you use Extension Mobility and make an emergency call from a site other than your own. It can be used when the emergency call goes out to the PSTN network, when the system includes the site emergency number so that the origin of the call is known. The system adds this calling party transformation to the DN2DDI4Emer-PT partition. The emergency call back number is not the number to dial for an emergency. Instead, it is the number used to identify the calling party for emergency calls originating from a particular site.
Use DDI for emergency calls	Define whether to use DDI for emergency calls when user is at home location.
Site ID	A read-only field that displays a unique, auto generated number for each customer site, which is prefixed to elements as an identifier (for example, Cu4Si2 indicates Customer 4, Site 2).

5. Click **Save**.

View transaction progress and details in the Transaction Logs.

The new site dial plan is added. The system takes a few minutes to provision the site dial plan, especially for the first site. The site information is loaded on CUCM, and is identifiable by its Customer ID, Site ID prefix.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

4.3.3. Update a Cisco HCS site dial plan

provider

Cisco

This procedure updates a Cisco HCS site dial plan.

1. Log in as the Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the site where you want to update the dial plan.
3. Go to the **Dial Plan** page.
4. In the list view, click on the site dial plan where you want to make changes.
5. On the **Dial Plan** page, you can update the following:

Field	Description
Area Code	You can modify or delete existing area codes, or add new area codes.
Local Number Length	The length of a locally dialed number for the specified area code.
Area Code Used for Local Dialing	Defines whether the area code is included in locally dialed calls.
Published Number	The site published number is the default E.164 mask when a line is associated to a phone at a particular site.
Emergency Call Back Number	The site emergency call-back number is the calling number when initiating an outgoing emergency call.

6. Click **Save**.

View transaction progress and details in the Transaction Logs.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

4.3.4. Area code changes in Cisco HCS site dial plans

For the Cisco Type 1-4 dial plans, area code changes result in the affected local dialing translation patterns getting reapplied for the site:

When adding new area codes	New translation patterns are deployed to the site, based on the country dial plan schema associated with the site.
When deleting area codes	Related translation patterns are un-deployed from CUCM, based on the country dial plan schema associated with the site.
When modifying area codes	Related translation patterns are un-deployed from CUCM, and new translation patterns are deployed, based on the updated area codes.

For the Cisco Type 1-4 dial plan schema groups, area code changes generate LBO IOS area code events. If you change the area code for a site associated with one or more Local SIP Gateways, area code IOS commands are generated:

When adding an area code	The area code add IOS command is generated.
When deleting an area code	The area code delete IOS command is generated if no other sites associated with the same SIP Local Gateway are using the deleted area code. If another site still references the same gateway's area code, the delete area code IOS command is not generated. This prevents invalidating the other site's local dialing behavior.
When updating an area code	The area code delete and add IOS commands are generated as necessary, based on the added and deleted logic.

4.3.5. Published number changes in Cisco HCS site dial plans

When changing an existing published number in a Cisco HCS site dial plan:

- The following site defaults are updated, if they were using the published number you changed:
 - Default CUCM Phone Line E164 Mask
 - Default CUCM Device Profile Line E164 Mask
 - Line E164 Mask
- Updates any phone line masks, device profiles, and remote destination profiles that were using the published number you changed.
- Automatically regenerates previously generated E164 IOS commands for a SIP Local Gateway associated with the site.

4.3.6. Emergency call back number changes in Cisco HCS site dial plans

When updating a Cisco HCS site dial plan and you have a Type 1 - 4 dial plan configured, two calling party transformations are created automatically with the Emergency Call Back Number.

Changing the Emergency Call Back Number updates the calling party mask in these calling party transformation patterns if it used the previous Emergency Call Back Number:

- "{{ macro.HcsDpSiteId}}!"
- "{{ macro.HcsDpSiteId}}\+!"

If the calling party mask has been manually changed, the fields are untouched.

These calling party transformation patterns insert the Emergency Call Back Number as the caller ID for any emergency calls placed from phones within the site.

Next Steps

Apply any generated or regenerated IOS commands to your IOS gateway.

4.4. Line classes of service

provider

Tip: [Use the Action search to navigate Automate](#)

4.4.1. Configure class of service for a site

This procedure creates a new Calling Search Space (CSS) or edits an existing CSS that is tied to a site. The CSS can be used as a Class of Service (COS) for a device or line, or any of the other templates that rely on COS to filter different features.

1. Log in as provider, reseller, or customer administrator.
2. Select the relevant site.

Note: When adding CoS, ensure you select a valid site under the customer in the hierarchy. You can only add CoS at a site.

3. Go to **Line Classes of Service**.

Note: There is one default Internal Calling Line Identification Presentation (CLIP) CoS that appears in the list. The default CoS is provisioned automatically based on the criteria you selected when you added the site.

4. Choose an option:

- To add a CoS, click **Add**.
- To edit an existing CoS, click on the relevant CoS, make your changes, then save.
- To clone an existing CoS, click on the relevant CoS, then click **Action > Clone**.

5. Fill out a unique name for the CoS in the **Class of Service Name** field.

Note: Ensure the name is descriptive, using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_). You can also use macros in Automate to create a CoS name. See the Automate documentation for a list of possible macros.

MMacros allow you to dynamically add site IDs, customer IDs, and other types of information to the CSS.

Example: Cu1-24HrsCLIP-PT-{{macro.HcsDpSiteName}}

The actual CSS that is sent to the UCM (based on the macros entered) is mirrored in the **Actual Calling Search Space** field. For example, the macro example above changes to Cu1-24HrsCLIP-PT-SiteABC.

6. Optional. Fill out a description for the CoS.
7. Choose route partition members to include in the CoS:
- Click the Plus icon (+) to add route partitions.
 - From the drop-down, select a route partition member.
 - Repeat this step until you have selected all the members you need for this CoS. If you want to remove any member from the CoS, click the Minus icon (-).
8. Click **Save** to add the new CoS. The new CoS will display in the summary list view, from where you can update it or delete it in future, if required.

When adding (including clone), updating, or deleting CoS, you can view transaction progress and details in the Transaction Logs.

Related topics

- Transaction Logging and Audit in the Core Feature Guide
- Class of Service in the Core Feature Guide

4.4.2. Clone a class of service for a site

This procedure clones an existing Class of Service (CoS) to the same site hierarchy node, with a new name.

- Log in as provider, reseller, customer, or site administrator.

Note: When cloning a CoS, ensure that you select a valid site under the customer in the hierarchy. Attempting to clone a CoS at any other node (at a customer or reseller for example), a system error reminds you that you must be at a site.

- Go to **Class of Service**.
- Click on the Class of Service to be cloned.
- Click **Action > Clone**.

5. Fill out a unique name for the Class of Service in the **Class of Service Name** field.

Note: Ensure the name is descriptive, using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).

6. Optionally, fill out a description.
7. Save the cloned CoS. This creates a new CoS.

When adding (including clone), updating, or deleting CoS, you can view transaction progress and details in the Transaction Logs.

Note: Save the cloned CoS to the same site hierarchy as the original CoS. You can't save the clone to a different site or to a different hierarchy.

The new CoS displays in the summary list view, from where it can be updated or deleted in future, if required.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

4.5. Short codes

Tip: *Use the Action search to navigate Automate*

4.5.1. Overview

Short codes are used for abbreviated dialing to other extensions and services.

4.5.2. Configure short codes

This procedure configures short codes.

Prerequisites:

- The site dial plan must be added. See [Site dial plans](#)

Perform these steps:

1. Log in as provider, reseller, customer, or site administrator.

Warning: When adding a short code, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. Adding a short code at any other node in the hierarchy triggers a system error indicating that you must be at a site.

2. Go to the **Short Code** page, then click the Plus icon (+) to add a short code.
3. Enter a short code in the **Short Code** field, using up to 16 characters with the following format:
 - The first character may be 0-9, or *
 - The last character may be 0-9, #, or the wildcard character X.
 - All other characters may be 0-9, . (period), or the wildcard character X. Only one . (period) is allowed.

Example:

*2.XXX

4. From the **Short Code Type** drop-down, choose one of:

Option	Description
Called Mask	The called mask maps to the Short Code. Valid entries include the digits 0 through 9; the international escape character + and the wildcard character X. For example, a called mask of 567XXX using Short Code *2.123 converts to 567123.
Directory Number	The directory number maps to the Short Code. Valid entries are digits 0 through 9.
Pre-dot with Called Prefix	The called prefix maps to the Short Code.

5. Enter the value for the Short Code Type in the **Value** field.
6. Select the **Use Originator's Calling Search Space** check box to indicate that the Short Code will use the originator's calling search space for routing a call rather than an explicit customer CSS.

If the originating device is a phone, the originator's calling search space is a combination of the device calling search space configured on their phone and line calling search space configured on the originating line.
7. Click **Save** to add the Short Code that you defined. The new Short Code appears in the table of Short Codes and it can be edited or deleted as required.

4.6. Directory number routing

Tip: *Use the Action search to navigate Automate*

4.6.1. Overview

Directory number routing is a translation pattern that is put into the PreISR and ISR partitions to route intrasite and intersite calls to extensions (directory numbers). This is similar to the way site location codes (SLCs) are used as short codes for Type 1, 2, and 3 customer dial plans.

Typically, directory number routing is used for Type 4 (flat dial plans) so that from a customer and site perspective, you can see which patterns are directory numbers because there are no SLCs available.

4.6.2. Add a directory number routing

This procedure adds a directory number routing.

1. Log in as provider, reseller, customer, or site administrator.

Warning: When adding directory number routing, you must select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. Adding a directory number routing at any other node in the hierarchy triggers a system error indicating that you must be at a site.

2. Go to the **Directory Number Routing** page, then click the Plus icon (+).
3. In the **Directory Number Routing Prefix**, enter a prefix, using up to 30 characters (for example, 234).
4. In the **Directory Number Mask Length** field, enter a DN mask length. For example, if you enter 4, the Directory Number Routing would be 234XXXX, where XXXX is the mask.
5. Click **Save**. The Directory Number Routing is added.

The new Directory Number Routing appears in the table and it can be edited or deleted as required.

4.7. Customers

Tip: *Use the Action search to navigate Automate*

4.7.1. Overview

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

- Provider
- Reseller
- Customer
- Sites (locations)

Optional intermediary nodes can also be created.

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

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

Related topics

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

4.7.2. Add or update a customer

This procedure adds or updates a customer.

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

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

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

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

To add or update a customer:

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

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

2. Choose the hierarchy.

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

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

<input type="checkbox"/>	Customer Name	Domain Name	Shared UC Applications	Disable Number Management	Public Sector	Inactive Billing
<input type="checkbox"/>	AAAGlobal	aaaglobal.com				
<input type="checkbox"/>	AutoCustomer250					
<input type="checkbox"/>	AutoCustomer300					
<input type="checkbox"/>	GeoLogic	geologic.com				
<input type="checkbox"/>	NBIcorp	nbi-corp.com				

4. Choose an option:

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

Customer Details

Customer Name *

GeoLogic

Description

GeoLogic Description

Extended Name

External Customer ID

Domain Name

geologic.com

Account ID

Deal IDs

Shared UC Applications

☒

Disable Number Management

☐

Public Sector

☐

Inactive Billing

☐

Contact Information

Address 1

7100-9 Kit Creek Road

Address 2

City

RTP

State

NC

Postal Code

27709

Country

USA

Name

GeoLogic Admin

Email Address

contactus@geologic.com

Telephone Number

919-555-0001

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

Customer Details	Description
Customer Name	Mandatory. The name of the customer.
Description	Customer description
Extended Name (Provider)	Descriptive name for the customer, used by external clients to correlate their own customer records with customer records stored in HCS.
External Customer ID (Provider)	External customer ID used by the Service Inventory service, and included as a column in the customer record of the service inventory report. Specify an External Customer ID in this field that matches the customer ID used by the external inventory tool that receives the Service Inventory reports. If the Service Inventory service is not being used, this field is not required. However, it can be used to correlate customer records in external systems with customer records in HCS.
Domain Name	<p>Customer domain. This field is used to create email addresses for:</p> <ul style="list-style-type: none"> The customer default local administrator, for example: <code>Customer1Admin@customer1.com</code> Site default local administrators under the customer, for example: <code>Site1Admin@customer1.com</code> <p>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.</p>
Account ID	The Account ID is used by external clients to correlate their own customer records with the customer records stored in HCS. This Account ID value is synced to the Customer record in the Shared Data Repository.
Deal IDs	Deal IDs are used by the Hosted License Manager (HLM) service. HLM supports Point of Sales (POS) report generation. The report includes all customers on the system with aggregate license consumption at customer level. The optional Deal ID field associated with the customer is included in the report. Each customer can have zero or more Deal IDs. The Deal ID field is free text format and each deal ID is separated by a comma.

Customer Details	Description
Shared UC Applications	Indicates whether the customer can use Shared UC Apps. If selected, the customer sites can use Network Device Lists that contain Shared UC Apps. Shared UC Apps are UC Apps that are defined above the Customer hierarchy level.
Disable Number Management	<p>Enable or disable Number Management for this customer.</p> <ul style="list-style-type: none"> When disabled (checkbox selected), you cannot add directory numbers and E164 numbers to inventories for this customer. When enabled (checkbox clear), you can add directory numbers and E164 numbers to inventories for this customer.
Public Sector	Defines whether the customer is a Public Sector customer. Used for License Reporting.
Inactive Billing	Defines whether to exclude the customer from billing (for testing). Used for License Reporting.

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

5. Save your changes.

Related topics

- [Number inventory audit](#)
- Delete issues and purges in the Core Feature Guide
- Role-based dashboards and menus in the Core Feature Guide

4.7.3. Add custom fields to customer configuration screens

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

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

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

Macros for custom string fields for relation/HcsCustomerREL:

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

Macros for custom boolean fields for relation/HcsCustomerREL:

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

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

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

Expose custom fields for *relation/HcsCustomerREL*

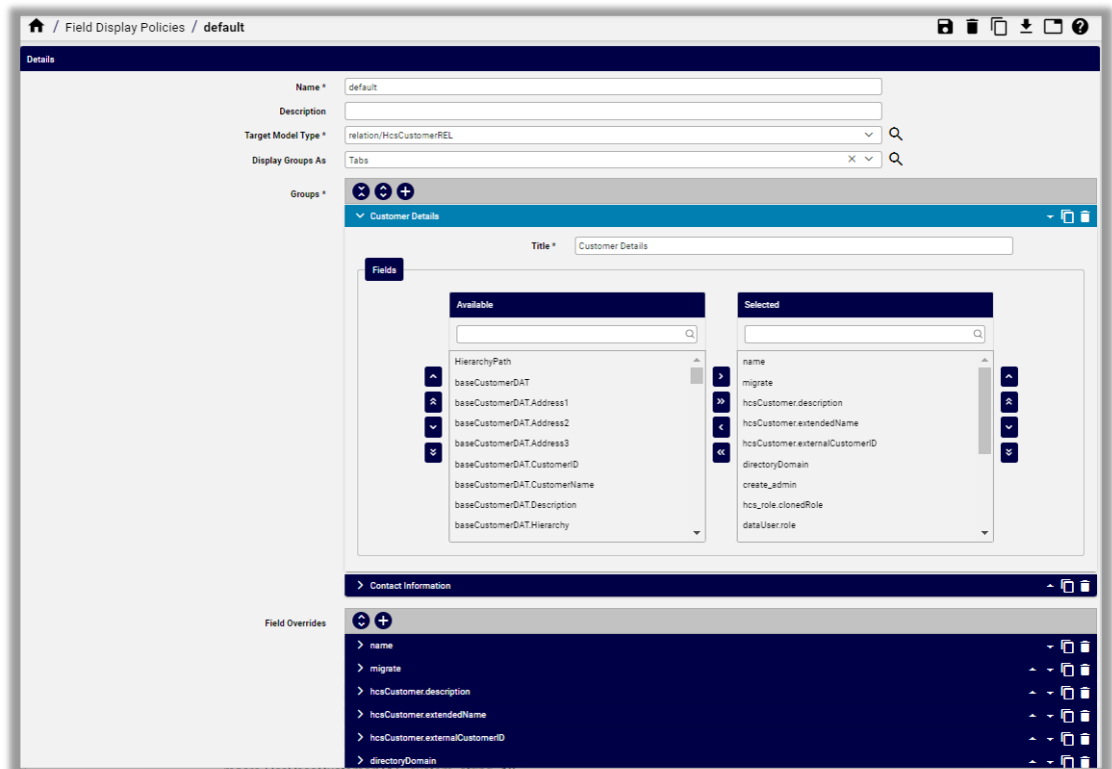
1. Log in to Automate as Provider admin or higher.
2. Create or update the Customers data model field display policy:
 - Go to the **Field Display Policies** page, then locate the entry for target model type, *relation/HcsCustomerREL*.
 - Click on the default field display policy (FDP) for the model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

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

- Modify the new FDP (the clone).

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

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



- Save your changes.

3. Update the menu layout to apply the field display policy:

- Go to **Menu Layouts**, and locate the Provider admin menu layout (HcsProviderMenu).
- Click on **HcsProviderMenu**, and create a clone with a new name.

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

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

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

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

4.8. Introduction to number management in Automate

4.8.1. Overview

Automate provides support for consolidating and managing your full number inventory. The system also supports various dial plan designs, whether E164 dial plans or traditional internal numbers mapped to external numbers.

The table summarizes Automate's main inventory capabilities:

Inventory capability	Description
Number Inventory	Automate's main inventory, also known as the <i>internal number inventory</i> (INI), contains all numbers that are assigned to devices, users, and services. While this is called an <i>internal</i> inventory, it can also include extensions (in traditional dial plans or for internal-only services), or full E164 numbers (if those are assigned directly to users, devices, and services).
E164 Inventory and Associations	An inventory that provides E164 numbers to map to the number inventory entries if they are <i>internal only</i> numbers, as required for traditional internal or external dial plans. In this inventory, internal numbers are assigned to devices and are then mapped to external numbers for external access. To use this inventory you'll need to load appropriate transformations and other dial plan elements. The association workflow when mapping E164 numbers to number inventory instances work with dial plan schemas or your own dial plan (dial plan tools). If E164 numbers are assigned directly to users, devices, and services, then those numbers are added directly in the number inventory and this E164 inventory and associations functionality is not required (and is then typically not visible in the system menus).

Once numbers are loaded into Automate, inventory details are shared and incorporated into other parts of the system, allowing users to choose numbers and to automatically track their status.

Automate provides the ability to reconcile (audit) the inventory against currently configured services in the event that changes are made outside the system, thus ensuring that the inventory stays up to date and accurate to reduce errors when selecting numbers or when manually reconciling.

Many of the inventory capabilities in the system focus around the internal number inventory as these are the numbers assigned to users, devices, and services directly.

Related topics

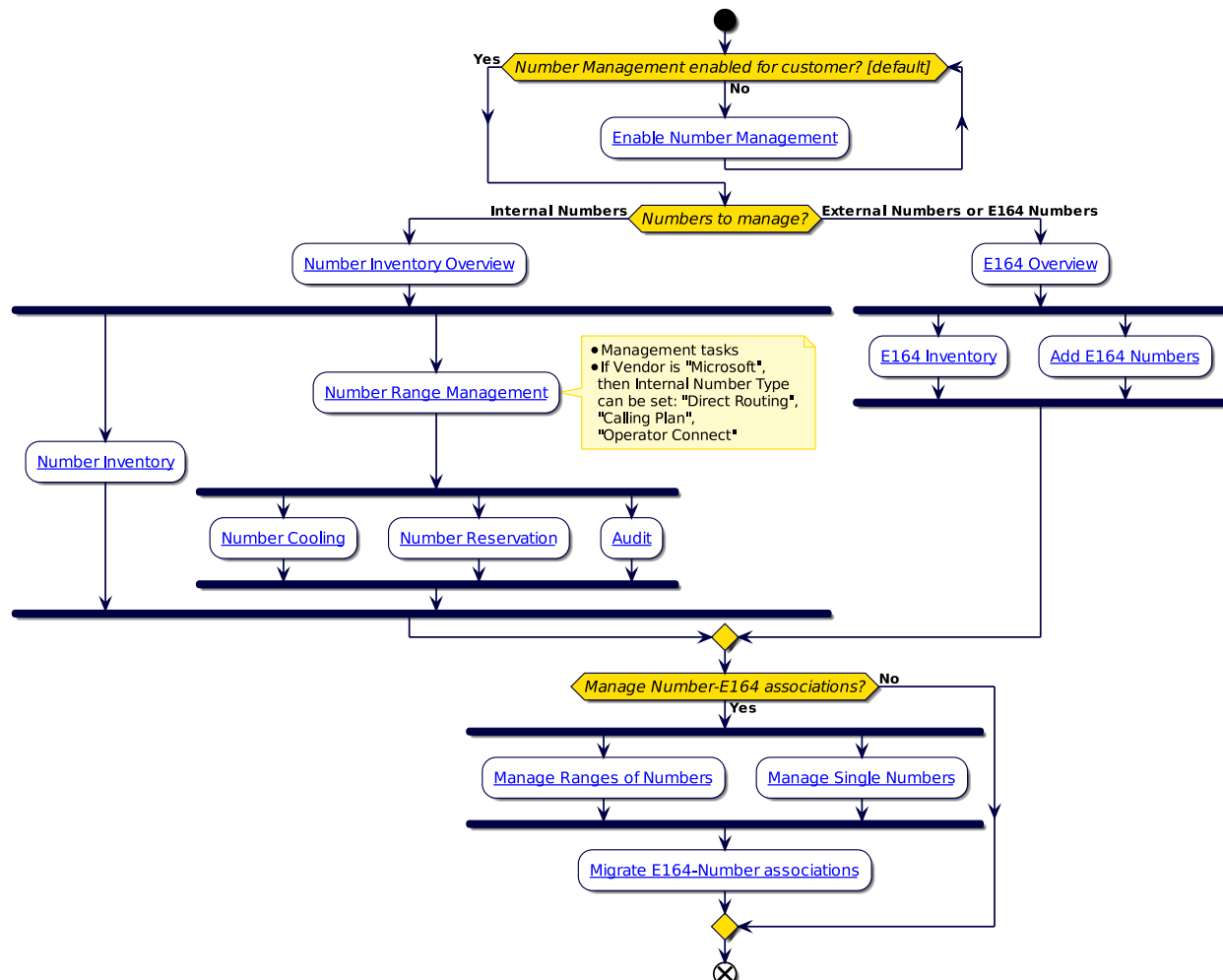
- [Number cooling](#)
- [Number reservation](#)
- Prevent duplicate numbers in the Core Feature Guide

4.8.2. Number management workflow in Automate

The flowchart in this section provides an overview of Automate's number management feature, highlighting internal number and external E164 number management and association.

Note:

- Number management functionality in Automate can be disabled for a customer if it's not required. To disable this feature, select the **Disable Number Management** setting. See: [Customers](#).
- E164 number management is used only in a Cisco UCM environment, which has the concept of internal numbers and associated E164 numbers. It is valid in Microsoft and in some Cisco deployments to add E164 numbers directly to the number inventory (and to completely ignore E164 number management).



4.9. Number inventory

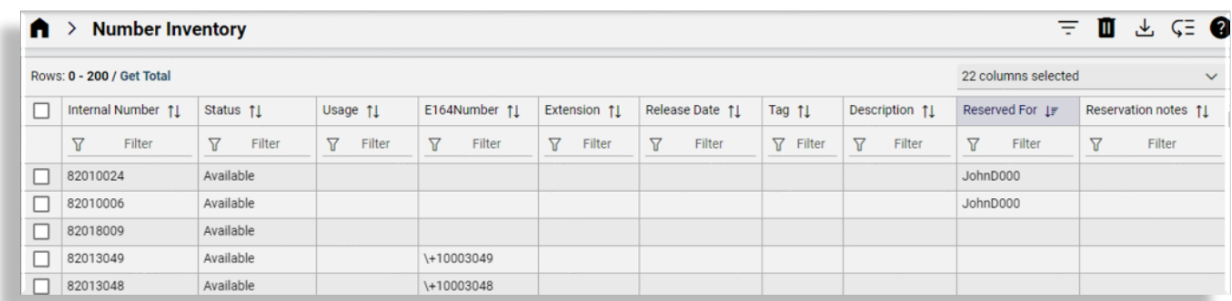
Tip: Use the Action search to navigate Automate

4.9.1. Overview

The Automate number inventory allow you to view and manage the numbers used by users, devices, and services for the given hierarchy level. The number inventory includes a combination of data that is automatically managed by the system (such as usage), and other fields that are configurable and available to store any additional useful information you choose about the numbers (such as ranges, billing IDs, and circuit IDs), to complete your inventory view.

Important: The number format in the Automate Internal Number Inventory (INI) is with prefix \+, including a leading slash \ when the INI is in E164 format.

Verify that entries in the **Internal Number** column of the Number Inventory - also Webex Calling numbers - follow this format.



Number Inventory									
Rows: 0 - 200 / Get Total								22 columns selected	
<input type="checkbox"/>	Internal Number ↑↓	Status ↑↓	Usage ↑↓	E164Number ↑↓	Extension ↑↓	Release Date ↑↓	Tag ↑↓	Description ↑↓	Reserved For ↑↓
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
<input type="checkbox"/>	82010024	Available							JohnD000
<input type="checkbox"/>	82010006	Available							JohnD000
<input type="checkbox"/>	82018009	Available							
<input type="checkbox"/>	82013049	Available		\+10003049					
<input type="checkbox"/>	82013048	Available		\+10003048					

The Automate number inventory functionality supports a range of capabilities outside of the basic loading and tracking of inventory status.

The table describes the additional number inventory capabilities:

Functionality	Description
Number Reservation	Numbers can be reserved and made unavailable until you change their <i>reserved</i> status (unreserve). Reserved numbers can't be assigned to any user, device, or service. When reserving a number you can add a note about why its reserved.
Reserved For	Allows the admin to flag numbers (INI) as reserved for a specific user. When used with the <i>next available number</i> option for onboarding and provisioning, the system first looks for a number reserved for the user you're working with. If there's a match, this number is assigned to the user at the site. If no match is found, the next available number is assigned to this user. A number that is reserved for a specific user cannot be assigned to a different user unless the Reserved For flag is removed.
Number Cooling	<p>Numbers can be placed into a cooling period, either manually or automatically. Placing a number into <i>cooling</i> quarantines the number for a specified number of days so that it can't be re-used for that period. When automated number cooling is enabled, numbers are placed into cooling for a predefined period when the subscriber or phone associated with the number is deleted. Automated number cooling is enabled and disabled in the Global Settings. The default is disabled.</p> <p>A number that is in <i>cooling</i> is unavailable and can't be allocated to a subscriber, phone, or device.</p> <p>A number is released from cooling and is available for use when:</p> <ul style="list-style-type: none"> • The cooling period reaches its end date • The number is manually released from the cooling period
Number Audit	Checks the inventory against the currently configured devices and updates the inventory where needed to keep the inventory in sync for changes made outside the system.
Number Inventory Alerting	Configure alerts to be sent if a threshold is met (e.g less than 10% of numbers are available) to allow for proactive management of the inventory.

Note: Typically, numbers are pushed to the UC applications when they're assigned to users, devices, or services.

While some available numbers may be in the UC apps for various reasons, the platform is not trying to maintain the available numbers in the underlying UC applications as it is only important when assigning the numbers to be used.

Related Topics

- [Number inventory alerting](#)
- [Number cooling](#)
- [Global settings](#)
- Reserve a number for a user in the Core Feature Guide

4.9.2. Number inventory and hierarchy in Automate

To ensure proper visibility and allocation, numbers should be added to the inventory at the correct hierarchy level in Automate, based on where and how they will be used. Proper planning of hierarchy and inventory allocation is essential for a scalable and efficient setup when building out the number inventory.

Hierarchy relationship

- Inventory numbers can be placed at the same level or higher than the users, services, or devices they're assigned to.
- The hierarchy level of a number determines its visibility for MACD (Move, Add, Change, Delete) operations like user onboarding.

Choosing the right hierarchy level

Consider the following scenarios when deciding where to load inventory numbers:

- **Site-level numbers**

Use the site level if numbers are tied to a specific site due to:

- Local trunks
- Area codes
- Emergency routing

Assign these numbers directly to the site in Automate so they're only available for that site's users and services.

- **Intermediate nodes**

If a number range is shared across multiple sites within a region, city, or country:

- Group the sites under an intermediate node.
- Assign the inventory to that node to allow shared access across all included sites.

- **Global use**

If numbers aren't tied to specific sites:

- Assign these numbers to a common hierarchy node, such as customer level.
- This is ideal for centralized environments or enterprises operating within a single region.

Dial plan considerations

If using dial plan schemas, the schema rules may dictate where numbers must reside. For example, site-based dial plans with site codes require numbers to be loaded at the site level.

System behavior

Automate does not automatically move inventory numbers to match the hierarchy of the assigned service.

- Example: A number at the customer level assigned to a site user will remain at the customer level unless manually moved.
- Admins can relocate numbers if needed, but this is not required (the admin may simply prefer the number to be at the same hierarchy).

Typical usage

Users, devices, and services that will consume numbers usually exist at the site level. Therefore, inventory numbers should be placed at the same site, or above (intermediate or customer level).

You can also combine strategies:

- Site-specific numbers at the site level.
- Shared pools at intermediate or customer levels.

4.9.3. Number inventory and end-user provisioning

The number inventory is integrated into various features in the system to:

- Display options of numbers for selecting/assignment across the system. Numbers presented for selection follow rules specific to the feature in many cases, for instance, whether lines can be shared or not.
- Manage the state of the numbers in the inventory via the workflows - marking the number used, available, and updating other managed fields depending on the MACD being performed. This includes any specific logic setup for the un-managed fields. See the section on flexibility for options to control the update that occurs.

Related Topics

- [Number status and usage](#)
- [Number cooling](#)
- [Number reservation](#)
- [Number inventory alerting](#)
- AudioCodes Device Number Integration in the Core Feature Guide

4.9.4. UC vendor guidelines for numbers

This section provides UC vendor-specific guidance and behaviors related to how their numbers are handled in Automate.

Cisco UCM/dedicated instance

When the Automate number inventory is used in a Cisco UCM/Webex Dedicated instance environment:

- The value for the **Vendor** field is either *Cisco* or blank, depending on how numbers are loaded
- The **Internal Number Type** field is not relevant in UCM or Dedicated Instance deployments

Partition and cluster

The Automate number inventory is not partition or cluster aware:

- If the same numbers are used multiple times but in different *partitions*, these all map to the same number. This should be considered for the hierarchy level at which the number inventory exists.
- If the same number exists on different *clusters*, this will map back to the same inventory value unless numbers are assigned to the site level.

Cisco-Microsoft hybrid number inventory

This section applies if you're using Automate's Cisco-Microsoft hybrid feature for integrated services.

A Cisco-Microsoft hybrid setup is an integration of Cisco and Microsoft capability, where Microsoft calls are routed via Cisco UCM.

In a hybrid setup, the internal number inventory (INI) can be set up in two ways:

- E164 number based, for example:
 - an INI entry 3334567 is mapped to an external number of +15553334567.
 - The number 3334567 is set up in Cisco (along with routing for the mapped external number).
 - The number +15553334567 is set up in Microsoft as the line.
 - The numbers 3334567 and +15553334567 should be seen as the *same* number from an INI tracking perspective.
- Internal number based (site code+extension or just extension)
 - an E164 number is generated by adding a prefix (+88800) to the internal number for setup in Microsoft.

Note: A name macro, `MultiVendorLine-InternalExt-E164Prefix`, is used to store the prefix - currently set to `+88800`.

- For example, 3334567 is set up as an internal number for the user and no external number is mapped. The line is selected in the Hybrid setup. Then the prefix is added, so the number +1888003334567 is the number in MS Teams for that user.

Important: The numbers 3334567 and +888003334567 should be seen as the *same* number from an INI tracking perspective. The mapping is also reflected in the [Number inventory audit](#). In this case, an update of the inventory takes place so that these are not counted as two separate numbers.

The table summarizes the number inventory data for these cases:

Note: **Extra2** and **Extra4** hold the service type and E164 number (includes generated) respectively.

Scenario	Status	Vendor	E164 Num-ber ⁷	Usage	Extra2	Extra4
Cisco-MS-Hybrid	Used	Cisco, crosoft	Mi- Exists	Device, User	Cisco-MS-Hybrid	<blank>
Cisco-MS-Hybrid ⁸	Used	Cisco, crosoft	Mi- <blank>	Device, User	Cisco-MS-Hybrid	+88800<INI>
Cisco-No-Services	Avail	<blank>	<blank>	<blank>	<blank>	<blank>
Cisco-Only	Used	<blank>	Exists	Device	<blank>	<blank>
MS-Only-Entvoice	Used	Microsoft	Exists	User	MS-Only-Entvoice	<blank>
MS-Only-Entvoice	Used	Microsoft	<blank>	User	MS-Only-Entvoice	+88800<INI>
MS-Only-Hybrid	Used	Microsoft	Exists	User	MS-Only-Hybrid	<blank>
MS-Only-Hybrid	Used	Microsoft	<blank>	User	MS-Only-Hybrid	+88800<INI>
MS-Only-No-Entvoice	Avail	<blank>	<blank>	<blank>	<blank>	<blank>
No-Hybrid-Service	Avail	<blank>	<blank>	<blank>	<blank>	<blank>

For details on the service type scenarios, see Multi Vendor Service Definitions in the Core Feature Guide.

Footnote

Microsoft Teams deployments

The use of the inventory and how it is maintained or managed can differ depending on the types of numbers in your environment. The following is some guidance and best practices to consider for the different number types. If you have a mix of number types, then consider the notes for different number types.

In the number inventory:

- The **Vendor** field value is typically Microsoft. If numbers aren't loaded with this value initially, the system updates the numbers as they are allocated to vendor Microsoft.

⁷ If assigned (and associated with Extra4 - prefix e.g. +88800)

⁸ Generated TelURI will start with prefix e.g. +88800

- The **Internal Number Type** field is used to reflect the type of number in a Microsoft environment, either of the following:
 - Direct Routing
 - Operator Connect
 - Calling Plan

The internal number type can be selected when loading the numbers. It is recommended that the relevant values are chosen. Typically, the system also updates the value for this field as required during audit or allocation of numbers, if they're incorrect or left blank.

General Notes

The hierarchy consideration is a key section in this chapter to read in planning for numbers in the inventory. Often the numbers are meant to be used in specific sites or regions only due to agreements or emergency services requirements. This is the business context which the Automate number inventory can provide when the numbers are loaded into the inventory at the appropriate hierarchy level. It is often found, after adding Automate to an existing environment, that we identify various numbers that have been incorrectly assigned previously and allow them to be corrected. Any numbers that were added to the Automate inventory through the sync/audit process will likely require moving to the correct hierarchy level. You can find more information related to the specific numbers types below.

This section covers specific logic related to creating and managing the inventory in relation to specific number types in the Microsoft environment. In Automate you can mix and match the types for different needs, so one or more of the sections may apply.

Direct Routing

In this type of setup, you are getting ranges of numbers outside the Microsoft framework from one or more providers. For these number types, the Microsoft tenant only knows about the numbers that you have assigned to users/services. The tenant has no knowledge of the ranges or available/unused numbers.

So the Automate number inventory capability can only auto-populate the inventory from a sync/audit with those used numbers discovered from the tenant. In this scenario, you will need to load the available numbers into the Automate number inventory to be managed and available for administrators to assign going forward.

Guidelines for this setup:

- You can preload the ranges of numbers you own ahead of any overbuild process that will sync/audit the inventory. In this case, the system will update the inventory as part of the sync/audit process to mark assigned numbers used. It will still add any used numbers it discovered from the tenant if there were any missed in the preload process.
- You can load the full ranges after the overbuild process - this will fill in the inventory around the used numbers that were discovered and auto created in the inventory from the tenant. You may need to move the created numbers to a different hierarchy level depending on your needs (intermediate node, moving to site/customer). When you load the ranges after the sync/overbuild, the system will fill in the gaps by adding numbers as available that are missing in the inventory while leaving the ones added via the sync/audit process alone.
- Any future ranges you add to the system beyond the initial overbuild will need to be added to Automate to be available for administrators to use.

Operator Connect and Calling Plan numbers

In this type of setup, you are getting ranges facilitated by the Microsoft Teams framework. For these types of numbers, the Microsoft tenant is fully aware of the ranges of numbers available as they are populated into the system by Microsoft (Calling Plans) or the selected Provider (Operator Connect). So it is important to note the numbers can only actually be used (e.g assigned to a user) when the numbers are available in the Microsoft Tenant post ordering – from Microsoft (Calling Plan) or the selected Provider (Operator Connect). If you add them to the Automate inventory and try to allocate them before they are present in the tenant, you will get an error message about the numbers not existing in the tenant.

Currently, the data we receive from the Microsoft tenant about the numbers does not provide any information regarding how the numbers are to be used - e.g site specific, etc.

The hierarchy recommendations earlier in this chapter should be referenced and numbers should be loaded according to how the numbers are ordered and registered with Microsoft or the Provider (e.g site specific, global, etc).

The best practice recommendation to streamline the inventory management of these number types is:

- Number ranges are loaded into the Automate number inventory at the appropriate hierarchy *before* they're synced in from the Microsoft tenant
- This ensures that the numbers are at the correct hierarchy level and context in the system for use in the system - that users and services can only be assigned appropriate numbers.

Important: New Calling Plan numbers cannot be assigned to users unless an emergency location is set.

To set the emergency location for new Calling Plan numbers:

1. Select the relevant customer or site hierarchy, then go to **Emergency Location Ops Tool**.
 2. On the Ops Tool form, verify that **Number Type** is set to `CallingPlan`.
 3. Select an **Emergency Location** from the drop-down. Also ensure a temporary user is created at the location and has the Calling Plan assigned.
 4. Click **Save** to update the emergency location of the numbers at this hierarchy where this has not been set.
-

- When the sync/audit process completes, the system updates those inventory entries with status, usage, type, etc., and won't move them.

Automate can generate inventory entries for numbers of these types. However, there are some considerations and for this reason it is recommended to preload the numbers for improved accuracy and ease of use.

The following are considerations of the generated inventory and potential actions if the sync/audit was run before you loaded your inventory:

- It will generate inventory entries for numbers assigned to users/services in the tenant only. We do this for assigned numbers to ensure they are at least captured and since they are assigned there is not a risk of being assigned incorrectly.
- Numbers that are not assigned will not be generated in the inventory. This is to avoid available numbers being created at the wrong place in the hierarchy and inadvertently being assigned to users in the wrong sites, etc.
- It will create the generated inventory entries at the same hierarchy level as the tenant details (typically customer). Typically, they are required at a different level in the hierarchy and they will need to be moved after this creation.

- The ranges will need to be loaded to create the available numbers in the range within the inventory so they are available to be assigned to users/services. You can just load the whole range and the system will fill in the blanks, creating inventory entries for missing numbers while leaving existing numbers (created by the sync) alone.

You can look at the number data provided by Microsoft for these number types by reviewing the `device/msteamsonline/Number` device model. Note - these model instances will always be at the same level as the tenant - they do not get moved around and are completely independent of the inventory entries for the numbers.

4.9.5. Number inventory for Webex Calling

This section describes number inventory handling in a Webex Calling environment.

Key considerations in a Webex Calling environment:

- In a Webex Calling environment, resources all reside in locations including numbers regardless of the source (for example, CCP, non-integrated CCP, or Cisco).
- PSTN numbers must be loaded into Webex as available numbers before they can be used/assigned to users. This process can vary depending on how you're sourcing the numbers - for example, CCP, or Cisco Cloud. For this reason, the numbers are typically already in Webex - to pull into the Automate system and inventory.

From the **Number Range Management** page at a site:

- For numbers and ranges of numbers, **Starting Extension** and **Ending Extension** number values must be prefixed with + and are then created and maintained in Automate with the prefix format \+. When adding numbers, this can also be seen in the **Transaction** detail.
- **Vendor** – this field will typically be Webex Calling. If they are not loaded with this value initially, the system will update the numbers as they are allocated to vendor Webex Calling.

Note: Numbers can be pushed to the Webex Control Hub when adding number ranges at site level with the Vendor set as Webex Calling.

The screenshot shows the 'Number Range Management' interface. The main form is titled 'Base' and contains the following fields:

- Operation:** A dropdown menu set to 'Add'.
- Target Site *:** A dropdown menu set to 'Site1'.
- Starting Extension *:** A text input field containing '+155512340'.
- Ending Extension *:** A text input field containing '+155512349'.
- Status *:** A dropdown menu set to 'Available'.
- Vendor:** A dropdown menu set to 'Webex Calling'.
- Internal Number Type:** A dropdown menu set to 'Phone Number'.

On the right side, there is a 'Webex Control Hub' panel with two checkboxes:

- Push Numbers to Webex:** Checked (indicated by a blue checkmark).
- Push as Active:** Checked (indicated by a blue checkmark).

- If the **Operation** is *Add*:

When *adding* numbers and selecting the **Vendor** as Webex Calling, a **Webex Control Hub** panel displays the options if:

1. The Webex App is configured at the customer hierarchy.

See the Webex App chapter in the Core Feature Guide.

2. The available macro `WebexCallingNumberMgmtEnabledSite` has not been cloned to the site and set to value `False`. (If required, this task can be carried out if Webex Calling number management should be disabled for a site.)

The options are:

- **Push Numbers to Webex:** this allows for numbers to be added to the site in Automate and to the Webex Control Hub. (Refer to the `Create Spark Number` action in the **Transaction** list.)
- **Push as Active:** dependent on the option **Push Numbers to Webex** set to enabled.

If enabled and **Push Numbers to Webex** is enabled, numbers are added in Automate INI added as **Status of Available**, and on Webex Control Hub created as **Active**.

If disabled and **Push Numbers to Webex** is enabled, numbers are added in both Automate INI and the Webex Control Hub as **Inactive**.

Number extensions are added to the INI when a user is assigned a number and an extension is then added.

- If the **Operation** is **Modify**:

This operation can be used on selected numbers that are in **Status of Inactive** - to set them as:

- **Active** in the Webex Control Hub. Refer to the `Activate Spark Number` action in the **Transaction** list.
- Status is **Available** in the Automate INI.

- If the **Operation** is **Delete**:

Selected numbers are deleted from Automate INI and the Webex Control Hub. Refer to the `Delete Spark Number` action in the **Transaction** list.

- **Internal Number Type** – this field is used to reflect the type of number in the Webex environment. If you are adding or activating numbers via Number Range Management then the type is `Phone Number`. Any numbers marked as `Extension` have been synced in from the Webex Control Hub.

Since the numbers are known in the Webex environment, as well as the Locations for use, the Automate system will generate the inventory based on the data from Webex. This includes:

- The sync process handles the creation of inventory entries in the Automate platform as numbers are pulled in. You should ensure the sync process handles Locations in Webex prior handling numbers (out of the box syncs ensure this).
- During a site handling Webex Locations, if a corresponding Automate site does not exist, Automate will create a site.

See the Webex Location Node Mapping topic in the Core Feature Guide for more details on Site to Location mapping for Webex for more details on how they are aligned.

- When Webex numbers are synced into Automate, the prefix format `\+` is used. Any inventory entries that don't exist are created in the Automate site corresponding to the Webex Location. This includes PSTN numbers and also internal-only extensions.
- The internal number in the Automate number inventory uses the PSTN number (if it has one); or it uses the extension number, if that is the only data available.
- For PSTN numbers, the extension (if there is one) is also captured in the number inventory record via the **Extension** field.

- Removal of numbers
- Typically, inventory audit functionality won't be required if good sync practices are followed, as the inventory changes are handled through the sync process.

4.10. View number details and usage

Tip: *Use the Action search to navigate Automate*

4.10.1. Overview

To view the details of a number in the number inventory, go to the **Number Inventory** list view, then click on a number to open its details page.

Related topics

- [Number range management](#)
- Prevent duplicate numbers in the Core Feature Guide

4.10.2. Number settings

The management page for a number contains two tabs/panels:

Note: You can toggle between a tab/panel layout via a toolbar icon.

- Number Details
- Usage

Number Management > Number Inventory > 1001

Number Details	Usage
Internal Number * 1001	Extension Mobility
Status * Available	Extension Mobility
Vendor	Extension Mobility
Usage	Extension Mobility
E164Number	Extension Mobility
Release Date	Extension Mobility
Internal Number Type	Extension Mobility
Tag test	Extension Mobility
Description	Extension Mobility
Reserved For JohnD000	Extension Mobility
Reservation notes	Remote Destination Profile (SNR)
Extra1	Remote Destination Profile (SNR)
Extra2	Remote Destination Profile (SNR)
Extra3	Remote Destination Profile (SNR)
Extra4	Remote Destination Profile (SNR)
Extra5	Remote Destination Profile (SNR)
Extra6	Remote Destination Profile (SNR)
Extra7	Remote Destination Profile (SNR)
Extra8	Remote Destination Profile (SNR)
Extra9	Remote Destination Profile (SNR)

Number Details tab/panel

The **Number Details** tab/panel displays both read-only and editable fields. For example, you cannot update the internal number, or its status, vendor, usage, E164 number, or release date (if applicable).

Note: In the case of Cisco-Microsoft hybrid entries, the vendor added would be “Cisco, Microsoft”.

You can update the following details for a number on the **Details** tab/panel:

- Update the internal number type
- Add or edit a tag
- Add or edit a description
- Choose a user to reserve this number for
- Add reservation notes
- Fill out additional custom attributes

The table describes the fields on the **Number Details** panel/tab:

Column	Description
Internal number	Numbers created in the number inventory are in Automate only. These are not synced to Cisco UCM.
Status	Current status of the number. Options are: <ul style="list-style-type: none"> • Available • Used-Utility • Used • Cooling • Reserved
Vendor	Optional, typically used to designate vendor-specific information for a device in a multi vendor setup.
Usage	Available and Usage is empty when a number is first added to the number inventory.
E164Number	Displays E164 Associations (N to 1 DN), depending on the number of E164s associated and whether a primary E164 is set or not.
Release Date	Defines the date on which a number that is currently in Status : Cooling or Reserved will become available again.
Internal Number Type	Used in conjunction with the Vendor field. See the vendor specific section of Number Inventory topic for more details on usage in different vendor use cases.
Tag	A free text field, auto-populated when a new number or range of numbers is added. Used to identify or comment on a number or number range.
Description	Free text field, available to provide additional information for a given number or range of numbers.
Reserved For	If you want to reserve a number for a specific user, choose the user from this drop-down.
Reservation notes	A free text field, typically used to provide more details about a status Reserved number.
Extra	Extra1 to Extra9 fields are free text fields that are available to provide additional information for a given number or range of numbers. Field Display Policies can be used to change the field names and also add tooltip help text to reflect how you want to use the fields.

Usage tab/panel

The **Usage** tab/panel provides links to all instances where the number is used, representing a dynamic view of all the service(s) that are assigned to that number. This includes links to easily navigate to the service instance for further details or to unassign the number if required.

Note: If the same number is shared by multiple devices/services of the same type, only the first 10 instances display.

- In the case of Cisco-Microsoft hybrid usage, the last vendor added would be appended, as seen above in the “Device, User” instances.
- In the case of **Webex App Calling** usage, the link directs to the Webex App user.

See *Webex App* in the Core Feature Guide.

Note: If the same number is shared by multiple devices/services of the same type, using different partitions, only the first 10 instances are displayed.

Related topics

- Webex App in the Core Feature Guide.
- Prevent duplicate numbers in the Core Feature Guide

4.10.3. Managed and non-managed number inventory fields

Automate provides two types of number inventory data fields, managed by Automate, and un-managed:

- Managed - managed by Automate:
 - **Status** - managed automatically by the system
 - **Vendor** - can be set on loading the range; afterwards it is managed automatically.
 - **Usage** - managed automatically
 - **E164Number** - if the number has an E164 number associated in the system it is shown here (read only). If not using E164 number inventory, then not relevant and you can hide the field.
 - **Release Date** - if the number is in Cooling, this is the date/time the number will become available - managed automatically. See number cooling for how to change the cooling status for a number.
 - **Internal Number Type** - set when adding then managed automatically if relevant.
- Un-managed - not managed by the system:
 - **Tag** - free text and can be utilized as needed
 - **Description** - free text field that can be utilized as required for additional useful information
 - **Extra 1-9** - free text field that can be utilized as required for additional useful information

These additional useful information fields can be utilized to store any extra business information you require to store in the inventory with the numbers. This can be static data defined when the numbers are loaded or updated or it can be dynamically updated as the system manages the numbers (allocated to a user, unassigned, etc). For instance, the system provides some out-of-the-box options for description to utilize, or if you want to set a value in **Extra1** when events happen in the system.

See Number Inventory Flexibility and Description Customization in the Advanced Configuration Guide on how to utilize this capability.

If you are using any of the fields to store additional information, you can re-label the fields and include relevant help text for tool tips to be meaningful for administrators according to the data you are storing (e.g Billing ID if using a field for that) by means of a Field Display Policy for the `relation/NumberInventory` model.

For more details on the automated logic for managing status and usage, see [Number status and usage](#).

4.10.4. Edit a number via the number inventory

You can update some (editable) details for a number when clicking on that number from the **Number Inventory** page.

To modify a range of numbers, see [Number range management](#).

4.10.5. Reserve a number for future use via the number inventory

To reserve a number that you're viewing from the number inventory:

1. Go to the **Number Inventory** list view.
2. Click on an unused number to open its detail view.

Note: Only numbers that are currently in status *Available* or already in *Reserved* state can be moved to reserved state.

3. From the toolbar overflow menu, select **Reserve Number**.

Note: If the transaction succeeds, the number is reserved.

Related topics

- [Number range management](#)
- [Number reservation](#)
- [Number status and usage](#)
- [Number cooling](#)
- Reserve a Number for a User in the Core Feature Guide

4.11. E164 numbers in the number inventory

Note: In Automate, a wildcard (*) can appear before a directory number in a Type 4 dial plan.

The **E164Number** column and value displays E164 Associations (N to 1 DN), depending on the number of E164s associated and whether a primary E164 is set or not.

Examples of E164 format:

Note: The first example below is for E164 Associations (N to N DN):

- \+27726043938

No primary is set. The first number associated is displayed. Only one number is associated.

- \+27726043938 (P)

The displayed number is primary. Only one number is associated.

- \+27726043938 (P) [+8]

The displayed number is primary. Eight (8) more numbers have been associated in addition to the displayed number.

- \+27726043938 [+8]

No primary is set. The first number associated is displayed. Eight (8) more numbers have been associated in addition to the displayed number.

This type of number cannot be reached from an outside line. Typically, a number with the '*' prefix is not called from another line (user), but is tied to a service feature such as call pickup, hunt groups, or contact center.

Note: Adding a new number to the number inventory on Automate does not add a number on Cisco Unified Communications Manager (CUCM / CallManager) until it is associated to a line.

4.12. Number status and usage

4.12.1. Overview

Values in the **Status** and **Usage** columns in the number inventory allow administrators to understand how numbers are used at a specific hierarchy level.

Tip: *Use the Action search to navigate Automate*

The table describes values in the **Status** and **Usage** columns in the Number Inventory:

Number Use	Device	Status	Usage	Vendor ^{Page 49, 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
Webex User	device/spark/Number	Used	User	Webex Calling
Number inactive		Inactive ³	blank	Webex Calling
AudioCodes devices	device/audiocodes	Used	Device	AudioCodes ⁴
Not used by anything		Available	blank	blank, Microsoft, Webex Calling

¹ Default vendor value is blank (for Cisco).

² If a number is used by both a Phone and Hunt Pilot then the **Usage** column will display both usage values, i.e. Device, Hunt_Pilot. This could be the case if you change the Partition and enter the DN manually so that they share the same DN.

However, the **Status** column will display only *one* status: the status triggered by the most recent transaction. The Status would change from Used to Used-Utility if you added the Hunt Pilot last. If it was already a Hunt Pilot and then you added it to a Phone, then Status would change from Used-Utility to Used.

Numbers can also be shared between Call Handlers and one or more device types. Status depends on whether Call Handler or devices were added first to the number. Usage will typically be Call_Handler_Pilot, Device.

³ Status is Inactive by adding a number in Number Range Management, where **Vendor** is Webex Calling and **Push as Active** is unchecked on the **Webex Control Hub** frame on the input form.

Modifying the number in a range by setting the status as Available will activate it in the Webex Control Hub and update its status.

⁴ For AudioCodes, see the AudioCodes topic in the Core Feature Guide.

Number Use	Device	Status	Usage	Vendor ¹
Number in cooling ⁵		Cooling	-	blank, Microsoft, Webex Calling
Number reserved ⁶		Reserved	-	blank, Microsoft, Webex Calling
Webex Calling ownerType is unset	device/spark/Number	Available	-	Webex Calling
Webex Calling ownerType is PEOPLE	device/spark/Number	Used	User	Webex Calling
Webex Calling ownerType is <i>not</i> unset or PEOPLE	device/spark/Number	Used-Utility	Matches the ownerType: Device (for PLACE), Auto_Attendant, Call_Queue, Group_Paging, Hunt_Pilot, Voice-mail_Pilot, Broadworks_Anywhere, Contact_Center_Link, Route_List, Voice-mail_Group	Webex Calling

For further details on Vendor and Internal Number Type fields – see [UC vendor guidelines for numbers](#).

Related Topics

For details on call handlers and shared numbers, see Auto-Attendant Call Handler in the Core Feature Guide.

4.13. Number range management

Tip: [Use the Action search to navigate Automate](#)

⁵ If a number is currently in **Cooling**, the release date indicates when the number will come out of cooling.

⁶ If a number is currently **Reserved**, you can enter an optional **Tag** to identify the user for which the number is reserved. An optional **Reservation notes** field is also available to allow you to enter additional information regarding the reserved number.

4.13.1. Overview

Automate's number range management feature allows you to add and manage a range of internal numbers, at a customer, at a site, or at an intermediate node.

Note: An internal number range created at an intermediate node is also available at the sites below this intermediate node.

You can add an internal number range that includes existing numbers, but in this case, it is not possible to modify the existing numbers. New, unused numbers are added only to complete the range. This means that the number range will display as complete, with unused numbers displaying along with numbers imported from Cisco UCM.

For Microsoft deployments, if you wish to prevent the creation of duplicate numbers when creating a number range, enable (set to *Yes*) the *Prevent Duplicate Numbers* global setting. See:

- Prevent duplicate numbers in the Core Feature Guide

>

Number Range Management

Base

Operation

Add

Target Site

LOC001

ISP

8

Extension Length

4

Site Location Code

8201

Starting Extension *

Ending Extension *

Status *

Available

Reserved For

JohnD006

Vendor

Microsoft

Internal Number Type

Calling Plan

Tag

Description

Extra1

Note: Using a bulk loader sheet or the API, you can create the number inventory at the customer hierarchy only. The **Details** column of sub-transactions shows whether the number already exists or if it is creating a new number. If any numbers exist in the range, the sub-transaction fails and the parent transaction shows the status *Success with Async Failures*.

While you can delete a number range, only numbers in this range with a status of *Available* can be deleted. Numbers in the range with the following statuses are ignored and can't be deleted unless their status changes to *Available*:

- Used
- Used-Utility
- Reserved
- Cooling

Numbers with status *Available* and *Reserved* can be modified manually once they're added.

Numbers can be added, edited, or deleted. When modifying a number, you can only edit the free text fields. The usage and availability property for each number is associated with a line or taken into use by a service.

The number inventory isn't partition-aware so if the same directory number is used on a cluster but in different partitions, Automate updates the inventory when any of these instances are changed. For example, if there's a number, *1111*, in the *Cluster X* partition, and a number, *1111*, in the *Cluster Y* partition, this number is marked as *Used*. If either of these instances are deleted, Automate checks whether other instances of this line exists (based on the number only, not partition) before it clears the *Used* flag. If other instances exist, the number status remains as *Used*.

Tip: [Use the Action search to navigate Automate](#)

Related topics

- For details around managing number ranges specific to the UC vendors you're using, see [UC vendor guidelines for numbers](#)
- Reserve a Number for a User in the Core Feature Guide
- Prevent duplicate numbers in the Core Feature Guide

4.13.2. Manage numbers and number ranges

Tip: [Use the Action search to navigate Automate](#)

This procedure adds, updates, and deletes numbers and number ranges.

Note: If you don't want the system to create duplicate numbers when creating a number range (duplicates of numbers in the range already exist), enable (set to *Yes*) the *Prevent Duplicate Number* global settings.

1. In the Admin Portal, go to **Add Internal Number Inventory**.
2. Select the relevant hierarchy, customer or site.
3. Optionally, choose a target site.

Note: Target site may be auto-populated as a read-only field if you've chosen to open this page from the site hierarchy. If you've opened this page from the customer hierarchy, you may need to select a

target site (mandatory in some dial plans, such as site code based dial plan).

4. At **Operation**, choose an option:

- **Add or Modify?**

- By default, **Status** is set to *Available*.
- When changing status to *Reserved*, optionally, fill out a value for **Reservation duration (days)**, for example, *30*. At the end of this period, status returns to *Available*. If no value is specified the numbers are reserved indefinitely.
- If you choose **Modify** and wish to modify the range free text fields (see below for details), then manually set the **Status** drop-down to *Unchanged*. This allows for the modification of the fields of numbers in the range - regardless of current number status - without modifying the original number **Status**.

- **Delete?**

- Only the following fields are now available: Target Site, Starting Extension, Ending Extension
- When deleting a number range, you won't be able to mark lines as either **Available** or **Reserved** (these options won't display on the form).
- If a number in a deleted number range was set at *Used*, it won't be deleted.

5. Fill out a starting and ending extension.

Note: The maximum allowed range is 1000 for a single action. The starting extension should always be smaller than the ending extension.

If you're adding or deleting a single number, the starting and ending extension number will be the same. If numbers in the range already exist, they won't be affected - only non-existing numbers will be added.

6. If required, at **Reserved For**, you can reserve a number for a specific user. Choose an existing username, or fill out a custom value. Here you can also remove the *Reserved For* flag (clear the field) to allow the number to be assigned to other users.
7. At **Vendor**, select the relevant vendor for the number range (Cisco, Microsoft, Cisco/Microsoft, or Webex Calling).
8. Based on the vendor you chose, select an appropriate option at **Internal Number Type** (direct routing, calling plan, or operator connect).

Note: For more information for your use case, see [UC vendor guidelines for numbers](#)

9. Optionally, fill out values for the additional free text fields, for example **Tag**, **Description**, **Reservation notes**, **E164Number** (if applicable), and **Extra1** to **Extra9**.

These values can be updated for a range of numbers - regardless of the number **Status** in the range - by setting the **Status** drop-down to *Unchanged* during the update process. The original number **Status** in the range will remain unchanged.

10. Save your changes.

Note: Numbers at a specific hierarchy can be viewed on the **Number Inventory** list view. See [View number details and usage](#).

When a line is added and selected from the drop-down list of available numbers, it has a status of **Used**. If the line is used by a device or service that does not allow a shared line (for example, a Hunt Pilot), it has a status of **Used-Utility**. See [Number status and usage](#).

Internal numbers are available when adding users.

Related topics

- [UC vendor guidelines for numbers](#)
- [Number status and usage](#)
- [View number details and usage](#)
- Reserve a Number for a User in the Core Feature Guide
- Number Reservation
- Prevent duplicate numbers in the Core Feature Guide

4.13.3. Modify a number in the number inventory

This procedure modifies an individual number via the number inventory list view.

Tip: [Use the Action search to navigate Automate](#)

1. In the Admin Portal, go to **View Internal Inventory**.
2. Click on the relevant number in the list to view its detailed management page.
3. Choose an available edit option:
 - To reserve the number, click the vertical ellipsis toolbar button to display the overflow menu, then select **Reserve Number**. Transaction is scheduled for processing. When done, the status of the number changes to *Reserved*.
 - To select the internal number type, select an option at **Internal Number Type**, either Direct Routing, Calling Plan, or Operator Connect.
 - Edit free text fields, such as Tag, Description, Reservation notes, E164Number (if applicable), and Extra1 to Extra9.
 - To reserve a number for a specified user, at **Reserved For**, choose an existing username or fill out a username for a new user. This number won't be available for allocation to any other user until you remove this *reserved for* flag.
4. Save your changes.

Related topics

- [View number details and usage](#)
- Reserve a number for a user in the Core Feature Guide

4.13.4. Number range management Extra1 to Extra9 fields

When editing numbers in the Number Inventory or when adding or updating number ranges, you can modify values in additional fields called **Extra1** to **Extra9**.

- When the status of a number changes, for example, from *Used* to *Available* - this may occur when an associated device is unassociated with the line - then any values originally in any of the **Extra1** to **Extra9** fields, remain unchanged by default.
- A default custom Configuration Template (CFT), `IniUpdateCustomCFT`, which applies to `data/InternalNumberInventory`, can be cloned to the user hierarchy and then to modify the custom persistence of extra field values.

For more information around CFT cloning and custom configuration, see the Advanced Configuration Guide.

Important: Any changes to this custom CFT *only* apply to updates in workflows resulting in number status changes - manual updates are *not* affected.

The following default values in this CFT can be modified according to your needs:

```
"description": "{{ pwf.ini_dat_before.description }}",
"extra1": "{{ pwf.ini_dat_before.extra1 }}",
"extra2": "{{ pwf.ini_dat_before.extra2 }}",
"extra3": "{{ pwf.ini_dat_before.extra3 }}",
"extra4": "{{ pwf.ini_dat_before.extra4 }}",
"extra5": "{{ pwf.ini_dat_before.extra5 }}",
"extra6": "{{ pwf.ini_dat_before.extra6 }}",
"extra7": "{{ pwf.ini_dat_before.extra7 }}",
"extra8": "{{ pwf.ini_dat_before.extra8 }}",
"extra9": "{{ pwf.ini_dat_before.extra9 }}",
"tag": "{{ pwf.ini_dat_before.tag }}"
```

The default macros for each extra field can thus be replaced inside the cloned CFT with custom text and macros as needed. Use the macro `{{ macro.CLEAR }}` if it is necessary to clear a field.

- The **Description** field is *always* cleared when the status of the number changes to **Available**, regardless of CFT value. For other number status changes, the CFT value will apply.

There is full customization functionality of the **Description** field available to allow values in accordance with Automate feature usage.

For details, see the **Number Inventory Flexibility and Description Customization** topic in the Advanced Configuration Guide.

- This CFT can't be used to modify any other VOSS managed fields in `data/InternalNumberInventory`.

4.14. Number cooling

Tip: *Use the Action search to navigate Automate*

4.14.1. 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 & Reserved Number Management** form allows a Provider administrator to manually add numbers to a cooling period (which removes these numbers from the list of available numbers), or to manually remove numbers from a cooling period (which returns these numbers to the list of available numbers).

Related topics

- [Number inventory](#)
- [Number inventory audit](#)
- Number Cooling Auto Expiry Schedule in the Advanced Configuration Guide
- Global Settings in the Core Feature Guide

4.14.2. 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 **Cooling & Reserved Number Management**.
3. At **Select action**, choose **Apply cooling**.
4. Optionally, fill out a cooling duration in days (max = 999) to apply to the selected numbers.

Note: This value overrides the value set in their global settings. If this field is left blank, the cooling duration set in *Global settings* for each number will apply.

5. Configure values in **Filters** to define the numbers to include in the **Available** box in the **Select Numbers** area, these include:
 - **Include available numbers**
 - **Include cooling numbers**
 - **Contains.** Used to further refine the numbers displayed in the **Available** box.
 - **Show numbers at/below hierarchy.** Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
6. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.

Note: The **Available** field displays only unused and available numbers. Used numbers don't display.

7. Click **Save**.

The selected number(s) are placed into a **Cooling** status, and are no longer available for use until they reach either the **Release Date** or until they are manually removed from cooling.

4.14.3. 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 **Cooling & Reserved Number Management**.
3. From the **Select action** drop-down, choose **Remove from cooling**.
4. Configure values at **Filters** to determine which numbers will be included in the **Available** box in the **Select Numbers** area, these include:
 - **Include cooling numbers**
 - **Expires from cooling within (days).**
 - **Contains.** Used to further refine the numbers displayed in the *Available* box.
 - **Show numbers at/below hierarchy.** Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
5. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
6. Click **Save**. The selected number(s) are removed from the cooling period and are available for allocation to a subscriber or phone, etc.

4.15. Number reservation

Tip: *Use the Action search to navigate Automate*

4.15.1. Overview

Number reservation allows numbers to be reserved for future use. Reserved numbers cannot be allocated to a device or line.

The **Cooling & Reserved Number Management** list view allows a Provider administrator to manually reserve numbers at the selected hierarchy (Provider, Customer or Site) for a specified number of days. While a number is within the **Reservation duration (days)** period, it is unavailable and cannot be used by a device or line.

If the **Reservation duration (days)** period is left blank, the numbers remain in the **Reserved** status. Currently reserved numbers can be unreserved manually, thereby *adding them back* to the list of available numbers.

Related topics

- [Number inventory](#)
- [Number inventory audit](#)
- [Number cooling](#)
- Reserve a Number for a User in the Core Feature Guide

4.15.2. Reserve numbers for future use

Note: Numbers can be reserved to make them unavailable to assign to any user until they're unreserved.

A separate feature, *Reserved for*, allows you to reserve numbers for a specific user. When used with *use next available line* during provisioning or onboarding, numbers reserved for a particular user can't be assigned to any other user. See:

Reserve a Number for a User in the Core Feature Guide

1. In the Admin Portal, choose the relevant hierarchy level (Provider, Customer or Site) where you want to reserve numbers.
2. Go to **Cooling & Reserved Number Management**.
3. At the **Select action** drop-down, select **Reserve**.
4. At **Reservation duration (days)**, define the number days to reserve the number/s.
5. Fill out **Reservation Notes** for the reserved numbers to describe why the numbers are being reserved. This is displayed in the **Reservation notes** field on the **Number Inventory** list.

Note: Un-reserving the number (setting *Reserved* status to *Available*) automatically clears the **Reservation notes** field.

6. At **Filters**, define filters to determine which numbers will be included in the **Available** box in the **Select Numbers** area. Options are:
 - Include available numbers
 - Include reserved numbers
 - Contains. Filter criteria to further refine the numbers displayed in the *Available* box.
 - Show numbers at/below hierarchy. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
7. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
8. Click **Save**.

The selected number(s) are placed into a **Reserved** status, and are no longer available for allocation to a subscriber or phone, etc.

Note: Individual numbers can also be reserved directly from the **Number Inventory** list view by clicking on the required number on the list view and then selecting **Reserve Number** on the toolbar.

Related topics

- Reserve a Number for a User in the Core Feature Guide

4.15.3. 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 **Cooling & Reserved Number Management**.
3. From the **Select action** drop-down, choose **Unreserve**.
4. Set **Filters** to determine which numbers will be included in the **Available** box in the **Select Numbers** area. Options are:
 - Include reserved numbers
 - Contains. Additional criteria to further refine the numbers displayed in the *Available* box.
 - Show numbers at/below hierarchy. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
5. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
6. Click **Save**.

The selected number(s) are removed from the **Reserved** status, and are available for allocation to a subscriber or phone, etc.

If reservation notes were included for a number when it was reserved, un-reserving the number automatically clears any notes in the **Reservation notes** field.

4.16. Number inventory alerting

Tip: *Use the Action search to navigate Automate*

4.16.1. Overview

Alerts can be configured to be sent if a specific internal number inventory threshold is reached - for example, if less than ten percent of numbers are available. This alert then allows for proactive management of the inventory.

Optionally, you can enable email so that a summary of the inventory status is emailed each day when the schedule runs.

There are two key hierarchy elements to the setup:

- Hierarchy the alerting is enabled for - since this is managed through Global Settings, it can be enabled at the required hierarchy level(s) based on your needs and it will be enabled for all hierarchy levels below that. For instance, if you wanted this enabled for all sites, you could enable it at say the customer level. All the sites would then be enabled. Alternatively, if you only wanted this enabled for some sites, you can enable the global setting at those sites only.
- It also includes the concept of an aggregation level - this determines how the calculation for available percentage is executed. For instance, if you set aggregation to the customer level, determining if the threshold is exceeded is determined by looking at all the inventories at the customer and below. However, if you set it to site, then the threshold calculation is run for each site and the alert will indicate any site(s) that exceed the threshold.

Therefore, you can determine the best setup based on your specific needs and how you are using the inventory. If you generally use a more a site-based inventory (due to geographical numbers, local breakout, etc) then site aggregation is likely your best option. On the other hand, if your setup is more of a shared number pool environment, then customer level is likely a better aggregation choice.

Use cases would be:

- An administrator wishes to determine if any *sites* within the organization are running low on numbers. Each site has their own dedicated pool of numbers. So the administrator configures alerting at the Customer level with an **Alert Aggregate Level** of "Site" in the **Global Settings**.
- An administrator has a single pool of numbers, shared across locations in the organization. So the administrator configures an **Alert Aggregate Level** of "Customer".

In the event that a Provider would want to monitor any customer that is running low on numbers, they would configure the alert at Provider level and set the **Alert Aggregate Level** to "Customer".

4.16.2. Configure number inventory alerting

1. In the Global Settings, on the Number Inventory Alerting tab, set **Enable Alert on Available Numbers** to **Yes**, and configure also:

- Select a hierarchy level at which the *aggregate* of available numbers should be calculated.
- Select or fill out a percentage available of the total numbers at which point alerts will be raised.
- Enable an Email Group to be notified and select it.

Email content templates can be configured.

See Number Inventory Alerting Email Template Variables section under Email Setup in the Core Feature Guide.

- Ignore hierarchies with no numbers.

2. If required, modify scheduled time for alerts.

When alerts are enabled, a schedule called `InternalNumberInventoryAlert` is created that, by default runs daily at the time `00:00:00` and raises an alert if the availability threshold in the global settings is exceeded. This scheduled time can be modified. See *Create or Update a Schedule* in the Core Feature Guide.

3. View raised alert messages, which display via the **Messages** toolbar icon, or via the **Alerts** page.

See Number Inventory Alerts under Alert Types in the Core Feature Guide.

Related topics

- See the Number Inventory Alerting tab description for Global Settings in the Core Feature Guide.

4.17. Number inventory audit

Tip: [Use the Action search to navigate Automate](#)

4.17.1. Overview

The Number Inventory Audit tool provides the ability to perform an audit of the number inventory to ensure that the *status* and *usage* values of each number aligns to the devices or services configured with these matching numbers.

Numbers that are in a *Cooling* or *Reserved* state are included in the audit:

- If the audit finds that these numbers are unused, they are left in a *Cooling* or *Reserved* state.
- If the audit finds that any of these numbers are used - an admin may have manually updated a user in MS Teams to assign the number - then the number's status is changed to a state that indicates they're in use, to *Used* or *Used-Utility* for example, and they're associated with the correct user.

Note:

- For more information about the values for Status and Usage, see [Number status and usage](#).

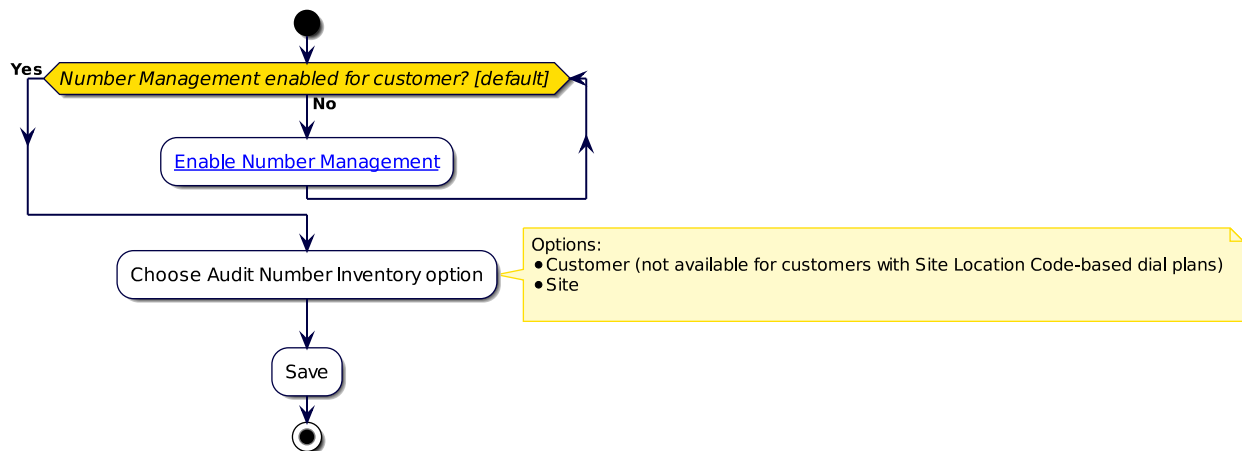
- For vendor-specific audit details, see [UC vendor guidelines for numbers](#).
- You can only run the number inventory audit for customers that have number management enabled. See [Create and Modify a Customer](#).
- You can view the list of internal numbers, and move, delete, and export them as required, on the **Number Inventory** list view.

For Microsoft environments, available numbers are added (else updated if present) to the inventory, with:

- Status: Available
- Vendor: Microsoft
- Number type: Operator Connect or Calling Plan

Note: For details, see: [Microsoft Teams deployments](#)

The audit creates new numbers for devices or services that don't already exist, and updates existing number entries so that the **Status** and **Usage** fields display accurate information at the time the audit is run. Importantly, number entries are *not* deleted.



Related topics

- Prevent duplicate numbers in the Core Feature Guide

4.17.2. Number inventory audit and hierarchies

The table describes the difference between running a number audit inventory at the customer level compared to the site level:

Customer	<ul style="list-style-type: none"> Running the number inventory audit at <i>customer</i> level adds directory numbers at the customer level for services that exist at <i>site</i> or <i>customer</i> level, provided that there is not already a directory number for that service at <i>site</i> level. <p>If there are already directory numbers at the <i>site</i> level, then those numbers are also updated.</p> <p>This is a mixed mode of audit, which audits directory numbers at both <i>customer</i> and <i>site</i> level. For example, if directory numbers only exist at <i>customer</i> level, then the audit only adds and updates directory numbers that exist at the <i>customer</i>.</p> <p>If there are directory numbers at <i>site</i> level, the audit will still add new directory numbers at the <i>customer</i> level, but will also update the existing directory numbers at <i>site</i> level.</p>
Site	<ul style="list-style-type: none"> Running the number inventory audit at <i>site</i> level adds directory numbers at <i>site</i> level, and updates any existing directory numbers at <i>site</i> level only. No <i>customer</i> level directory numbers will be audited and no directory numbers will be added to <i>customer</i> level for <i>customer</i> level services. You can choose to audit either <i>all</i> the <i>sites</i> for the <i>customer</i>, or selected <i>sites</i>

Note: For sites using *Site Location Code-based* dial plans, number inventories can be created only at the *site* hierarchy. The *customer* hierarchy won't be available.

4.17.3. Audit number inventory troubleshooting

The table describes common errors and steps to resolve, when running *audit number inventory*:

Error	Resolution
Duplicate device profiles (same profile name) in different clusters	Ensure that device profiles are not duplicated across the sites.
Duplicate phones (same MAC) in different clusters	Ensure that phones are not duplicated across the clusters.
Same internal number in one or more clusters	Ensure that internal numbers (even in different partitions) are not duplicated across clusters.

Related topics

- Prevent duplicate numbers in the Core Feature Guide

4.17.4. Run a number inventory audit

This procedure runs a number inventory audit.

1. Log in to the Automate Admin Portal as a provider or reseller administrator.
2. Select the relevant *Customer* hierarchy level.

Note: You can only run **Audit Number Inventory** from a customer hierarchy. If you try to run it from a hierarchy that is not of type Customer, you will be prompted to choose a valid customer hierarchy.

3. Go to **Audit Number Inventory**.
4. From the **Is Number Inventory deployed at Customer or Site Level** drop-down, select an option, either of the following:
 - If your number inventory is deployed at customer level, select **Customer**, then click **Save** to run the audit number inventory at all sites at the selected customer.
 - If your number inventory is deployed at site level, choose **Site**, then, at **Would you like to audit all sites or a subset of sites**, select an option:
 - Select **All** to run audit number inventory at all sites at the selected customer.
 - Select **Specific** to choose the sites where you want to audit the number inventory, then select sites, one or more (maximum 200), from **Available** to **Selected** in the transfer box.

Note: The number of sites you have in your environment may exceed the number of sites displayed in the transfer box. You can use a *contains* search to filter the list for the sites you want to include in the number inventory audit.

Click **Save** to run audit number inventory.

5. View transaction progress. The number inventory is updated at the hierarchy you specified, and below.

4.18. E.164 inventory management

4.18.1. Introduction to E164 inventory management

E164 inventory management uses translation patterns in Automate to provide a Direct Dial-In (DDI)/Direct Inward Dialing (DID) mapping to internal numbers.

DDI-to-DN mapping allows you to route incoming PSTN calls to the appropriate internal number.

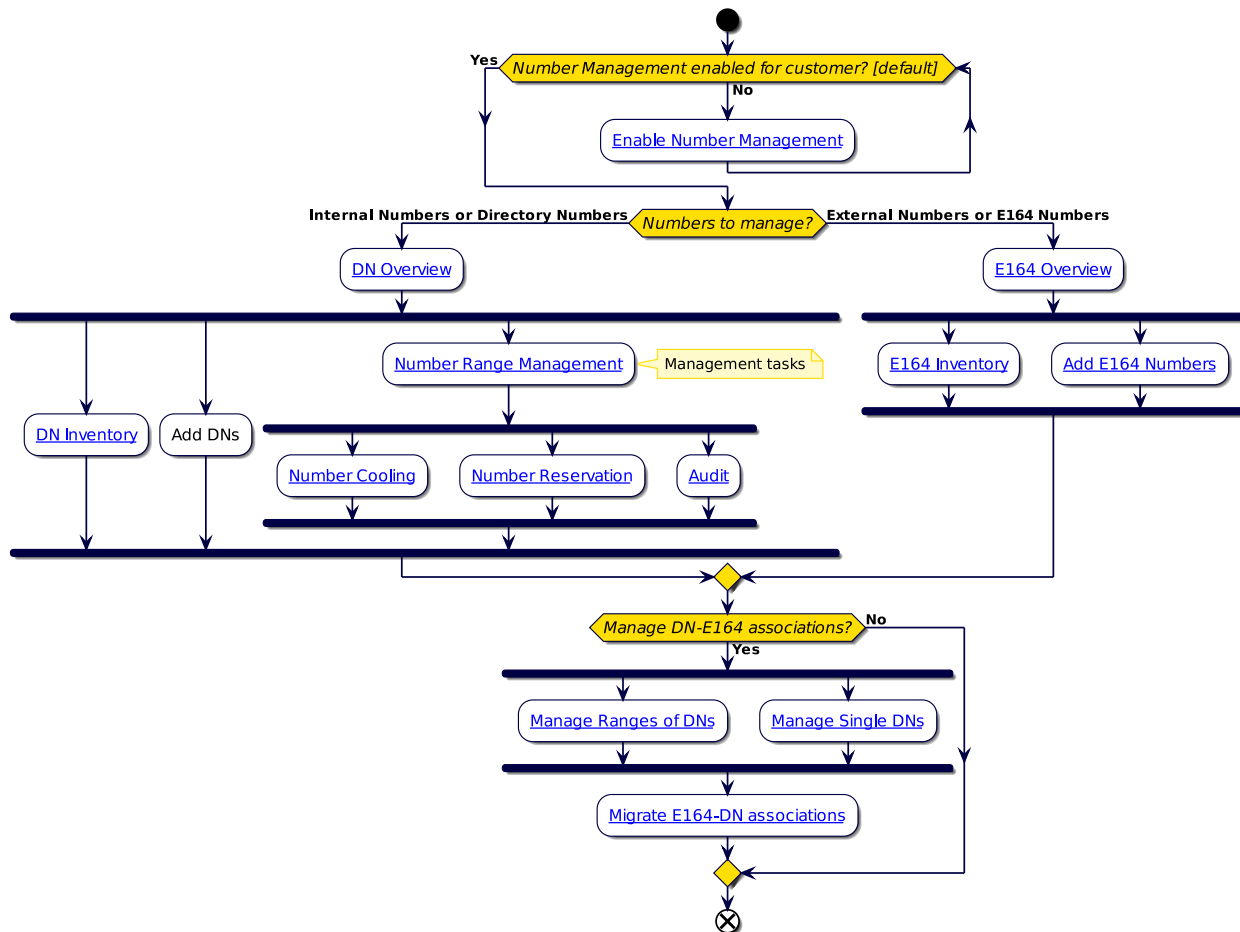
Managing the E164 inventory involves:

- Viewing, adding, or deleting E164 number inventory
- Associating a range of E164 numbers to a range of internal numbers

- Viewing an associated range of E164 numbers to a range of internal numbers
- Disassociating a range of E164 numbers from a range of internal numbers
- Associating a range or set of E164 numbers to a single internal number
- Disassociating a range or set of E164 numbers from a single internal number
- Viewing single internal number associations

The E164 inventory is available in the drop-down menus for Site Published Number and Emergency Number when creating a Site Dial Plan.

- Note: Underlined flowchart titles refer to topic headings in this guide.



4.18.2. Add an inventory of E164 numbers

Tip: Use the Action search to navigate Automate

This procedure defines an inventory of E164 numbers available to users at a customer hierarchy *only*.

Important: Each addition to the E164 inventory must contain a unique set of numbers. That is, you can't assign the same number more than once (globally).

1. Go to **Add E164 Inventory**.
2. Choose the relevant hierarchy.
3. Fill out and select relevant values on the **Add E164 Inventory** page:

Fields	Description
Site	For a site-specific E164 inventory, select the customer site. For a customer-wide E164 inventory, leave this field blank.
Country*	Mandatory. Select the country associated with the E164 inventory. If you chose a site in the previous field, this field is automatically populated with the country associated with the site.
Country Code	Read-only field. The country code for the selected country. Refer to this read-only field when specifying the Starting Number and Ending Number fields, which must contain a valid country code.
Starting Number*	Mandatory. Enter the starting number of the range of E164 numbers. The field is populated with '+' followed by the country code for the selected country. Append the rest of the starting number after the country code.
Ending Number	Optional. Enter the ending number of the range of E164 numbers. The format is the same as the Starting Number . If not provided, the single E164 Number specified in the Starting Number is added. If provided, the range of E164 Numbers is added: Starting Number, Ending Number , inclusive. A maximum of 1000 numbers can be added at a time.
Number Type	Number type, e.g. geo, non geo, etc. Informational only. The field may be hidden.

3. Click **Save**.

4.18.3. View an E164 inventory and delete E164 numbers

Tip: *Use the Action search to navigate Automate*

View E164 number inventory

To view an E164 inventory, go to the **E164 Inventory** page.

This page presents the list of E164 numbers (the inventory) at the customer or site (depending on the hierarchy you're at). At higher levels of the hierarchy, for example, Provider, the **Located At** column shows whether the number is at a customer or site. Click on the link for the customer or site to view the numbers in the inventory at that customer or site.

To view (read-only) details for an E164 number, click on the number in the list.

The list view on the **E164 Inventory** page provides the following information:

Column	Description
E164 Number	The individual E164 number in the inventory.
Country	The country associated with the E164 number.
Associated Flag	Indicates the E164 number has been associated with a Directory Number
Located At	Indicates the hierarchy of the site the E164 number was created for.

Delete E164 numbers from the inventory

This procedure deletes one or more E164 numbers from an E164 inventory.

Note: You can't delete E164 numbers that are associated with an internal number.

1. Log in as provider, reseller, or customer administrator.
2. Go to the **E164 Inventory** list view.
3. Choose an option:
 - Delete one number? Select the number, then click **Delete**.
 - Delete multiple E164 numbers? Select the checkbox adjacent to each number you want to delete, then click **Delete**.

Note: Use column filtering, or click on the **Located At** column to narrow and refine the list of items to select for a batch delete.

4. Click **Yes** to confirm the deletion.

4.18.4. E164 associations (N to N DN)

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes managing a range of internal numbers (Directory Numbers, or DNs) associated with a range of E164 numbers.

View E164 associations (N to N DN)

To view the ranges of E164 numbers that are associated with a range of internal numbers (Directory Numbers, or DNs):

1. In the Admin Portal, go to the **E164 Associations (N to N DN)** list view.
2. View E164 associations (N to N DN) in the list.

Note: You can filter the list and change the hierarchy by selecting a link in the **Located At** column.

The table describes column data in the **E164 Associations (N to N DN)** list view:

Column	Description
E164 Number	The starting E164 number in the range.
DN Number	The starting internal number in the range.
Range	One of the following: <ul style="list-style-type: none"> • 1 - To indicate that one E164 number and internal number are associated. • 10 - To indicate that a range of ten numbers including the starting E164 and starting internal number are associated. • 100 - To indicate that a range of 100 numbers including the starting E164 and starting internal number are associated. • 1000 - To indicate that a range of 1000 numbers including the starting E164 and starting internal number are associated.
Located At	Indicates the hierarchy of the site where the E164 number range and internal number range association was created.

Add an E164 association (N to N DN)

This procedure associates a range of E164 numbers to a range of internal numbers, at a site.

Note:

- You can also perform the association in ranges of 10, 100, and 1000, on a one-to-one basis. These associations create Direct Dial Inward (DDI) associations so that incoming PSTN numbers are routed to internal numbers.
 - Only internal numbers or E164 numbers that are not currently associated, are available for association.
 - In Automate, the HcsSipLocalGwAddE164AssociationEVT event related to SIP Local Gateway is generated
-

1. In the Admin Portal, go to the **E164 Associations (N to N DN)** list view.
2. Set the hierarchy to the relevant customer.
3. In the **E164 Associations (N to N DN)** list view, click the Plus icon (+) to add a new record. Choose a site.
4. Configure E164 Association (N to N DN). The table describes configuration options:

Field	Description
Range	<p>Mandatory. Choose the range before choosing other settings on this page. Defines the range value for the E164 to DN association. Options are: 1, 10, 100, or 1000</p> <p>The range value you select maps to the mask value when the association translation pattern is created. For example, when 10 is selected, all E164 numbers and directory numbers that end in 0 are listed. The mask affects all digits 0 to 9, so you can't start the mask on a non zero number. Likewise, when 100 is selected, the E.164 number and DN end in two zeros. This pattern results in a mask of XX.</p> <ul style="list-style-type: none"> • 1 - To list all E164 numbers and internal numbers • 10 - To list all E164 numbers and internal numbers that end in one zero (0) • 100 - To list all E164 numbers and internal numbers that end in two zeros (00) • 1000 - To list all E164 numbers and internal numbers that end in three zeros (000)
E164 Number	<p>Mandatory. Choose the starting number of the range of E164 numbers.</p> <ul style="list-style-type: none"> • If the association is performed at customer level, the drop-down only shows E164 numbers that were added at customer level. • If the association is performed at site level, the drop-down contains E164 numbers that were added at either customer or site level provided the country matches the site's country.

Field	Description
DN Number	<p>Mandatory. Choose the starting internal number.</p> <ul style="list-style-type: none"> • If the association is performed at customer level, the drop-down only shows internal numbers that were added at customer level. • If the association is performed at site level, the drop-down shows internal numbers that were added at either customer or site level. • You cannot associate internal numbers that begin with the prefix '*' (asterisk) or '#' (hash).
Dial Plan Model Selection	<p>This field displays only when the Enforce HCS Dialplan Rules setting in the Global Settings is set to <i>False</i></p> <p>Defines the translation pattern template configured in the dial plan modeling tool. The values for the pattern, transform mask, and associated range masking are hard coded in the workflow. +1555 111 5555 (Range 10) = +1555 111 555X</p> <p>Other values, such as partition and CSS) come from this template.</p> <p>The translation pattern must have its description set to display in this drop-down.</p>

4. Save your changes.

You can view transaction progress and details in the Transaction Logs.

Note:

- When listing the Number Inventory and displaying an internal number, the E164 Number format is as listed in *E164 numbers in the number inventory*.
 - A translation pattern (which is the mapping between the E164 range and internal number range) is created on the CUCM. This translation pattern is used to route inbound PSTN calls to their associated internal numbers.
 - If the association is performed at a Site, the translation pattern is only added to the CUCM referenced by the site's network device list (NDL).
 - If the association is performed at Customer level, the translation pattern is added to all the customer's CUCMs.
 - If the Site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwAddE164AssociationEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.
-

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Delete an E164 association (N to N DN)

This procedure deletes one or more E164 (N to N DN) associations to disassociate a range of E164 numbers from a range of internal numbers.

Note: In Automate, the HcsSipLocalGwDelE164AssociationEVT event related to SIP Local Gateway is generated as a result.

1. Go to the **E164 Associations (N to N DN)** list view.
2. Change your hierarchy, if required.
3. View E164 Associations (N to N DN) in the list, which displays the following information:

Column	Description
E164 Number	The starting E164 number in the range.
DN Number	The starting DN number in the range.
Range	<ul style="list-style-type: none"> • 1 - Indicates that one E164 number and internal number are associated • 10 - Indicates that a range of ten numbers including the starting E164 and starting internal number are associated • 100 - Indicates that a range of 100 numbers including the starting E164 and starting internal number are associated • 1000 - Indicates that a range of 1000 numbers including the starting E164 and starting internal numbers are associated
Located At	Indicates the hierarchy of the site where the E164 number range and internal number range association was created.

4. Choose an option:

- To disassociate multiple ranges, select the check boxes in the far left column of the table for the ranges you want to disassociate.
- To disassociate one range, click its row in the table. The details about the association appear.

5. Click **Delete**, then click **Yes** to confirm the disassociation.

Note:

- The translation pattern mapping between the E164 range and internal number range is deleted from CUCM.

The E164 number association with the internal number is removed on the Number Inventory list view display and in any **Lines** drop-down list and **Lines** displays.

- If the site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwDelE164AssociationEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

4.18.5. E164 associations (N to 1 DN)

Tip: *Use the Action search to navigate Automate*

Overview

This topic describes managing single internal numbers associated with a range of E164 numbers.

View E164 associations (N to 1 DN)

This procedure displays sets of E164 numbers associated with a single internal number (directory number, or DN).

1. Go to the **E164 Associations (N to 1 DN)** list view.
2. On the **E164 Associations (N to 1 DN)** list, view E164 associations (N to 1 DN).

Note: You can filter the list and change the hierarchy by selecting a link in the **Located At** column.

The table describes column data in the E164 Associations (N to 1 DN) list view:

Column	Description
DN Number	The associated internal number (directory number).
Located At	The hierarchy of the site where the E164 number range and internal number association was created.

3. Click on a directory number in the list to view its details.

The page displays read-only details about the E164 Association (N to 1 DN) configuration (the sets of E164 numbers that are associated with the internal number):

DN Number	The number you're viewing.
Primary E164	Displays the E164 number associated to the internal number in the Number Inventory. Other E164s are indicated as [x] showing that there are more associated E164s to this internal number but their details are only available when opening the relevant Number Inventory.

Add E164 association (N to 1 DN)

This procedure associates multiple E164 numbers (a set of E164 number) to a single internal number, at a site. For example, you could associate a set of E164 numbers for the sales department with an attendant's internal number.

Note:

- You can also perform association in ranges of 10, 100, and 1000, on a one-to-one basis. These associations create Direct Dial Inward (DDI) associations so that incoming PSTN numbers are routed to internal numbers.
 - You can optionally specify a primary E164 number to associate with the internal number. This is useful when performing an internal number to E164 translation (for example, when provisioning translation rules for LBO gateways) and the internal number is associated to more than one E164 presentation.
 - You can only associate internal numbers or E164 numbers that are not currently associated.
 - You can also *modify* a **E164 Associations (N to 1 DN)** association instance and add additional ranges of E164 numbers to a DN. Open the existing, saved association and then add the additional ranges using the plus icon (+) - as described in the steps below.
-

Prerequisites:

- Enable number management for the customer.

Perform these steps:

1. Go to the **E164 Associations (N to 1 DN)** list view.
2. Choose the site (if required).
3. In the **E164 Associations (N to 1 DN)** list view, click the Plus icon (+) to add a new record.
4. Configure E164 association (N to 1 DN). The table describes configuration options:

Field	Description
DN Number	<p>Choose an internal number.</p> <ul style="list-style-type: none"> If the association is performed at Customer level, the drop-down only shows internal numbers that were added at Customer level. If the association is performed at Site level, the drop-down shows internal numbers added at either Customer or Site. You can't associate internal numbers that begin with the prefix '*' (asterisk) or '#' (hash).
E164 Ranges	<p>Click the Plus icon (+) to add one or more sets of E164 numbers. These E164 numbers do not need to be contiguous. For each E164 number you add, choose an E164 range and the E164 number, as follows:</p> <ul style="list-style-type: none"> E164 Range <p>Choose an E164 range, either 1, 10, 100, or 1000.</p> <p>The range value you choose maps to the mask value when the association translation pattern is created. For example, choose 10 to list all E164 numbers and internal numbers ending in 0. The mask affects all digits 0 to 9, so you can't start the mask on a non-zero number. When 100 is chosen the E164 number and internal number end in two zeros, resulting in a pattern with a mask of XX.</p> <ul style="list-style-type: none"> 1 - to list all E164 numbers 10 - to list all E164 numbers ending in one zero (0) 100 - to list all E164 numbers ending in two zeros (00) 1000 - to list all E164 numbers that end in three zeros (000) <p>This field is mandatory and affects what appears in the E164 Number field.</p>
E164 Number	<p>Mandatory. Choose the starting number of E164 numbers.</p> <ul style="list-style-type: none"> If the association is performed at customer level, the drop-down only shows E164 numbers that were added at customer level. If the association is performed at site level, the drop-down contains E164 numbers that were added at either customer or site level provided the country matches the site's country.
Primary E164	<p>Optional. Fill out the primary E164 number to associate with the internal number. Ensure the E164 number you enter starts with \+ and falls within the range you specified in in E164 Range</p>
Dial Plan Model Selection	<p>This field displays only when the Enforce HCS Dialplan Rules setting in the Global Settings is set to <i>False</i></p> <p>Defines the translation pattern template configured in the dial plan modeling tool. The values for the pattern, transform mask, and associated range masking are hard coded in the workflow. +1555 111 5555 (Range 10) = +1555 111 555X</p> <p>Other values, such as partition and CSS) come from this template.</p> <p>The translation pattern must have its description set to display in this drop-down.</p>

5. Save your changes.

View transaction progress and details in the Transaction Logs.

Note:

- When listing the number inventory and displaying an internal number, the E164 number format is as listed in *E164 numbers in the number inventory*.
- One or more translation patterns are created on the CUCM. The translation patterns are the mappings between the set of E164 numbers and the single internal number, and are used to route inbound PSTN calls to their proper internal numbers.

When you associate a set of E164 numbers to a single internal number, multiple translation patterns are created (each DN-to-E164 range association results in a translation pattern being created on the CUCM).

- If the association is performed at Site level, the translation pattern is only added to the CUCM referenced by the site's network device list (NDL).
- If the association is performed at Customer level, the translation pattern is added to all of the CUCMs that exist for the customer.
- If the site is associated with one or more SIP Local Gateways, the HcsSipLocalGwAddMultiE164AssociationEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

Delete an E164 associations (N to 1 DN)

This procedure disassociates a set of E164 numbers from an internal number.

Note:

- When disassociating a set of E164 numbers from an internal number, multiple translation patterns are deleted. For each association you delete, a translation pattern is deleted from the CUCM.
In Automate, the HcsSipLocalGwDelMultiE164AssociationEVT event related to SIP Local Gateway is generated as a result.
- If the Local Gateway is set up to override the Voice Translation limit and the **Enable Command Builder** setting is enabled, disassociation will fail if it exceeds the default Voice Translation limit. In this case, first disable the **Enable Command Builder** setting.

1. Go to the **E164 Associations (N to 1 DN)** list view.
2. Change the hierarchy, if required.
3. In the **E164 Associations (N to 1 DN)** list, view the following details:

Column	Description
DN Number	The internal number.
Located At	The hierarchy of the site where the E164 number range and internal number range association was created.

4. Choose an option:

- To disassociate multiple associations, click the check box in the far left column of the table, next to the numbers you want to disassociate.
- To disassociate one association, click its row in the table. The details about the association appear.

5. Click **Delete**, then click **Yes** to confirm the disassociation.

Note:

- The translation pattern mapping between the E164 set and the internal number is deleted from the CUCM.

The E164 number association with the internal number is removed from the **Number Inventory** list view, and from any **Lines** drop-downs and **Lines** displays.

- If the site is associated with one or more SIP Local Gateways, the HcsSipLocalGwDelMultiE164AssociationEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.
-

Related Topics

- Transaction Logging and Audit in the Core Feature Guide

4.18.6. Migrate translation patterns for E164 to internal number associations

This procedure migrates existing translation patterns for E164 to internal number associations, if you manually configured translation patterns in the E164 lookup partition to associate E164 numbers to internal numbers for Direct Dial Inward (DDI) routing.

Note: It is recommended that you migrate your existing translation patterns to use E164-to-Internal number (DN) association.

Perform this procedure only once. If you did this migrate when upgrading to VOSS Automate, there is no need to migrate again when upgrading to a later VOSS Automate release.

To migrate translation patterns:

1. Log in as provider, reseller, or customer administrator.
2. Add the appropriate E164 number inventory. See [Add an inventory of E164 numbers](#).
3. View the E164 number inventory. See [View an E164 inventory and delete E164 numbers](#).
4. To verify that the selected directory number (DN) inventory is available for association, go to the **Number Inventory**.
5. Remove the translation patterns you added previously, via the **Translation Patterns** page.
6. Create the appropriate E164-to-DN associations, via the **E164 Associations (N to N DN)** page. See [E164 associations \(N to N DN\)](#). These associations restore the appropriate translation patterns in the E164 Lookup partition for the selected customer.
7. View the new translation pattern, via the **Translation Patterns** page.

Related Topics

- CUCM Translation Patterns in the Core Feature Guide.

4.19. Inter-site cross-cluster support

4.19.1. Configure inter-site cross-cluster support

This procedure configures the environment to provide support for inter-site calls for customers that have sites spanning multiple clusters.

1. Create a full-mesh network between clusters for customers.

Create trunk, route group, and route list with Automate for a given cluster to every other cluster owned by the customer.

For a shared Cisco UCM, a SIP security profile is needed for each trunk.

See *Configure SIP Trunks*, *Configure Route Groups*, *Configure Route Lists*.

2. For each site added to a cluster, add a route pattern to all the other clusters in the mesh network owned by the customer.

The route pattern is added to the InterSiteRouting partition, the partition name in UCM is Cu<CustomerID>-ISR-PT, where <CustomerID> is the customer ID.

- The pattern in the route pattern depends on the internal dial plan type:
 - Type 1 and type 3 are the site location code (SLC) plus the extension mask of the site.
 - Type 2 is the ISP plus the SLC plus the extension mask of the site.
 - Type 4 is the DN range of the site.
- The route list in the route pattern is the route list associated to the site cluster.

4.20. Local breakout support

4.20.1. Manually configure local breakout support

This procedure manually configures a local gateway for a site to support local breakout (LBO).

1. Ensure that the Automate hierarchy is set to the site where the local gateway is to be added.
2. In Automate, to create trunks, route groups, and route lists to the local gateway. For procedures, see *Configure SIP Trunks*, *Configure Route Groups*, and *Configure Route Lists*.
3. In Cisco Unified Communications Manager (UCM), create a partition Cu<CustomerID>Si<SiteID>-LBO-LBR-PT to be used in the class of service. Refer to *Configure Class of Service*.
4. In UCM, create a partition and CSS to handle LBO routing for the site.
5. Add the following translation patterns to the partition defined in step 3:

- a. Add the ++061.0! translation pattern to handle calls without forced authorization code (FAC) and client matter codes (CMC).
 - b. Add the ++061.1! translation pattern to handle calls with FAC and without CMC.
 - c. Add the ++061.2! translation pattern to handle calls with CMC and without FAC.
 - d. Add the ++061.3! translation pattern to handle calls with CMC and FAC.
6. Associate the patterns in step 5 with the CSS defined in step 4.
 7. For the patterns in step 5, ensure that the called number transformation is PreDot and add the **** prefix.
 8. Create a default translation pattern in the routing partition defined in step 4 with an ***X!* pattern. Set the CSS to Cu<CustomerID>-<CC>DP-LBRRteSel-CSS. This is used to switch the call processing back to central breakout (CBO) for all call types that are not sent using LBO.
 9. Create a route pattern for each call type that breaks out from the local gateway in step 4. Use the route list created in step 3.

Note: The called and calling number between the local gateway and UCM is in +E.164 format. Therefore, all incoming and outgoing calls between the gateway and UCM conform to it. It is also assumed that you provide the IOS gateway configuration.

10. Create a new CoS to be included in step 3 before LBRtg-PT.

4.21. Voice mail

4.21.1. Voice mail services

Tip: *Use the Action search to navigate Automate*

Add voice mail service

This procedure adds a voice mail service, associates the service with a Cisco Unity Connection (CUC) server, and integrates it with a Cisco Unified Communications Manager (UCM) and/or Cisco Webex DI (Dedicated Instance).

Prerequisites

- To associate the voice mail service with a UCM, ensure you know the SIP trunking endpoint information between the voice mail server and the UCM.
- A CUC server must be configured.

Perform these steps:

1. Log in as provider or reseller administrator.
2. Set the hierarchy to the correct provider or reseller node.

Note: The voice mail service is always added above the customer level, so either at provider level or reseller level, and is associated to the customer.

3. Go to **Voice Mail Service**.
4. Click the Plus icon (+) to add a voice mail service.
5. On the **New Record** page, fill out details for the new voice mail service:

Field	Description
Voice Mail Service Name	The voice mail service name. Ensure there are no spaces in the name.
Cisco Unity Connection Cluster	<p>Mandatory. The name of the CUC server for the voice mail service.</p> <hr/> <p>Note:</p> <ul style="list-style-type: none"> • The CUC server must have been added at the Provider level. • This is also where the voice mail server in a multi-tenant environment is categorized as <i>Dedicated</i> or <i>Partitioned</i>, which defines the elements available to the voice mail server, for example, whether another tenant should be created on the voice mail server. <hr/>
Integrate with Cisco Unified CM	<p>Defines whether to integrate the voice mail service with UCM (UCM will manage the voice mail service). The default is False (unchecked).</p> <p>When choosing Integrate with Cisco Unified CM, the Cisco Unified CM Cluster drop-down displays.</p>
Cisco Unified CM Cluster	<p>The UCM cluster associated with the voice mail service. This drop-down displays only if you've selected Integrate with Cisco Unified CM.</p> <p>From this drop-down, select the UCM to be paired with the CUC server.</p> <hr/> <p>Note: The UCM must have been added and configured at the Provider level (via the CUCM page).</p> <hr/>
Integrate with Cisco Unified CM Webex DI	<p>Defines whether to integrate a voice mail Webex Dedicated Instance with UCM.</p> <p>When choosing Integrate with Cisco Unified CM Webex DI, the rest of the fields on this form are hidden, and the Voice Mail Trunk Address drop-down displays.</p> <p>In a UCM Webex DI environment, the routing rules in the Automate provisioning workflow uses the calling search space (CSS) for Webex DI to allow for adding multiple voice mail services for Webex DI.</p>

Field	Description
Voice Mail Trunk Address	<p>This drop-down displays only if you've selected the Integrate with Cisco Unified CM Webex DI checkbox.</p> <p>The drop-down displays available existing entries on the selected UCM cluster, which will be associated with the Route Group as a part of the Route List and Route Group provisioning.</p>
Cisco Unity Connection Server Address	<p>The hostname or IP address of the voice mail server.</p> <p>This field is hidden on the form if you've selected Integrate with Cisco Unified CM Webex DI.</p> <p>This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).</p>
Cisco Unity Connection Server Port	<p>The voice mail server port number (1 to 65535).</p> <hr/> <p>Note: Do not use port 5061, which is reserved for secure SIP.</p> <hr/> <p>This field is hidden on the form if you've selected Integrate with Cisco Unified CM Webex DI.</p> <p>This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).</p>
Cisco Unified CM Server Address	<p>The hostname or IP address for the voice mail server to reach the UCM.</p> <p>This field is hidden on the form if you've selected Integrate with Cisco Unified CM Webex DI.</p> <p>This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).</p>
Cisco Unified CM Server Port	<p>The UCM port number.</p> <hr/> <p>Note:</p> <ul style="list-style-type: none"> • Do not use port 5061, which is reserved for secure SIP. • Only one UCM and one CUC can be specified here. To support redundancy and failover in a multinode configuration, the trunk information must be manually updated on the UC apps. <hr/> <p>This field is hidden on the form if you've selected Integrate with Cisco Unified CM Webex DI.</p> <p>This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).</p>

Field	Description
Voice Messaging Ports	<p>Mandatory. Fill out the number of voice messaging ports to be created for the voice mail service and associated with the appropriate Port Group on CUC when the voice mail service is associated to a customer. Valid values are 1 - 250. The default = 3.</p> <hr/> <p>Note: The number of voice messaging ports you add can't bring the total number of voice messaging ports for all port groups to more than the maximum number of voice messaging ports that are enabled by the CUC license files. If the license files don't enable the total number of ports, you won't be able to add the new ports.</p> <hr/> <p>This field is hidden on the form if you've selected Integrate with Cisco Unified CM Webex DI. This field value is part of the SIP trunk provisioning information (between the SIP trunk and the CUC server).</p>

6. Save your changes to add the new voice mail service.

Once a shared voice mail service is created, if you have enabled **Integrate with Cisco Unified CM**:

- In UCM, cluster-level SIP trunk and route group is provisioned for the shared voice mail service.
- In CUC, cluster-level port group appears on the PhoneSystem for the shared voice mail service.

Next steps

- *Associate or disassociate voice mail services to a customer*

Delete voice mail service

1. Log in to the Automate Admin Portal as Provider administrator.
2. Go to **Voice Mail Service**.
3. From the list of voice mail services, select the checkbox for the voice mail service you want to remove.
4. Click **Delete**, then click **Yes** to confirm.

Once the transaction completes, the voice mail service is removed from the list.

4.21.2. Associate or disassociate voice mail services to a customer

Tip: *Use the Action search to navigate Automate*

Associate voice mail services to customer

Prerequisites

- Create the voice mail service. See [Voice mail services](#).
- If you've selected the **Integrate with Cisco Unified CM** checkbox when creating the voice mail service, create a customer dial plan and a site dial plan before attempting to associate the voice mail service with the customer, else, the association will fail.

Note: If you've selected the **Integrate with Cisco Unified CM Webex DI** checkbox when creating the voice mail service, the selected **Cisco Unified CM Cluster** provides the **Voice Mail Trunk Address** selection.

Perform these steps:

1. Log in as provider or reseller administrator.
2. Set the hierarchy path to the customer where you want to associate the voice mail service.
3. Go to the **Associate Voice Mail Service to Customer** page.
4. Click **Add** to associate voice mail service to the customer.
5. From the **Voice Mail Service** drop-down, choose the name of the voice mail service that has been defined by the provider and available to this customer.
6. Click **Save**. The voice mail service is now associated with this customer and appears in the list.
 - When the voice mail service is associated with a customer and the **Integrate with Cisco Unified CM** checkbox was selected for the voice mail service, the following is provisioned based on the deployment mode of the voice mail server:

Voice Mail Deployment Mode	Cisco Unified Communications Manager	Cisco Unity Connection
Dedicated	Creates integration at customer level: SipTrunk, Route Group, AllowVm route partition	Creates customer-specific Port Group, ports (3), route partition, calling search space and user template
Partitioned	Creates integration at customer level: SipTrunk, Route Group, AllowVm route partition	Creates new tenant (partition), port group, ports (3), route partition, calling search space and user template

Note: The deployment mode for the voice mail service is determined by the mode selected when the Cisco Unity Connection is first added to Automate via the **CUC** page.

- When the **Integrate with Cisco Unified CM Webex DI** checkbox was selected for the voice mail service, the **Voice Mail Trunk Address** selected from the selected **Cisco Unified CM Cluster** - is associated with the route group as a part of the route list and route group provisioning.

Disassociate voice mail services from customers

1. Log in as the Provider Administrator.
2. Set the hierarchy path to the customer from which you want to disassociate the Voice Mail Service.
3. Go to **Associate Voice Mail Service to Customer**.
4. From the list of associations, choose the Voice Mail Service customer association to be disassociated, by clicking the check box in the leftmost column.
5. Click **Delete** to disassociate the Voice Mail Service from the customer.
6. From the popup window, click **Yes** to confirm the change. When the delete action is complete, the Voice Mail Service association to the customer disappears from the list.

4.21.3. Pilot numbers

Tip: *Use the Action search to navigate Automate*

Add a pilot number

This procedure creates one or more voicemail pilot numbers for voicemail services that have previously been associated with the customer.

Prerequisites:

- Create the voicemail service.
- Associate voicemail service with the customer.

Note: In Automate, you can select the voice mail pilot number from a list of available DN inventory.

Perform these steps:

1. Log in as provider or customer administrator.
2. Set the hierarchy to the customer or site that you are defining a Voice Mail Pilot Number for.
3. Go to the CUC **Pilot Numbers** page.
4. Click **Add** to associate a pilot number with the voice mail service that has been associated with the customer.
5. From the **Voice Mail Service** drop-down, select the appropriate Voice Mail Service from the list of Voice Mail Services associated with the customer.
6. From the **Voice Mail Pilot Number** drop-down, select a Pilot Number from the list of your available DN inventory, or type the Pilot Number you want to use in the field. This is the internal Voice Mail Pilot Number that can be dialed from site.

Note: You can add one or more pilot numbers for a single voice mail service.

- Click **Save** to create the pilot number.

The Pilot Number appears in the list. When a Pilot Number is created for a Voice Mail Service and the **Integrated with CUCM** checkbox was selected for the Voice Mail Service, the following is provisioned based on the deployment mode of the Voice Mail server:

Voice Mail Deployment Mode	Cisco Unified Communications Manager
Dedicated	At customer level: Route List, Route Pattern, CSS, Voice Mail Pilot, Voice Mail Profile
Partitioned	At customer level: Route List, Route Pattern, CSS, Voice Mail Pilot, Voice Mail Profile

Delete a voicemail pilot number

- Log in as the Customer Administrator. For a list of the roles and tasks that can be done at each level, see [Dial plan roles and privileges](#).
- Go to the CUC **Pilot Numbers** page.
- From the **Pilot Numbers** list view, select the number to be deleted.
- Click **Delete** to delete the Voice Mail Pilot Number.
- From the popup window, click **Yes** to confirm the deletion.

When the delete action is complete, the Voice Mail Pilot Number disappears from the list.

4.21.4. Creating DDIs for voice mail pilot numbers

Tip: [Use the Action search to navigate Automate](#)

This procedure creates a DDI for a voice mail pilot number.

Prerequisites:

- Create the voice mail pilot number. Refer to [Define a voice mail pilot number](#).

Perform these steps:

- Log in to Automate as a Provider, Reseller, or Customer administrator.
- Set the hierarchy to the customer node containing the voice mail pilot number.
- Go to **Route Patterns**.
- Select **Add**.
- Create a new route pattern instance with the following information:
 - On the **Pattern Definition** tab, complete the following item:
 - CUCM:** Select the appropriate Cisco Unified Communications Manager cluster for this route pattern. This should be the cluster on which you created the voice mail pilot.
 - Route Pattern:** +<E.164 number>: Enter an appropriate DDI number.

- iii. **Route Partition:** Cu<customerId>-E164LookUp-PT
 - iv. **Route List:** From the drop-down, choose the appropriate route list for the target voice mail pilot number. The pilot number will be in the route list name. Example:
 Cu<customerId>-<voicemail service name><targetVM pilot number>-RL, Cu5-TestVmService1000-RL
 - b. On the **Called Party Transforms** tab, enter a pilot number in the Called Party Transform Mask field; for example, 1000.
6. Select **Save**.
 7. Repeat these steps for each voice mail pilot number.

Note: This route pattern needs to be deleted from the **Route Patterns** page before the voice mail pilot can be deleted. This is because this new route pattern will still reference the pilot-specific route list, causing the voice mail pilot number delete workflow to fail. If this occurs, delete the route pattern and attempt to delete the voice mail pilot again.

4.21.5. Associate or disassociate pilot number and site

Tip: *Use the Action search to navigate Automate*

Associate pilot number to site

This procedure associates an existing voicemail pilot number to a site.

Prerequisites

- Add the voicemail pilot number. See [Pilot numbers](#)

Note: In Automate, the event related to SIP Local Gateway may be generated as a result. Also you can select an E164 number to associate with the Pilot Number.

Perform these steps:

1. Log in as a Customer or Provider administrator.
2. Set the hierarchy to the relevant site.
3. Go to **Associate Pilot Number to Site**.
4. Click the Plus icon (+) to add the pilot number to site association.
5. At **Voice Mail Service** (mandatory), choose the voicemail service to associate with the site.
6. At **Voice Mail Service Pilot Number** (mandatory), choose the pilot number for the voicemail service you selected.
7. At **E164 Number** (optional), choose a E164 number from your site's inventory to associate with the pilot number, or type the E164 number you want to use.

Note: You must choose (or specify) an available E164 number. The transaction will fail if you choose an E164 number that is already assigned.

8. Click **Save**.

The voicemail service pilot number is associated with the site:

- The association appears in the list. When a pilot number is associated to a site, **CUC Defaults** are updated so that the user management templates can take advantage of this new voicemail service for the site.
- If the site has one or more SIP Local Gateways associated with it and an E164 number has been specified, the HcsSipLocalGwAddVoiceMailPilotNumberEVT is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

Disassociate pilot number from a site

Note: In Automate, the event related to SIP Local Gateway is generated as a result.

Perform these steps:

1. Log in as the Customer administrator. For a list of the roles and tasks that can be done at each level, see [Dial plan roles and privileges](#).
2. Go to **Associate Pilot Number to Site**.
3. From the list of associations, select the pilot number association to be disassociated.
4. Click **Delete** to disassociate the Pilot Number from the site.
5. From the popup window, click **Yes** to confirm the change.
 - When the delete action is complete, the Pilot Number association to the site disappears from the list.
 - If the site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwDelVoiceMailPilotNumberEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

4.22. Adding aggregation trunk and route group and associating to existing route list and SLRG

4.22.1. Add aggregation trunk and route group and associate to existing route list and SLRG

Tip: [Use the Action search to navigate Automate](#)

In Automate, the dial plan creates a route list to route the calls to the aggregation for central breakout (CBO). However, the following procedure is required to enable calls to egress to the PSTN network using a SIP trunk. Before adding a SIP trunk using Configure SIP Trunks, you must provision the following:

1. In Automate, create a region for the trunk:
 - a. Sign in as a Provider or Reseller admin, then go to **Region**.
 - b. Click **Add**.
 - c. Provide a name in the format Cu<cid>-Trunk-<TrunkName>-Region.
2. In Cisco UCM, navigate to **CUCM System > Device Pool** and provision a device pool as follows:
 - a. Click **Add**.
 - b. Enter a device pool a name in the format Name Cu<cid>-DP-Trunk.
 - c. Choose a CCM group from the dropdown or leave at the default group.
 - d. Ensure that the region is set to the name created in step 1.
 - e. Set the location to **Hub Non**.
3. To create an aggregation SIP trunk, sign in as a provider in Automate and perform the following:
 - a. Go to **SIP Trunks**.
 - b. Click **Add**.
4. In the **Device Information** tab, perform the following:
 - a. Choose the CUCM from the drop-down list.
 - b. Provide a device name; for example, Cu<cid>-Trunk-<TrunkName>.
 - c. Set the device pool to the device pool name you created.
 - d. Set the region to the name created in step 1.
 - e. Set call classification to OffNet.
 - f. Click **Redirecting Diversion Header Delivery - Inbound**.
 - g. Click **Run On All Active Unified CM nodes**.
5. In the **Call Routing Inbound** tab, perform the following:
 - a. Choose the calling search space by selecting Cu<cid>-IngressFromCBO-CSS from the drop-down list.
 - b. Choose the connected party transformation CSS by selecting Cu<cid>-CNPNTtransform-CSS from the drop-down list.
 - c. Uncheck the **Use Device Pool Connected Party Transformation CSS** box.
 - d. Check the **Redirecting Diversion Header Delivery - Outbound** box.
6. In the **Call Routing Outbound** tab, perform the following:
 - a. Choose the called party transformation CSS by selecting Cu<cid>-CDPNTtransform-CSS from the drop-down list.
 - b. Uncheck the **Use Device Pool Called Party Transformation CSS** box.
 - c. Choose the calling party transformation CSS by selecting Cu<cid>-CGPNTtransform-CSS from the drop-down list.
 - d. Uncheck the **Use Device Pool Calling Party Transformation CSS** box.

7. In the **SIP Info** tab, provide the destination IP address. It is assumed that the default SIP profile and SIP trunk security profile are used.
8. Once the aggregation SIP trunk is created, assign it to a route group as follows:
 - a. Go to **Route Groups**.
 - b. Click **Add**.
 - c. Provide a name for the route group in the format Cu<cid>-RouteGroup-<Name>.
 - d. Set the distribution algorithm to Top Down.
 - e. Add the above trunk as a member of the route group.

Note: For line-based routing (LBR), perform steps 9 and 10.

9. Associate the above route group to the route lists. The assumption is that there is one trunk or route group to the aggregation that is shared by the whole country. However, if there is a trunk per country, then repeat the above step to create trunk and route groups for each country. The country dial plan automatically creates the following LBR route lists for each country for each customer:
 - Cu<cid>-<ISO>Intl-RL . (cid is the customer ID number and <ISO> is the 3-letter alpha code for the countries of the world. For more information on ISO, refer to http://en.wikipedia.org/wiki/ISO_3166-1).
 - Cu<cid>-<ISO>Natl-PL
 - Cu<cid>-<SIO>Mobl-PL
 - Cu<cid>-<ISO>Emer-RL
 - Cu<cid>-<ISO>Serv-RL
 - Cu<cid>-<ISO>Local-RL
 - Cu<cid>-<ISO>PRSN-RL
 - Cu<cid>-<ISO>FPHN-RL
 - Cu<cid>-<ISO>PCSN-RL
 - Cu<cid>-<ISO>SRSN-RL
 - Cu<Cid>-<ISO>Oper-RL

Note: The SLRG-Emer local route group must be provisioned even for line-based routing (see step 11).

10. Update each of the route lists to include the above-created route group as follows:
 - a. Go to **Route Lists**.
 - b. Select and enter each of the route list pages from the step above.
 - c. Click on the **Add Route Group Items** and select the above route group.
 - d. Save and proceed to the next route list until all the route lists include the route group.
11. For device-based routing (DBR), nothing is needed for DBR route lists because they already contain the correct *well-known* local route groups. For each location that uses DBR, update the device pool as follows:

- a. Go **Device Pools**.
- b. Select and enter the device pool SLRG page.
- c. Add the following *well-known* SLGs and associate them to the route group created above.
 - SLRG-Emer

Note: SLRG-Emer must be added regardless of whether DBR is used. Emergency call handling depends on this in order to work.

- SLRG-Intl
- SLRG-Mobl
- SLRG-Serv
- SLRG-Local
- SLRG-PRSN
- SLRG-FPHN
- SLRG-PCSN
- SLRG-SRSN
- SLRG-Oper

4.23. Configure SIP profiles

4.23.1. SIP profiles

provider

Tip: *Use the Action search to navigate Automate*

Add or manage SIP profiles

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (CUCM, or CallManager) is configured.
3. Go to **SIP Profiles**.
4. **Choose an option:**
 - **Add a new SIP profile?** Click the Plus icon (+) to add a new record, then go to Step 5.
 - **Edit an existing SIP profile?** Choose the SIP profile to be updated by clicking it in the list of SIP profiles. Go to Step 6.

5. If the **Network Device List** dialog displays, select the NDL for the SIP profile from the drop-down menu.

This dialog displays when you're on a non-site hierarchy node. If you're at a site hierarchy node, the NDL associated with the site is automatically used.

Note: The **Network Device List** drop-down menu displays only when adding a SIP profile. It does not display when editing a SIP profile.

6. Fill out a unique name for the new SIP profile, or modify the existing name, if required.
7. Configure at least the mandatory settings on the following tabs/panels of this page:
 - *SIP Profile Information settings.*
 - *SDP Information settings.*
 - *Parameters used in Phone settings.*
 - *Normalization Script settings.*
 - *Incoming Requests FROM URI Strings settings.*
 - *Trunk Specific Configuration settings.*
 - *Trunk SIP OPTIONS Ping settings.*
 - *Trunk SDP Information settings.*
8. Click **Save** to save a new SIP profile or to update an existing SIP profile.

SIP Profile Information settings

Option	Description
Name (Mandatory)	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description (Optional)	This field identifies the purpose of the SIP profile; for example, SIP for 8865. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Default MTP Telephony Event Payload Type (Optional)	<p>This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. Usually, the default value specifies the appropriate payload type. Be sure that you have a good understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated.</p> <p>Default-101 Range-96 to 127</p> <p>This parameter's value affects calls with the following conditions:</p> <ul style="list-style-type: none"> • An outgoing SIP call from Cisco Unified Communications Manager • For the calling SIP trunk, the Media Termination Point Required check box is checked on the SIP Trunk Configuration window
Early Offer for G.Clear Calls (Optional)	<p>This feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP).</p> <p>To enable or disable Early Offer for G.Clear Calls, choose one of the following options:</p> <ul style="list-style-type: none"> • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD

Option	Description
User-Agent and Server header information (Mandatory)	<p>This feature indicates how Unified CM handles the User-Agent and Server header information in a SIP message. Choose one of the following options:</p> <ul style="list-style-type: none"> • Send Unified CM Version Information as User-Agent Header - For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified CM passes any contact headers through untouched. • Pass Through Received Information as Contact Header Parameters - If selected, the User-Agent and Server header information is passed as Contact header parameters. The User-Agent and Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent and Server headers. • Pass Through Received Information as User-Agent and Server Header - If selected, the User-Agent and Server header information is passed as User-Agent and Server headers. The User-Agent and Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent and Server headers. <p>Default: Send Unified CM Version Information as User-Agent Header</p>
Version in User Agent and Server Header (Mandatory)	<p>This field specifies the portion of the installed build version that is used as the value of the User Agent and Server Header in SIP requests. Possible values are:</p> <ul style="list-style-type: none"> • Major and Minor; for example, Cisco-CUCM10.6 • Major; for example, Cisco-CUCM10 • Major, Minor and Revision; for example, Cisco-CUCM10.6.2 • Full Build; for example, Cisco-CUCM10.6.2.98000-19 • None; header is omitted <p>Default: Major and Minor</p>
Dial String Interpretation (Mandatory)	<p>Possible values are:</p> <ul style="list-style-type: none"> • Phone number consists of characters 0-9, *, #, and + (others treated as URI addresses). This is the default value. • Phone number consists of characters 0-9, A-D, *, #, and + (others treated as URI addresses) • Always treat all dial strings as URI addresses
Redirect by Application (Optional)	<p>If you select this check box and configure this SIP Profile on the SIP trunk, the Unified CM administrator can:</p> <ul style="list-style-type: none"> • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the calls get routed correctly. • Prevent a DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. <p>Getting redirected to a restricted phone number (such as an international number) means that handling redirection at stack level causes the call to be routed, not blocked. This behavior occurs if you leave the Redirect by Application check box clear.</p>

Option	Description
Disable Early Media on 180 (Optional)	<p>By default, Unified CM signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in these responses, instead of playing ringback locally, Unified CM connects media. The calling phone then plays whatever the called device is sending (such as ringback or busy signal). If you receive no ringback, the device you are connecting to may include SDP in the 180 response, but not send media before 200OK response. In this case, select this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response.</p> <p>Note:</p> <p>Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.</p>
Outgoing T.38 INVITE include audio mline (Optional)	<p>The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, configure a SIP trunk with this SIP profile.</p> <p>Note:</p> <p>The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.</p>
Use Fully Qualified Domain Name in SIP Requests (Optional)	<p>This feature enables Unified CM to relay a caller's alphanumeric hostname by passing it to the called device or outbound trunk as SIP header information. Enter one of the following:</p> <ul style="list-style-type: none"> f - To disable this option. The IP address for Unified CM is passed to the line device or outbound trunk instead of the user's hostname. t - To enable this option. Unified CM relays an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call originates from a line device on the Unified CM cluster, and is routed on a SIP trunk, then the configured Organizational Top-Level Domain (for example, Cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call originates from a trunk on Unified CM and is being routed on a SIP trunk, then: <ul style="list-style-type: none"> If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging preserves the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. <p>Default: f - Disabled</p>
Assured Services SIP conformance (Optional)	<p>Select this check box for third-party AS-SIP endpoints and AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.</p>

SDP Information settings

Option	Description
SDP Transparency Profile (Optional)	Displays the SDP Transparency Profile Setting (read-only)
Accept Audio Codec Preferences in Received Offer (Optional)	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • On - Enables Unified CM to honor the preference of audio codecs in the received offer and preserve it while processing. • Off - Enables Unified CM to ignore the preference of audio codecs in a received offer and apply the locally configured Audio Codec Preference List. The default selects the service parameter configuration. • Default - Selects the service parameter configuration. <p>Default: Default</p>
Require SDP Inactive Exchange for Mid-Call Media Change (Optional)	<p>This feature determines how Unified CM handles midcall updates to codecs or connection information such as IP address or port numbers.</p> <p>If you select this check box, during midcall codec or connection updates Unified CM sends an INVITE a-inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls.</p> <p>Note</p> <p>For early offer enabled SIP trunks, the Send send-receive SDP in midcall INVITE parameter overrides this parameter.</p> <p>If this check box is clear, Unified CM passes the midcall SDP to the peer leg without sending a prior Inactive SDP to break the media exchange.</p> <p>Default: Clear</p>
Allow RR/RS bandwidth modifier (RFC 3556) (Mandatory)	<p>Specifies the RR (RTDP bandwidth allocated to other participants in an RTP session) and RS (RTCP bandwidth allocated to active data senders) in RFC 3556. Options are:</p> <ul style="list-style-type: none"> • Transport Independent Application Specific bandwidth modifier (TIAS) and AS • TIAS only • AS only • CT only <p>Default: TIAS and AS</p>

Parameters used in Phone settings

Option	Description
Timer Invite Expires (seconds) (Optional)	This field specifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values: Any positive number Default: 180 seconds
Timer Register Delta (seconds) (Optional)	This field is intended to be used by SIP endpoints only. The endpoint receives this value through a TFTP config file. The endpoint reregisters Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station KeepAlive Interval service parameter. Valid values: 0 to 32767 Default: 5 seconds
Timer Register Expires (seconds) (Optional)	This field is intended to be used by SIP endpoints only. The SIP endpoint receives the value through a TFTP config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. Valid values: Any positive number Default: 3600 seconds (1 hour) If the endpoint sends a shorter Expires value than the SIP Station Keepalive Interval service parameter, Unified CM responds with a 423 "Interval Too Brief." If the endpoint sends a greater Expires value than the SIP Station Keepalive Interval service parameter, Unified CM responds with a 200 OK with the Keepalive Interval value for Expires. Note: For mobile phones running SIP, Unified CM uses this value instead of the SIP Station KeepAlive Interval service parameter to determine the registration period. Note: For TCP connections, the value for the Timer Register Expires field must be lower than the value for the SIP TCP Unused Connection service parameter.
Timer T1 (msec) (Optional)	This field specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values: Any positive number Default: 500 msec
Timer T2 (msec) (Optional)	This field specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values: Any positive number Default: 4000 msec
Retry INVITE (Optional)	This field specifies the maximum number of times that an INVITE request gets retransmitted. Valid values: Any positive number Default: 6

Option	Description
Retry Non-INVITE (Optional)	This field specifies the maximum number of times that a SIP message other than an INVITE request gets retransmitted. Valid values: Any positive number Default: 10
Start Media Port (Optional)	This field designates the start real-time protocol (RTP) port for media. Range: 2048 to 65535 Default: 16384
Stop Media Port (Optional)	This field designates the stop real-time protocol (RTP) port for media. Range: 2048 to 65535 Default: 32766
Call Pickup URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call pickup feature.
Call Pickup Group URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call pickup group feature.
Meet Me Service URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the meet me conference feature.
User Info (Optional)	This field configures the user- parameter in the REGISTER message. Valid values are: <ul style="list-style-type: none"> • None - No value is inserted • Phone - The value user-phone is inserted in the To, From, and Contact Header for REGISTER • IP - The value user-ip is inserted in the To, From, and Contact Header for REGISTER Default: None
DTMF DB Level (Optional)	This field specifies the in-band DTMF digit tone level. Valid values are: <ul style="list-style-type: none"> • 6 dB below nominal • 3 dB below nominal • Nominal • 3 dB above nominal • 6 dB above nominal Default: Nominal
Call Hold Ring Back (Optional)	This parameter causes the phone to ring in cases where you have another party on hold when you hang up a call. Valid values are: <ul style="list-style-type: none"> • Off - Off permanently and cannot be turned on and off locally by the user interface • On - On permanently and cannot be turned on and off locally by the user interface
Anonymous Call Block (Optional)	The field configures anonymous call block. Valid values are: <ul style="list-style-type: none"> • Off - Disabled permanently and cannot be turned on and off locally by the user interface • On - Enabled permanently and cannot be turned on and off locally by the user interface

Option	Description
Caller ID Blocking (Optional)	<p>This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or email address from phones that have caller identification enabled. Valid values are:</p> <ul style="list-style-type: none"> • Off - Disabled permanently and cannot be turned on and off locally by the user interface • On - Enabled permanently and cannot be turned on and off locally by the user interface
Do Not Disturb Control (Optional)	<p>This field sets the Do Not Disturb (DND) feature. Valid values are:</p> <ul style="list-style-type: none"> • User - The dndControl parameter for the phone specifies 0. • Admin - The dndControl parameter for the phone specifies 2.
Telnet Level for 7940 and 7960 (Optional)	<p>Cisco Unified IP Phones 7940 and 7960 do not support SSH for sign-in access or HTTP that is used to collect logs. However, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values:</p> <ul style="list-style-type: none"> • Disabled - No access • Limited - Some access but cannot run privileged commands • Enabled - Full access
Resource Priority Namespace (Optional)	<p>This field enables the administrator to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line using its SIP Profile.</p>
Timer Keep Alive Expires (seconds) (Optional)	<p>Unified CM requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages sent to the backup Unified CM to ensure its availability for failover.</p> <p>Default: 120 seconds</p>
Timer Subscribe Expires (seconds) (Optional)	<p>This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the `` Expires `` header field.</p> <p>Valid values: Any positive number</p> <p>Default: 120 seconds</p>
Timer Subscribe Delta (seconds) (Optional)	<p>Use this parameter with the Timer Subscribe Expires setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires.</p> <p>Range: 3 to 15 seconds</p> <p>Default: 5 seconds</p>
Maximum Redirections (Optional)	<p>Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call.</p> <p>Default: 70 redirections</p>
Off hook To First Digit Timer (msec) (Optional)	<p>This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set.</p> <p>Range: 0 to 15,000 microseconds</p> <p>Default: 15,000 microseconds</p>
Call Forward URI (Optional)	<p>This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call forward feature.</p>

Option	Description
Speed Dial (Abbreviated Dial) URI (Optional)	<p>This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the abbreviated dial feature.</p> <p>Speed dials that are not associated with a line key (abbreviated dial indices) do not download to the phone. The phone uses the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI contains the abbreviated dial digits (for example, 14), and the Call-Info header indicates the abbreviated dial feature. Unified CM translates the abbreviated dial digits into the configured digit string and extends the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.</p>
Conference Join Enabled (Optional)	<p>Select this check box to join the remaining conference participants when a conference initiator using a Cisco Unified IP Phone 7940 or 7960 hangs up. Leave it clear if you do not want to join the remaining conference participants.</p> <p>Note:</p> <p>This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.</p>
RFC 2543 Hold (Optional)	<p>Select this check box to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Unified CM. This allows backward compatibility with endpoints that do not support RFC3264.</p>
Semi Attended Transfer (Optional)	<p>This check box determines whether the Cisco Unified IP Phones 7940 and 7960 caller can transfer an attended transfer's second leg while the call is ringing. Select the check box if you want semi attended transfer enabled; leave it clear if you want semi attended transfer disabled.</p> <p>Note:</p> <p>This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.</p>
Enable VAD (Optional)	<p>Select this check box if you want voice activation detection (VAD) enabled; leave it clear if you want VAD disabled. When VAD is enabled, no media is sent when voice is detected.</p>
Stutter Message Waiting (Optional)	<p>Select this check box if you want stutter dial tone when the phone goes off hook and a message is waiting. Leave clear if you do not want a stutter dial tone when a message is waiting.</p> <p>This setting supports Cisco Unified IP Phones 7960 and 7940 that run SIP.</p>
MLPP User Authorization (Optional)	<p>Select this check box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.</p>

Normalization Script settings

Option	Description
Normalization Script	<p>From the drop-down list, choose the script that you want to apply to this SIP profile.</p> <p>To import another script from Unified CM, go to the SIP Normalization Configuration window (Device Device Settings SIP Normalization Script), and import a new script.</p>
Enable Trace	<p>Select this check box to enable tracing within the script or clear this check box to disable tracing. When selected, the trace.output API provided to the Lua scripter produces SDI trace.</p> <p>Note:</p> <p>We recommend that you only enable tracing while debugging a script. Tracing impacts performance and is not recommended under normal operating conditions.</p>
Script Parameters	<p>Enter parameter names and parameter values in the Script Parameters box as comma-delineated key-value pairs. Valid values include all characters except equals signs (-), semicolons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value.</p> <p>Alternatively, to add another parameter line from Unified CM, click the + (plus) button. To delete a parameter line, click the - (minus) button.</p>

Incoming Requests FROM URI Strings settings

Option	Description
Caller ID DN	<p>Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America:</p> <ul style="list-style-type: none"> 555XXXX - Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. 55000 - Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. <p>You can also enter the international escape character +.</p>
Caller Name	<p>Enter a caller name to override the caller name that is received from the originating SIP Device.</p>

Presentation Info

Option	Description
Is Anonymous	Display configured External Presentation Number and External Presentation as Anonymous on the called party device.
External Presentation Name	Configure presentation number of choice.
External Presentation Number	Configure presentation name of choice.

Trunk Specific Configuration settings

Option	Description
Reroute Incoming Request to new Trunk based on	<p>Unified CM only accepts calls from a SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Unified CM accepts the call, Unified CM uses the configuration for this setting to determine whether to reroute the call to another trunk. From the drop-down list, choose the method that Unified CM uses to identify the SIP trunk where the call gets rerouted:</p> <ul style="list-style-type: none"> • Never - If the SIP trunk matches the IP address of the originating device, choose this option. Unified CM, which identifies the trunk by the incoming packet's source IP address and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • Contact Info Header - If the SIP trunk uses a SIP proxy, choose this option. Unified CM parses the IP address or domain name and the signaling port number in the incoming request's header. Unified CM then reroutes the call to the SIP trunk using that IP address and port. If no SIP trunk is identified, the call occurs on the trunk where the call arrived. • Call-Info Header with purpose-x-cisco-origIP - If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Unified CM performs the following: <ul style="list-style-type: none"> – parses the Call-Info header – looks for the parameter <code>purpose-x-cisco-origIP</code> – uses the IP address or domain name and signaling port number in the header to reroute the call to the SIP trunk using the IP address and port <p>If the parameter is not in the header, or no SIP trunk is identified, the call occurs on the SIP trunk where the call arrived.</p> <p>Default: Never</p> <p>Note:</p> <p>This setting does not work for SIP trunks connected to:</p> <ul style="list-style-type: none"> • A Unified CM IM and Presence Service proxy server. • Originating gateways in different Unified CM groups

Option	Description
RSVP Over SIP	<p>This field configures RSVP over SIP trunks. From the drop-down list, choose the method that Unified CM uses to configure RSVP over SIP trunks:</p> <ul style="list-style-type: none"> • Local RSVP - In a local configuration, RSVP occurs within each cluster, between the endpoint and the local SIP trunk, but not on the WAN link between the clusters. • E2E - In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the endpoints, including within the local cluster and over the WAN.
Resource Priority Namespace List	<p>Select a configured Resource Priority Namespace list from the drop-down menu. The Namespace List is configured in Unified CM in the Resource Priority Namespace List menu. You can access the menu in Unified CM from System MLPP > Namespace.</p>
Fall back to local RSVP	<p>Select this check box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this check box is clear, end-to-end RSVP calls that cannot establish an end-to-end connection fail.</p>
SIP Rel1XX Options	<p>This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint. Valid values are:</p> <ul style="list-style-type: none"> • Disabled - Disables SIP Rel1XX. • Send PRACK if 1XX contains SDP - Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • Send PRACK for all 1XX messages - Acknowledges all 1XX messages with PRACK. <p>If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.</p>
Video Call Traffic Class	<p>Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list, select one of:</p> <ul style="list-style-type: none"> • Immersive - High-definition immersive video. • Desktop - Standard desktop video. • Mixed - A mix of immersive and desktop video. <p>Unified CM Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth and Immersive Bandwidth. The pool used depends on the type of call determined by the Video Call Traffic Class. Refer to the “Call Admission Control” chapter of the Cisco Unified Communications Manager System Guide for more information.</p>

Option	Description
Calling Line Identification Presentation (Mandatory)	<p>Select one of:</p> <ul style="list-style-type: none"> • Strict From URI presentation Only - To select the network-provided identity • Strict Identity Headers presentation Only - To select the user-provided identity • Default - To select the system default calling line identification <p>Default: Default</p>
Session Refresh Method (Mandatory)	<p>Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions. This allows the Unified CM and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified CM received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified CM initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified CM can send both Update and Invite requests.</p> <p>Specify whether to use Invite or Update as the Session Refresh Method.</p> <p>Default: Invite</p> <p>Note:</p> <p>Sending a midcall Invite request requires specifying an offer SDP in the request. This means that the far end must send an answer SDP in the Invite response.</p> <p>Update: Unified CM requests a SIP Update if the SIP session's far end supports the Update method in the Supported or Require headers. When sending the Update request, the Unified CM includes an SDP. This simplifies the session refresh since no SDP offer or answer exchange is required.</p> <p>Note:</p> <p>If the far end of the SIP session does not support the Update method, the Unified CM continues using the Invite method for session refresh.</p>
Early Offer Support for voice and video calls (Mandatory)	<p>This field configures Early Offer support for voice and video calls. When enabled, Early Offer support includes a session description in the initial INVITE for outbound calls. Early Offer configuration settings on SIP profile apply only to SIP trunk calls. These configuration settings do not affect SIP line side calls. If this profile is shared between a trunk and a line, only a SIP trunk that uses the profile is affected by these settings.</p> <p>The Media Transfer Point (MTP) Required check box on the Trunk Configuration window, if enabled, overrides the early offer configuration on the associated SIP profile. Unified CM sends the MTP IP address and port with a single codec in the SDP in the initial INVITE.</p> <p>From the drop-down list box, select one of the following three options:</p> <ul style="list-style-type: none"> • Disabled (Default value) - Disables Early Offer; no SDP will be included in the initial INVITE for outbound calls. • Best Effort (no MTP Inserted) <ul style="list-style-type: none"> – Provide Early Offer for the outbound call only when caller side's media port, IP and codec information is available. – Provide Delayed Offer for the outbound call when caller side's media port, IP and codec information is not available. No MTP is inserted to provide Early Offer in this case. • Mandatory (insert MTP if needed) - Provide Early Offer for all outbound calls and insert MTP when caller side's media port, IP and codec information is not available. <p>Default: Disabled (Default value)</p>

Option	Description
Enable ANAT	<p>This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Selecting the Enable ANAT and MTP Required check boxes sets Unified CM to insert a dual-stack MTP and send an offer with two m-lines, for IPv4 and IPv6. If a dual-stack MTP cannot be allocated, Unified CM sends an INVITE without SDP.</p> <p>When you select the Enable ANAT check box and the Media Termination Point Required check box is clear, Unified CM sends an INVITE without SDP. When the Enable ANAT and MTP Required check boxes are cleared (or when an MTP cannot be allocated), Unified CM sends an INVITE without SDP.</p> <p>When you clear the Enable ANAT check box but you select the MTP Required check box, consider the information, which assumes that an MTP can be allocated:</p> <ul style="list-style-type: none"> Unified CM sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. Unified CM sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. For dual-stack SIP trunks, Unified CM determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.
Deliver Conference Bridge Identifier	<p>When checked, the SIP trunk passes the b-number identifying the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require this field.</p> <p>Selecting this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work.</p> <p>Selecting this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.</p>
Allow Passthrough of Configured Line Device Caller Information	Select this check box to allow passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Select this check box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Select this check box to reject anonymous outgoing calls.
Send ILS Learned Destination Route String	<p>When this check box is selected, for calls routed to a learned directory URI, learned number, or learned pattern, Unified CM:</p> <ul style="list-style-type: none"> adds the <code>x-cisco-dest-route-string</code> header to outgoing SIP INVITE and SUBSCRIBE messages inserts the destination route string into the header <p>When this check box is clear, Unified CM does not add the <code>x-cisco-dest-route-string</code> header to any SIP messages.</p> <p>The <code>x-cisco-dest-route-string</code> header allows Unified CM to route calls across a Session Border Controller.</p>

Trunk SIP OPTIONS Ping settings

Option	Description
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	<p>Select this check box if you want to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device is unresponsive or returns a SIP error response such as 503 Service Unavailable or 408 Timeout, Unified CM reroutes the calls by using other trunks or a different address.</p> <p>If this check box is clear, the SIP trunk does not track the status of SIP trunk destinations.</p> <p>When this check box is selected, you can configure two request timers.</p>
Ping Interval for In-service and Partially In-service Trunks (seconds)	<p>This field configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.</p> <p>Default: 60 seconds Range: 5 to 600 seconds</p>
Ping Interval for Out-of-service Trunks (seconds)	<p>This field configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if:</p> <ul style="list-style-type: none"> • it fails to respond to OPTIONS • it sends 503 or 408 responses • the Transport Control Protocol (TCP) connection cannot be established <p>If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.</p> <p>Default: 120 seconds Range: 5 to 600 seconds</p>
Ping Retry Timer (msec)	<p>This field specifies the maximum waiting time before retransmitting the OPTIONS request.</p> <p>Range: 100 to 1000 milliseconds Default: 500 milliseconds</p>
Ping Retry Count	<p>This field specifies the number of times that Unified CM resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low.</p> <p>Range: 1 to 10 Default: 6</p>

Trunk SDP Information settings

Option	Description
Send send-receive SDP in midcall INVITE	<p>Select this check box to prevent Unified CM from sending an INVITE a-inactive SDP message during call hold or media break during supplementary services.</p> <p>Note:</p> <p>This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls.</p> <p>When you enable Send send-receive SDP in midcall INVITE for an early offer SIP trunk in tandem mode, Unified CM inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a-inactive or sendonly or recvonly in audio media line. In tandem mode, Unified CM depends on the SIP devices to reestablish media path by sending either a delayed INVITE or midcall INVITE with send-recv SDP.</p> <p>When you enable Send send-receive SDP in midcall INVITE and Require SDP Inactive Exchange for Mid-Call Media Change on the same SIP Profile, the Send send-receive SDP in midcall INVITE overrides the Require SDP Inactive Exchange for Mid-Call Media Change, so Unified CM does not send an INVITE with a-inactive SDP in midcall codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled.</p> <p>Note:</p> <p>To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter in Unified CM (System Service Parameters) to True.</p>
Allow Presentation Sharing using BFCP	<p>If the check box is selected, Unified CM allows supported SIP endpoints to use the Binary Floor Control Protocol (BFCP) to enable presentation sharing. The use of BFCP creates an added media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from someone's laptop, into a SIP videophone.</p> <p>If the check box is clear, Unified CM rejects BFCP offers from devices associated with the SIP profile. The BFCP application line and associated media line ports are set to 0 in the answering SDP message.</p> <p>Default: Clear</p> <p>Note:</p> <p>BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP, or Transcoder. For more information on BFCP, refer to the Cisco Unified Communications Manager System Guide.</p>

Option	Description
Allow iX Application Media	Select this check box to enable support for iX media channel.
Allow multiple codecs in answer SDP	<p>This option applies when incoming SIP signals do not indicate support for multiple codec negotiation and Unified CM can finalize the negotiated codec. When this check box is selected, the endpoint behind the trunk can handle multiple codecs in the answer SDP.</p> <p>For example, an endpoint that supports multiple codec negotiation calls the SIP trunk, and Unified CM sends a Delay Offer request to a trunk. The endpoint behind the trunk returns all support codecs without the Contact header to indicate the support of multiple codec negotiation.</p> <p>In this case, Unified CM identifies that the trunk can handle multiple codec negotiation, and sends SIP response messages to both endpoints with multiple common codecs.</p> <p>When clear, Unified CM identifies that the endpoint behind the trunk cannot handle multiple codec negotiation, unless SIP contact header URI states it can. Unified CM continues the call with single codec negotiation.</p>

4.23.2. SIP profile configuration

Tip: *Use the Action search to navigate Automate*

Option	Description
Name (Mandatory)	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description (Optional)	This field identifies the purpose of the SIP profile; for example, SIP for 7970. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Default MTP Telephony Event Payload Type (Optional)	<p>This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. Usually, the default value specifies the appropriate payload type. Be sure that you have a good understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated.</p> <p>Default-101 Range-96 to 127</p> <p>This parameter's value affects calls with the following conditions:</p> <ul style="list-style-type: none"> • An outgoing SIP call from Cisco Unified Communications Manager • For the calling SIP trunk, the Media Termination Point Required check box is checked on the SIP Trunk Configuration window
Early Offer for G.Clear Calls (Optional)	<p>This feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options:</p> <ul style="list-style-type: none"> • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD

Option	Description
User-Agent and Server header information (Mandatory)	<p>This feature indicates how Unified CM handles the User-Agent and Server header information in a SIP message.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Send Unified CM Version Information as User-Agent Header - For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified CM passes any contact headers through untouched. • Pass Through Received Information as Contact Header Parameters - If selected, the User-Agent and Server header information is passed as Contact header parameters. The User-Agent and Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent and Server headers. • Pass Through Received Information as User-Agent and Server Header - If selected, the User-Agent and Server header information is passed as User-Agent and Server headers. The User-Agent and Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent and Server headers. <p>Default: Send Unified CM Version Information as User-Agent Header</p>
Version in User Agent and Server Header (Mandatory)	<p>This field specifies the portion of the installed build version that is used as the value of the User Agent and Server Header in SIP requests.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Major and Minor; for example, Cisco-CUCM10.6 • Major; for example, Cisco-CUCM10 • Major, Minor and Revision; for example, Cisco-CUCM10.6.2 • Full Build; for example, Cisco-CUCM10.6.2.98000-19 • None; header is omitted <p>Default: Major and Minor</p>
Dial String Interpretation (Mandatory)	<p>Possible values are:</p> <ul style="list-style-type: none"> • Phone number consists of characters 0-9, *, #, and + (others treated as URI addresses). This is the default value. • Phone number consists of characters 0-9, A-D, *, #, and + (others treated as URI addresses) • Always treat all dial strings as URI addresses

Option	Description
Redirect by Application (Optional)	<p>If you select this check box and configure this SIP Profile on the SIP trunk, the Unified CM administrator can:</p> <ul style="list-style-type: none"> • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the calls get routed correctly. • Prevent a DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. <p>Getting redirected to a restricted phone number (such as an international number) means that handling redirection at stack level causes the call to be routed, not blocked. This behavior occurs if you leave the Redirect by Application check box clear.</p>
Disable Early Media on 180 (Optional)	<p>By default, Unified CM signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in these responses, instead of playing ringback locally, Unified CM connects media. The calling phone then plays whatever the called device is sending (such as ringback or busy signal). If you receive no ringback, the device you are connecting to may include SDP in the 180 response, but not send media before 200OK response. In this case, select this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response.</p> <p>Note:</p> <p>Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.</p>
Outgoing T.38 INVITE include audio mline (Optional)	<p>The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, configure a SIP trunk with this SIP profile.</p> <p>Note:</p> <p>The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.</p>

Option	Description
Use Fully Qualified Domain Name in SIP Requests (Optional)	<p>This feature enables Unified CM to relay a caller's alphanumeric hostname by passing it to the called device or outbound trunk as SIP header information. Enter one of the following:</p> <p>f - To disable this option. The IP address for Unified CM is passed to the line device or outbound trunk instead of the user's hostname.</p> <p>t - To enable this option. Unified CM relays an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call originates from a line device on the Unified CM cluster, and is routed on a SIP trunk, then the configured Organizational Top-Level Domain (for example, Cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call originates from a trunk on Unified CM and is being routed on a SIP trunk, then:</p> <ul style="list-style-type: none"> • If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging preserves the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. • If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. <p>Default: f - Disabled</p>
Assured Services SIP conformance (Optional)	<p>Select this check box for third-party AS-SIP endpoints and AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.</p>

Table: SDP Information Tab

Option	Description
SDP Transparency Profile (Optional)	Displays the SDP Transparency Profile Setting (read-only)
Accept Audio Codec Preferences in Received Offer (Optional)	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • On - Enables Unified CM to honor the preference of audio codecs in the received offer and preserve it while processing. • Off - Enables Unified CM to ignore the preference of audio codecs in a received offer and apply the locally configured Audio Codec Preference List. The default selects the service parameter configuration. • Default - Selects the service parameter configuration. <p>Default: Default</p>
Require SDP Inactive Exchange for Mid-Call Media Change (Optional)	<p>This feature determines how Unified CM handles midcall updates to codecs or connection information such as IP address or port numbers. If you select this check box, during midcall codec or connection updates Unified CM sends an INVITE a-inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls.</p> <p>Note</p> <p>For early offer enabled SIP trunks, the Send send-receive SDP in midcall INVITE parameter overrides this parameter.</p> <p>If this check box is clear, Unified CM passes the midcall SDP to the peer leg without sending a prior Inactive SDP to break the media exchange.</p> <p>Default: Clear</p>
Allow RR/RS bandwidth modifier (RFC 3556) (Mandatory)	<p>Specifies the RR (RTDP bandwidth allocated to other participants in an RTP session) and RS (RTCP bandwidth allocated to active data senders) in RFC 3556. Options are:</p> <ul style="list-style-type: none"> • Transport Independent Application Specific bandwidth modifier (TIAS) and AS • TIAS only • AS only • CT only <p>Default: TIAS and AS</p>

Table: Parameters used in Phone Tab

Option	Description
Timer Invite Expires (seconds) (Optional)	This field specifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values: Any positive number Default: 180 seconds
Timer Register Delta (seconds) (Optional)	This field is intended to be used by SIP endpoints only. The endpoint receives this value through a TFTP config file. The endpoint reregisters Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station KeepAlive Interval service parameter. Valid values: 0 to 32767 Default: 5 seconds
Timer Register Expires (seconds) (Optional)	This field is intended to be used by SIP endpoints only. The SIP endpoint receives the value through a TFTP config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. Valid values: Any positive number Default: 3600 seconds (1 hour) If the endpoint sends a shorter Expires value than the SIP Station Keepalive Interval service parameter, Unified CM responds with a 423 "Interval Too Brief." If the endpoint sends a greater Expires value than the SIP Station Keepalive Interval service parameter, Unified CM responds with a 200 OK with the Keepalive Interval value for Expires. Note: For mobile phones running SIP, Unified CM uses this value instead of the SIP Station KeepAlive Interval service parameter to determine the registration period. Note: For TCP connections, the value for the Timer Register Expires field must be lower than the value for the SIP TCP Unused Connection service parameter.
Timer T1 (msec) (Optional)	This field specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values: Any positive number Default: 500 msec
Timer T2 (msec) (Optional)	This field specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values: Any positive number Default: 4000 msec
Retry INVITE (Optional)	This field specifies the maximum number of times that an INVITE request gets retransmitted. Valid values: Any positive number Default: 6

Option	Description
Retry Non-INVITE (Optional)	This field specifies the maximum number of times that a SIP message other than an INVITE request gets retransmitted. Valid values: Any positive number Default: 10
Start Media Port (Optional)	This field designates the start real-time protocol (RTP) port for media. Range: 2048 to 65535 Default: 16384

Option	Description
Stop Media Port (Optional)	This field designates the stop real-time protocol (RTP) port for media. Range: 2048 to 65535 Default: 32766
Call Pickup URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call pickup feature.
Call Pickup Group URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call pickup group feature.
Meet Me Service URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the meet me conference feature.
User Info (Optional)	This field configures the user- parameter in the REGISTER message. Valid values are: <ul style="list-style-type: none"> • None - No value is inserted • Phone - The value user-phone is inserted in the To, From, and Contact Header for REGISTER • IP - The value user-ip is inserted in the To, From, and Contact Header for REGISTER Default: None
DTMF DB Level (Optional)	This field specifies the in-band DTMF digit tone level. Valid values are: <ul style="list-style-type: none"> • 6 dB below nominal • 3 dB below nominal • Nominal • 3 dB above nominal • 6 dB above nominal Default: Nominal
Call Hold Ring Back (Optional)	This parameter causes the phone to ring in cases where you have another party on hold when you hang up a call. Valid values are: <ul style="list-style-type: none"> • Off - Off permanently and cannot be turned on and off locally by the user interface • On - On permanently and cannot be turned on and off locally by the user interface

Option	Description
Anonymous Call Block (Optional)	The field configures anonymous call block. Valid values are: <ul style="list-style-type: none">• Off - Disabled permanently and cannot be turned on and off locally by the user interface• On - Enabled permanently and cannot be turned on and off locally by the user interface
Caller ID Blocking (Optional)	This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or email address from phones that have caller identification enabled. Valid values are: <ul style="list-style-type: none">• Off - Disabled permanently and cannot be turned on and off locally by the user interface• On - Enabled permanently and cannot be turned on and off locally by the user interface
Do Not Disturb Control (Optional)	This field sets the Do Not Disturb (DND) feature. Valid values are: <ul style="list-style-type: none">• User - The dndControl parameter for the phone specifies 0.• Admin - The dndControl parameter for the phone specifies 2.

Option	Description
Telnet Level for 7940 and 7960 (Optional)	<p>Cisco Unified IP Phones 7940 and 7960 do not support SSH for sign-in access or HTTP that is used to collect logs. However, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values:</p> <ul style="list-style-type: none"> • Disabled - No access • Limited - Some access but cannot run privileged commands • Enabled - Full access
Resource Priority Namespace (Optional)	This field enables the administrator to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line using its SIP Profile.
Timer Keep Alive Expires (seconds) (Optional)	<p>Unified CM requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages sent to the backup Unified CM to ensure its availability for failover.</p> <p>Default: 120 seconds</p>
Timer Subscribe Expires (seconds) (Optional)	<p>This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the `` Expires `` header field.</p> <p>Valid values: Any positive number</p> <p>Default: 120 seconds</p>
Timer Subscribe Delta (seconds) (Optional)	<p>Use this parameter with the Timer Subscribe Expires setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires.</p> <p>Range: 3 to 15 seconds</p> <p>Default: 5 seconds</p>
Maximum Redirections (Optional)	<p>Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call.</p> <p>Default: 70 redirections</p>
Off hook To First Digit Timer (msec) (Optional)	<p>This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set.</p> <p>Range: 0 to 15,000 microseconds</p> <p>Default: 15,000 microseconds</p>

Option	Description
Call Forward URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call forward feature.
Speed Dial (Abbreviated Dial) URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) do not download to the phone. The phone uses the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI contains the abbreviated dial digits (for example, 14), and the Call-Info header indicates the abbreviated dial feature. Unified CM translates the abbreviated dial digits into the configured digit string and extends the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.
Conference Join Enabled (Optional)	Select this check box to join the remaining conference participants when a conference initiator using a Cisco Unified IP Phone 7940 or 7960 hangs up. Leave it clear if you do not want to join the remaining conference participants. Note: This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.

Option	Description
RFC 2543 Hold (Optional)	Select this check box to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Unified CM. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer (Optional)	This check box determines whether the Cisco Unified IP Phones 7940 and 7960 caller can transfer an attended transfer's second leg while the call is ringing. Select the check box if you want semi attended transfer enabled; leave it clear if you want semi attended transfer disabled. Note: This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.
Enable VAD (Optional)	Select this check box if you want voice activation detection (VAD) enabled; leave it clear if you want VAD disabled. When VAD is enabled, no media is sent when voice is detected.
Stutter Message Waiting (Optional)	Select this check box if you want stutter dial tone when the phone goes off hook and a message is waiting. Leave clear if you do not want a stutter dial tone when a message is waiting. This setting supports Cisco Unified IP Phones 7960 and 7940 that run SIP.
MLPP User Authorization (Optional)	Select this check box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.

Table: Normalization Script Tab

Option	Description
Normalization Script	From the drop-down list, choose the script that you want to apply to this SIP profile. To import another script from Unified CM, go to the SIP Normalization Configuration window (Device Device Settings SIP Normalization Script), and import a new script.
Enable Trace	Select this check box to enable tracing within the script or clear this check box to disable tracing. When selected, the trace.output API provided to the Lua scripter produces SDI trace. Note: We recommend that you only enable tracing while debugging a script. Tracing impacts performance and is not recommended under normal operating conditions.
Script Parameters	Enter parameter names and parameter values in the Script Parameters box as comma-delineated key-value pairs. Valid values include all characters except equals signs (=), semicolons (;), and nonprintable characters, such as tabs. You can enter a parameter name with no value. Alternatively, to add another parameter line from Unified CM, click the + (plus) button. To delete a parameter line, click the - (minus) button.

Table: Incoming Requests FROM URI Settings Tab

Option	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: <ul style="list-style-type: none"> 555XXXX - Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. 55000 - Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.

Table: Trunk Specific Configuration Tab

Option	Description
Reroute Incoming Request to new Trunk based on	<p>Unified CM only accepts calls from a SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Unified CM accepts the call, Unified CM uses the configuration for this setting to determine whether to reroute the call to another trunk.</p> <p>From the drop-down list, choose the method that Unified CM uses to identify the SIP trunk where the call gets rerouted:</p> <ul style="list-style-type: none"> • Never - If the SIP trunk matches the IP address of the originating device, choose this option. Unified CM, which identifies the trunk by the incoming packet's source IP address and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • Contact Info Header - If the SIP trunk uses a SIP proxy, choose this option. Unified CM parses the IP address or domain name and the signaling port number in the incoming request's header. Unified CM then reroutes the call to the SIP trunk using that IP address and port. If no SIP trunk is identified, the call occurs on the trunk where the call arrived. • Call-Info Header with purpose-x-cisco-origIP - If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Unified CM performs the following: <ul style="list-style-type: none"> – parses the Call-Info header – looks for the parameter <code>purpose-x-cisco-origIP</code> – uses the IP address or domain name and signaling port number in the header to reroute the call to the SIP trunk using the IP address and port <p>If the parameter is not in the header, or no SIP trunk is identified, the call occurs on the SIP trunk where the call arrived.</p> <p>Default: Never</p> <p>Note:</p> <p>This setting does not work for SIP trunks connected to:</p> <ul style="list-style-type: none"> • A Unified CM IM and Presence Service proxy server. • Originating gateways in different Unified CM groups

Option	Description
RSVP Over SIP	<p>This field configures RSVP over SIP trunks. From the drop-down list, choose the method that Unified CM uses to configure RSVP over SIP trunks:</p> <ul style="list-style-type: none"> • Local RSVP - In a local configuration, RSVP occurs within each cluster, between the endpoint and the local SIP trunk, but not on the WAN link between the clusters. • E2E - In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the endpoints, including within the local cluster and over the WAN.
Resource Priority Namespace List	<p>Select a configured Resource Priority Namespace list from the drop-down menu. The Namespace List is configured in Unified CM in the Resource Priority Namespace List menu. You can access the menu in Unified CM from System MLPP > Namespace.</p>
Fall back to local RSVP	<p>Select this check box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this check box is clear, end-to-end RSVP calls that cannot establish an end-to-end connection fail.</p>
SIP Rel1XX Options	<p>This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint. Valid values are:</p> <ul style="list-style-type: none"> • Disabled - Disables SIP Rel1XX. • Send PRACK if 1XX contains SDP - Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • Send PRACK for all 1XX messages - Acknowledges all 1XX messages with PRACK. <p>If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.</p>
Video Call Traffic Class	<p>Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list, select one of:</p> <ul style="list-style-type: none"> • Immersive - High-definition immersive video. • Desktop - Standard desktop video. • Mixed - A mix of immersive and desktop video. <p>Unified CM Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth and Immersive Bandwidth. The pool used depends on the type of call determined by the Video Call Traffic Class. Refer to the “Call Admission Control” chapter of the Cisco Unified Communications Manager System Guide for more information.</p>

Option	Description
Calling Line Identification Presentation (Mandatory)	<p>Select one of:</p> <ul style="list-style-type: none"> • Strict From URI presentation Only - To select the network-provided identity • Strict Identity Headers presentation Only - To select the user-provided identity • Default - To select the system default calling line identification <p>Default: Default</p>
Session Refresh Method (Mandatory)	<p>Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions. This allows the Unified CM and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified CM received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified CM initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified CM can send both Update and Invite requests.</p> <p>Specify whether to use Invite or Update as the Session Refresh Method.</p> <p>Default: Invite</p> <p>Note:</p> <p>Sending a midcall Invite request requires specifying an offer SDP in the request. This means that the far end must send an answer SDP in the Invite response.</p> <p>Update: Unified CM requests a SIP Update if the SIP session's far end supports the Update method in the Supported or Require headers. When sending the Update request, the Unified CM includes an SDP. This simplifies the session refresh since no SDP offer or answer exchange is required.</p> <p>Note:</p> <p>If the far end of the SIP session does not support the Update method, the Unified CM continues using the Invite method for session refresh.</p>

Option	Description
Enable ANAT	<p>This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media.</p> <p>Selecting the Enable ANAT and MTP Required check boxes sets Unified CM to insert a dual-stack MTP and send an offer with two m-lines, for IPv4 and IPv6. If a dual-stack MTP cannot be allocated, Unified CM sends an INVITE without SDP.</p> <p>When you select the Enable ANAT check box and the Media Termination Point Required check box is clear, Unified CM sends an INVITE without SDP.</p> <p>When the Enable ANAT and MTP Required check boxes are cleared (or when an MTP cannot be allocated), Unified CM sends an INVITE without SDP.</p> <p>When you clear the Enable ANAT check box but you select the MTP Required check box, consider the information, which assumes that an MTP can be allocated:</p> <ul style="list-style-type: none"> • Unified CM sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Unified CM sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Unified CM determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.
Deliver Conference Bridge Identifier	<p>When checked, the SIP trunk passes the b-number identifying the conference bridge across the trunk instead of changing the b-number to the null value.</p> <p>The terminating side does not require this field.</p> <p>Selecting this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work.</p> <p>Selecting this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.</p>
Allow Passthrough of Configured Line Device Caller Information	<p>Select this check box to allow passthrough of configured line device caller information from the SIP trunk.</p>

Option	Description
Reject Anonymous Incoming Calls	Select this check box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Select this check box to reject anonymous outgoing calls.
Send ILS Learned Destination Route String	<p>When this check box is selected, for calls routed to a learned directory URI, learned number, or learned pattern, Unified CM:</p> <ul style="list-style-type: none">• adds the <code>x-cisco-dest-route-string</code> header to outgoing SIP INVITE and SUBSCRIBE messages• inserts the destination route string into the header <p>When this check box is clear, Unified CM does not add the <code>x-cisco-dest-route-string</code> header to any SIP messages.</p> <p>The <code>x-cisco-dest-route-string</code> header allows Unified CM to route calls across a Session Border Controller.</p>

Table: Trunk SIP OPTIONS Ping Tab

Option	Description
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	<p>Select this check box if you want to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device is unresponsive or returns a SIP error response such as 503 Service Unavailable or 408 Timeout, Unified CM reroutes the calls by using other trunks or a different address. If this check box is clear, the SIP trunk does not track the status of SIP trunk destinations.</p> <p>When this check box is selected, you can configure two request timers.</p>
Ping Interval for In-service and Partially In-service Trunks (seconds)	<p>This field configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.</p> <p>Default: 60 seconds Range: 5 to 600 seconds</p>
Ping Interval for Out-of-service Trunks (seconds)	<p>This field configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if:</p> <ul style="list-style-type: none"> • it fails to respond to OPTIONS • it sends 503 or 408 responses • the Transport Control Protocol (TCP) connection cannot be established <p>If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.</p> <p>Default: 120 seconds Range: 5 to 600 seconds</p>
Ping Retry Timer (msec)	<p>This field specifies the maximum waiting time before retransmitting the OPTIONS request.</p> <p>Range: 100 to 1000 milliseconds Default: 500 milliseconds</p>
Ping Retry Count	<p>This field specifies the number of times that Unified CM resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low.</p> <p>Range: 1 to 10 Default: 6</p>

Table: Trunk SDP Information Tab

Option	Description
Send send-receive SDP in midcall INVITE	<p>Select this check box to prevent Unified CM from sending an INVITE a-inactive SDP message during call hold or media break during supplementary services.</p> <p>Note:</p> <p>This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls.</p> <p>When you enable Send send-receive SDP in midcall INVITE for an early offer SIP trunk in tandem mode, Unified CM inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a-inactive or sendonly or recvonly in audio media line. In tandem mode, Unified CM depends on the SIP devices to reestablish media path by sending either a delayed INVITE or midcall INVITE with send-recv SDP.</p> <p>When you enable Send send-receive SDP in midcall INVITE and Require SDP Inactive Exchange for Mid-Call Media Change on the same SIP Profile, the Send send-receive SDP in midcall INVITE overrides the Require SDP Inactive Exchange for Mid-Call Media Change, so Unified CM does not send an INVITE with a-inactive SDP in midcall codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled.</p> <p>Note:</p> <p>To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter in Unified CM (System Service Parameters) to True.</p>

Option	Description
Allow Presentation Sharing using BFCP	<p>If the check box is selected, Unified CM allows supported SIP endpoints to use the Binary Floor Control Protocol (BFCP) to enable presentation sharing.</p> <p>The use of BFCP creates an added media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from someone's laptop, into a SIP videophone.</p> <p>If the check box is clear, Unified CM rejects BFCP offers from devices associated with the SIP profile. The BFCP application line and associated media line ports are set to 0 in the answering SDP message.</p> <p>Default: Clear</p> <p>Note:</p> <p>BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP, or Transcoder.</p> <p>For more information on BFCP, refer to the Cisco Unified Communications Manager System Guide.</p>
Allow iX Application Media	Select this check box to enable support for iX media channel.
Allow multiple codecs in answer SDP	<p>This option applies when incoming SIP signals do not indicate support for multiple codec negotiation and Unified CM can finalize the negotiated codec.</p> <p>When this check box is selected, the endpoint behind the trunk can handle multiple codecs in the answer SDP.</p> <p>For example, an endpoint that supports multiple codec negotiation calls the SIP trunk, and Unified CM sends a Delay Offer request to a trunk. The endpoint behind the trunk returns all support codecs without the Contact header to indicate the support of multiple codec negotiation.</p> <p>In this case, Unified CM identifies that the trunk can handle multiple codec negotiation, and sends SIP response messages to both endpoints with multiple common codecs.</p> <p>When clear, Unified CM identifies that the endpoint behind the trunk cannot handle multiple codec negotiation, unless SIP contact header URI states it can. Unified CM continues the call with single codec negotiation.</p>

4.24. Configure SIP trunk security profiles

4.24.1. SIP trunk security profiles

provider

Tip: Use the Action search to navigate Automate

Add or edit SIP trunk security profiles

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (CUCM, or CallManager) is configured.
3. Go to **SIP Trunk Security Profiles**.
4. **Choose an option:**
 - **Add a new SIP trunk security profile?** Click the Plus icon (+) to add a new record, then go to Step 5.
 - **Edit an existing SIP trunk security profile?** Click the SIP trunk security profile to be updated. Go to Step 6.
5. If the **Network Device List** dialog displays, select the NDL for the SIP trunk security profile from the drop-down. The dialog displays only when you're on a non-site hierarchy node. If you're at a site hierarchy node, the NDL associated with the site is automatically used.

Note: The **Network Device List** drop-down displays when a SIP trunk security profile is added. It does not display when you edit a SIP trunk security profile.

6. Mandatory. Fill out a unique name for the new SIP trunk security profile in the **Name** field, or modify the existing Name if desired.
7. Complete, at minimum, the other mandatory [SIP trunk security profile settings](#)
8. Click **Save** to save a new SIP trunk security profile or to update an existing SIP trunk security profile.

SIP trunk security profile settings

SIP trunk security profiles are configured on the **SIP Trunk Security Profiles** page.

The table describes the configuration options on this page:

Option	Description
Name (Mandatory)	Enter a name for the security profile. When you save the new profile, the name displays in the SIP Trunk Security Profile drop-down list in the Trunk Configuration window. The maximum length for the name is 64 characters.
Description (Optional)	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Security Mode (Optional)	<p>From the drop-down list, choose one of the following options:</p> <ul style="list-style-type: none"> • Non Secure - No security features except image authentication apply. A TCP or UDP connection opens to Cisco Unified Communications Manager. • Authenticated - Unified CM provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • Encrypted - Unified CM provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling.
Incoming Transport Type (Optional)	<p>Choose one of:</p> <ul style="list-style-type: none"> • TCP+UDP • UDP • TLS • TCP <p>If you do not specify an incoming transport type, TCP+UDP is assigned.</p> <p>When Device Security Mode is Non Secure, TCP+UDP specifies the transport type.</p> <p>When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type.</p> <p>Note: The Transport Layer Security (TLS) protocol secures the connection between Unified CM and the trunk.</p>

Option	Description
Outgoing Transport Type (Optional)	<p>From the drop-down list, choose the outgoing transport mode. Choose one of:</p> <ul style="list-style-type: none"> • TCP+UDP • UDP • TLS • TCP <p>When Device Security Mode is Non Secure, choose TCP or UDP. When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type.</p> <p>Note: TLS ensures signaling integrity, device authentication, and signaling encryption for SIP trunks.</p> <p>Tip: Use UDP as the outgoing transport type when connecting SIP trunks between Unified CM systems and IOS gateways that do not support TCP connection reuse. See “Understanding Session Initiation Protocol (SIP)” in the “Cisco Unified Communications Manager System Guide” for more information.</p>
Enable Digest Authentication (Optional)	<p>Select this check box to enable digest authentication. If you select this check box, Unified CM challenges all SIP requests from the trunk.</p> <p>Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of Authenticated or Encrypted to use these features.</p> <p>Tip: Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.</p>
Nonce Validity Time (mins) (Optional)	<p>Enter the number of minutes (in seconds) that the nonce value is valid. When the time expires, Unified CM generates a new value.</p> <p>Note: A nonce value (a random number that supports digest authentication) is used to calculate the MD5 hash of the digest authentication password. Default = 600 minutes. If you do not specify a Nonce Validity Time, the default of 600 minutes is assigned.</p>

Option	Description
X.509 Subject Name (Optional)	<p>This field applies if you configured TLS for the incoming and outgoing transport type.</p> <p>For device authentication, enter the subject name of the X.509 certificate for the SIP trunk device. If you have a Unified CM cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts. This situation results in multiple X.509 subject names for the trunk. If multiple X.509 subject names exist, enter one of the following characters to separate the names: space, comma, semicolon, or a colon.</p> <p>You can enter up to 4096 characters in this field.</p> <p>Tip:</p> <p>The subject name corresponds to the source connection TLS certificate. Ensure that subject names are unique for each subject name and port. You cannot assign the same subject name and incoming port combination to different SIP trunks.</p> <p>Example:</p> <p>SIP TLS trunk1 on port 5061 has X.509 Subject Names my_cm1, my_cm2.</p> <p>SIP TLS trunk2 on port 5071 has X.509 Subject Names my_cm2, my_cm3.</p> <p>SIP TLS trunk3 on port 5061 can have X.509 Subject Name my_ccm4 but cannot have X.509 Subject Name my_cm1.</p>
Incoming Port (Optional)	<p>Choose the incoming port. Enter a value that is a unique port number from 0 to 65535. The value that you enter applies to all SIP trunks that use the profile. The default port value for incoming TCP and UDP SIP messages is 5060. The default SIP secured port for incoming TLS messages is 5061.</p> <p>If the incoming port is not specified, the default port of 5060 is used.</p> <p>Tip:</p> <p>All SIP trunks that use TLS can share the same incoming port; all SIP trunks that use TCP + UDP can share the same incoming port. You cannot mix SIP TLS transport trunks with SIP non-TLS transport trunk types on the same port.</p>

Option	Description
Enable application level authorization (Optional)	<p>Application-level authorization applies to applications that are connected through the SIP trunk.</p> <p>If you select this check box, also select the Enable Digest Authentication check box and configure digest authentication for the trunk. Unified CM authenticates a SIP application user before checking the allowed application methods. When application level authorization is enabled, trunk-level authorization occurs first, and application-level authorization occurs second. Unified CM checks the methods authorized for the trunk (in this security profile) before the methods authorized for the SIP application user in the Application User Configuration window.</p> <p>Tip: Consider using application-level authorization if you do not trust the identity of the application or if the application is not trusted on a particular trunk. Application requests may come from a different trunk than you expect. For more information about configuring application level authorization at the Application User Configuration window, see the “Cisco Unified Communications Manager Administration Guide”.</p>
Accept presence subscription (Optional)	<p>If you want Unified CM to accept presence subscription requests that come through the SIP trunk, select this check box.</p> <p>If you selected Enable Application Level Authorization, go to the Application User Configuration window and select Accept Presence Subscription for any application users authorized for this feature.</p> <p>When application-level authorization is enabled, if you select Accept Presence Subscription for the application user but not for the trunk, a 403 error message is sent to the SIP user agent connected to the trunk.</p>
Accept out-of-dialog refer (Optional)	<p>If you want Unified CM to accept incoming non-INVITE, Out-of-Dialog REFER requests that come through the SIP trunk, select this check box. If you selected Enable Application Level Authorization, go to the Application User Configuration window and select Accept out-of-dialog refer for any application users authorized for this method.</p> <p>Note: If this profile is associated with an EMCC SIP trunk, Accept Out-of-Dialog REFER is enabled regardless of the setting on this page.</p>
Accept unsolicited notification (Optional)	<p>If you want Unified CM to accept incoming non-INVITE, unsolicited notification messages that come through the SIP trunk, select this check box.</p> <p>If you selected Enable Application Level Authorization, go to the Application User Configuration window and select Accept Unsolicited Notification for any application users authorized for this method.</p>

Option	Description
Accept replaces header (Optional)	If you want Unified CM to accept new SIP dialogs, which have replaced existing SIP dialogs, select this check box. If you selected Enable Application Level Authorization , go to the Application User Configuration window and select Accept Header Replacement for any application users authorized for this method.
Transmit security status (Optional)	If you want Unified CM to send the security icon status of a call from the associated SIP trunk to the SIP peer, select this check box. Default = Cleared.
Allow charging header (Optional)	If you want to allow RFC 3455 SIP charging headers in transactions (for example, where billing information is passed in the headers for prepaid accounts), select this check box. If the check box is clear, RFC 3455 SIP charging headers are not allowed in sessions that use the SIP profile. Default = Cleared .
SIP V.150 Outbound SDP Offer Filtering (Mandatory)	Choose one of the following filter options from the drop-down list: <ul style="list-style-type: none"> • Use Default Filter - The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System Service Parameters Clusterwide Parameters (Device-SIP) in Unified CM Administration. • No Filtering - The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • Remove MER V.150 - The SIP trunk removes V.150 MER SDP lines in outbound offers. Choose this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified CM. • Remove Pre-MER V.150 - The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Choose this option to reduce ambiguity when your cluster is in a network of MER-compliant devices that cannot process offers with pre-MER lines. Default = Use Default Filter .

4.24.2. SIP trunk security profile configuration

Tip: *Use the Action search to navigate Automate*

Option	Description
Name (Mandatory)	Enter a name for the security profile. When you save the new profile, the name displays in the SIP Trunk Security Profile drop-down list in the Trunk Configuration window. The maximum length for the name is 64 characters.
Description (Optional)	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Security Mode (Optional)	<p>From the drop-down list, choose one of the following options:</p> <ul style="list-style-type: none"> • Non Secure - No security features except image authentication apply. A TCP or UDP connection opens to Cisco Unified Communications Manager. • Authenticated - Unified CM provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • Encrypted - Unified CM provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling.
Incoming Transport Type (Optional)	<p>Choose one of:</p> <ul style="list-style-type: none"> • TCP+UDP • UDP • TLS • TCP <p>If you do not specify an incoming transport type, TCP+UDP is assigned. When Device Security Mode is Non Secure, TCP+UDP specifies the transport type.</p> <p>When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type.</p> <p>Note: The Transport Layer Security (TLS) protocol secures the connection between Unified CM and the trunk.</p>

Option	Description
Outgoing Transport Type (Optional)	<p>From the drop-down list, choose the outgoing transport mode. Choose one of:</p> <ul style="list-style-type: none">• TCP+UDP• UDP• TLS• TCP <p>When Device Security Mode is Non Secure, choose TCP or UDP. When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type.</p> <p>Note: TLS ensures signaling integrity, device authentication, and signaling encryption for SIP trunks.</p> <p>Tip: Use UDP as the outgoing transport type when connecting SIP trunks between Unified CM systems and IOS gateways that do not support TCP connection reuse. See “Understanding Session Initiation Protocol (SIP)” in the “Cisco Unified Communications Manager System Guide” for more information.</p>

Option	Description
Enable Digest Authentication (Optional)	<p>Select this check box to enable digest authentication. If you select this check box, Unified CM challenges all SIP requests from the trunk. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of Authenticated or Encrypted to use these features.</p> <p>Tip: Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.</p>
Nonce Validity Time (mins) (Optional)	<p>Enter the number of minutes (in seconds) that the nonce value is valid. When the time expires, Unified CM generates a new value.</p> <p>Note: A nonce value (a random number that supports digest authentication) is used to calculate the MD5 hash of the digest authentication password. Default = 600 minutes. If you do not specify a Nonce Validity Time, the default of 600 minutes is assigned.</p>
X.509 Subject Name (Optional)	<p>This field applies if you configured TLS for the incoming and outgoing transport type.</p> <p>For device authentication, enter the subject name of the X.509 certificate for the SIP trunk device. If you have a Unified CM cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts. This situation results in multiple X.509 subject names for the trunk. If multiple X.509 subject names exist, enter one of the following characters to separate the names: space, comma, semicolon, or a colon. You can enter up to 4096 characters in this field.</p> <p>Tip: The subject name corresponds to the source connection TLS certificate. Ensure that subject names are unique for each subject name and port. You cannot assign the same subject name and incoming port combination to different SIP trunks.</p> <p>Example: SIP TLS trunk1 on port 5061 has X.509 Subject Names my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has X.509 Subject Names my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have X.509 Subject Name my_ccm4 but cannot have X.509 Subject Name my_cm1.</p>

Option	Description
Incoming Port (Optional)	<p>Choose the incoming port. Enter a value that is a unique port number from 0 to 65535. The value that you enter applies to all SIP trunks that use the profile.</p> <p>The default port value for incoming TCP and UDP SIP messages is 5060. The default SIP secured port for incoming TLS messages is 5061. If the incoming port is not specified, the default port of 5060 is used.</p> <p>Tip:</p> <p>All SIP trunks that use TLS can share the same incoming port; all SIP trunks that use TCP + UDP can share the same incoming port. You cannot mix SIP TLS transport trunks with SIP non-TLS transport trunk types on the same port.</p>

Option	Description
Enable application level authorization (Optional)	<p>Application-level authorization applies to applications that are connected through the SIP trunk.</p> <p>If you select this check box, also select the Enable Digest Authentication check box and configure digest authentication for the trunk. Unified CM authenticates a SIP application user before checking the allowed application methods.</p> <p>When application level authorization is enabled, trunk-level authorization occurs first, and application-level authorization occurs second. Unified CM checks the methods authorized for the trunk (in this security profile) before the methods authorized for the SIP application user in the Application User Configuration window.</p> <p>Tip: Consider using application-level authorization if you do not trust the identity of the application or if the application is not trusted on a particular trunk. Application requests may come from a different trunk than you expect.</p> <p>For more information about configuring application level authorization at the Application User Configuration window, see the “Cisco Unified Communications Manager Administration Guide”.</p>
Accept presence subscription (Optional)	<p>If you want Unified CM to accept presence subscription requests that come through the SIP trunk, select this check box.</p> <p>If you selected Enable Application Level Authorization, go to the Application User Configuration window and select Accept Presence Subscription for any application users authorized for this feature.</p> <p>When application-level authorization is enabled, if you select Accept Presence Subscription for the application user but not for the trunk, a 403 error message is sent to the SIP user agent connected to the trunk.</p>
Accept out-of-dialog refer (Optional)	<p>If you want Unified CM to accept incoming non-INVITE, Out-of-Dialog REFER requests that come through the SIP trunk, select this check box. If you selected Enable Application Level Authorization, go to the Application User Configuration window and select Accept out-of-dialog refer for any application users authorized for this method.</p> <p>Note: If this profile is associated with an EMCC SIP trunk, Accept Out-of-Dialog REFER is enabled regardless of the setting on this page.</p>
Accept unsolicited notification (Optional)	<p>If you want Unified CM to accept incoming non-INVITE, unsolicited notification messages that come through the SIP trunk, select this check box.</p> <p>If you selected Enable Application Level Authorization, go to the Application User Configuration window and select Accept Unsolicited Notification for any application users authorized for this method.</p>

Option	Description
Accept replaces header (Optional)	If you want Unified CM to accept new SIP dialogs, which have replaced existing SIP dialogs, select this check box. If you selected Enable Application Level Authorization , go to the Application User Configuration window and select Accept Header Replacement for any application users authorized for this method.
Transmit security status (Optional)	If you want Unified CM to send the security icon status of a call from the associated SIP trunk to the SIP peer, select this check box. Default = Cleared.
Allow charging header (Optional)	If you want to allow RFC 3455 SIP charging headers in transactions (for example, where billing information is passed in the headers for prepaid accounts), select this check box. If the check box is clear, RFC 3455 SIP charging headers are not allowed in sessions that use the SIP profile. Default = Cleared .
SIP V.150 Outbound SDP Offer Filtering (Mandatory)	Choose one of the following filter options from the drop-down list: <ul style="list-style-type: none"> • Use Default Filter - The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System Service Parameters Clusterwide Parameters (Device-SIP) in Unified CM Administration. • No Filtering - The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • Remove MER V.150 - The SIP trunk removes V.150 MER SDP lines in outbound offers. Choose this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified CM. • Remove Pre-MER V.150 - The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Choose this option to reduce ambiguity when your cluster is in a network of MER-compliant devices that cannot process offers with pre-MER lines. Default = Use Default Filter .

4.25. Configure SIP trunks

4.25.1. SIP trunks

Tip: *Use the Action search to navigate Automate*

Overview

This section describes how to add, edit, and delete SIP trunks, and how to reset or restart SIP trunks.

Add and edit SIP trunks

This procedure adds new SIP trunks and edits existing SIP trunks.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where the Cisco Unified Communications Manager (UCM) is configured.
3. Go to **SIP Trunks**.
4. **Choose an option:**
 - **Add a new SIP trunk?** Click the Plus icon (+) to add a new record, then go to Step 5.
 - **Edit an existing SIP trunk?** Click on the relevant SIP trunk in the list of SIP trunks; then, go to step 6.
5. From the **CUCM** drop-down, select the hostname, domain name, or IP address of the CUCM where you're adding the SIP trunk.

Note: The **CUCM** drop-down displays only when you're adding a new SIP trunk (not when editing). This drop-down menu displays the CUCM located at the node, and all the CUCM nodes in the hierarchies above the node where you're adding the SIP trunk.

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

6. At **Device Name**, fill out a unique name for the new SIP trunk (or modify the existing device name, as applicable).
7. Complete at least the minimum, mandatory fields on the following tabs/panels:
 - *Device Information tab*
 - *Call Routing General tab*
 - *Call Routing Inbound tab*
 - *Call Routing Outbound tab*
 - *SP Info tab*
 - *GeoLocation tab*
8. Save your changes for the new or modified SIP trunk.

The SIP trunk appears in the SIP trunk list. The SIP trunk is automatically reset on the CUCM once it's added. To reset the SIP trunk at any other time, see "Reset SIP Trunk".

To view the SIP trunk and its properties, log in to the CUCM where you added the SIP trunk, select Device Trunk, and perform the "Find" operation. Clicking on the SIP trunk name in the list displays its characteristics.

Delete a SIP trunk

To delete a SIP trunk:

1. Log in as provider, reseller or customer administrator.
2. Choose an option, depending on your login profile:
 - Logged in as Provider or Reseller admin? Go to (CUCM) **SIP Trunks**.
 - Logged in as Customer admin? Go to (Advanced) **SIP Trunks**.
3. From the list of trunks, choose the SIP trunk to be deleted.
4. Click **Delete** to delete the SIP trunk.
5. Click **Yes** to confirm the deletion.

Reset a SIP trunk

This procedure shuts down a SIP trunk and brings it back into service.

Note: This procedure does not physically reset the hardware; it only re-initializes the configuration that is loaded by the UCM cluster. To restart a SIP trunk without shutting it down, use **Restart SIP Trunks**.

Perform these steps:

1. Log in as provider, reseller or customer administrator.
2. Choose an option, depending on your login profile:
 - Logged in as Provider or Reseller admin? Go to (CUCM) **SIP Trunks**.
 - Logged in as Customer admin? Go to (Advanced) **SIP Trunks**.
3. From the list of SIP trunks, click the SIP trunk to be reset, then choose **Action > Reset**.

Restart SIP trunks

This procedure restarts a SIP trunk without shutting it down first.

Note:

- To shut down a SIP trunk prior to the reset, see [Reset a SIP trunk](#).
 - If the SIP trunk is not registered with Cisco UCM, you cannot restart it.
-

Warning: Restarting a SIP trunk drops all active calls that are using the trunk.

Perform these steps:

1. Log in as provider, reseller or customer administrator.
2. Choose an option, depending on your login profile:
 - Logged in as Provider or Reseller admin: Go to (CUCM) **SIP Trunks**.
 - Logged in as Customer admin? Go to (Advanced) **SIP Trunks**.

3. From the list of trunks, click the SIP trunk to be restarted, then click **Action > Restart**.

SIP Trunks Configuration Settings

Device Information tab

Option	Description
Device Name *	Enter a unique identifier for the trunk using up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only. Default value: None
Trunk Service Type	Choose one of: <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 non-encrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. <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 re-originate on the MTP device. If you clear the check box, the Unified CM can decide whether calls are to go through the MTP device or be connected directly between the endpoints.</p> <p>Note:</p> <p>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:</p> <p>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	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you select this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format. If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8 bit format) and encodes in ISO8859-1 format. Default value: False (Cleared)
Unattended Port	Select this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. Default value: False (Cleared)
SRTP Allowed	Select this check box if you want Unified CM to allow secure and nonsecure media calls over the trunk. Selecting this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not select this check box, Unified CM prevents SRTP negotiation with the trunk and uses RTP negotiation instead. Caution: If you select this check box, we strongly recommend that you use an encrypted TLS profile, so that keys and other security related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP still works but the keys get exposed in signaling and traces. In that case, you must ensure the security of the network between Unified CM and the destination side of the trunk. Default value: False (Cleared)
Consider Traffic on This Trunk Secure	This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. From the drop-down menu, select one of: <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. Default value: When using both sRTP and TLS

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: 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 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 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: 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-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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p>
	<p>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:</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-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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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:</p> <p>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 - Out-bound	<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"> • 55XXXXX = 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	<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>
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: 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>

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.</p> <p>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 Method	Signaling	<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 scripter 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)

4.26. Configure SIP route patterns

4.26.1. SIP route patterns

Tip: *Use the Action search to navigate Automate*

Overview

provider

Cisco Unified Communications Manager (Cisco UCM) uses SIP route patterns to route or block both internal and external calls.

The domain name or IP address provides the basis for routing. The administrator can add domains, IP addresses, and IP network (subnet) addresses and associate them to SIP trunks (only). This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

Configure SIP route patterns

This procedure configures a SIP route pattern.

Prerequisites

- Configure at least one SIP Profile and SIP trunk before configuring a SIP route pattern.

Perform these steps

1. Log in as Provider, Reseller, or Customer administrator.
2. Ensure that the hierarchy path is set to a customer or site level.

3. If prompted, choose the NDL that contains the UCM which you are configuring the SIP Route Pattern.
4. Go to **SIP Route Patterns**.
5. Click **Add**.
6. Configure settings on the tabs/panels on this page:
 - [Pattern Definition Tab](#)
 - [Calling Party Transformations Tab](#)
 - [Connected Party Transformations Tab](#)
7. Click **Save**.

SIP Route Patterns settings

Pattern Definition Tab

Field	Description
Pattern Usage	From the drop-down list, choose either Domain Routing or IP Address Routing . This field is mandatory.
IPv4 Pattern	<p>Enter the domain, subdomain, IPv4 address, or IP subnetwork address. This field is mandatory.</p> <p>For Domain Routing pattern usage, enter a domain name IPv4 Pattern field that can resolve to an IPv4 address. The domain name can contain the following characters: -, ., 0-9, A-Z, a-z, *,], and [.</p> <p>For IP Address Routing pattern usage, enter an IPv4 address with the format X.X.X.X, where X represents a number between 0 and 255.</p> <p>For the IP subnetwork address, in classless interdomain routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix that denotes the number of bits in the network address.</p> <p>Tip: If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.</p>
IPv6 Pattern	<p>UCM uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6.</p> <p>Tip: If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 pattern.</p>
Description	Enter a description of the SIP Route Pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Route Partition	If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, leave the Route Partition value empty.
SIP Trunk/Route List	Choose the SIP trunk or route list to which the SIP route pattern is associated. This field is mandatory.
Block Pattern	Select this check box if you want this pattern to be used for blocking calls.

Calling Party Transformations Tab

Field	Description
Use Calling Party's External Phone Mask	Select On if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. Select Default to use the default External Phone Number Mask. This field is mandatory.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 to 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not selected, no calling party transformation takes place.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 to 9 and the wildcard characters asterisk (*) and octothorpe (#). Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Line ID Presentation	Calling line ID presentation (CLIP/CLIR) is a supplementary service that allows or restricts the originating caller phone number on a call-by-call basis. Choose whether you want to allow or restrict the display of the calling party phone number on the called party phone display for this SIP route pattern. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want to allow the display of the calling number. Choose Restricted if you want to block the display of the calling number.
Calling Line Name Presentation	Calling line name presentation (CNIP/CNIR) is a supplementary service that allows or restricts the originating caller name on a call-by-call basis. Choose whether you want to allow or restrict the display of the calling party name on the called party phone display for this SIP route pattern. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want to allow the display of the caller name. Choose Restricted if you want to block the display of the caller name.

Connected Party Transformations Tab

Field	Description
Connected Line ID Presentation	<p>Connected line ID presentation (COLP/COLR) is a supplementary service that allows or restricts the called party phone number on a call-by-call basis. Choose whether you want to allow or restrict the display of the connected party phone number on the calling party phone display for this SIP route pattern. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party phone number. Choose Restricted if you want to block the display of the connected party phone number.</p> <p>If a call originating from an IP phone on UCM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed.</p>
Connected Line Name Presentation	<p>Connected name presentation (CONP/CONR) is a supplementary service that allows or restricts the called party name on a call-by-call basis. Choose whether you want to allow or restrict the display of the connected party name on the calling party phone display for this SIP route pattern. Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want to display the connected party name. Choose Restricted if you want to block the display of the connected party name.</p>

4.27. Configure route groups

4.27.1. Route groups

Tip: *Use the Action search to navigate Automate*

Overview

A route group allows you to define the order in which gateways are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

For example, if you use two long distance carriers, you could add a route group so that long distance calls to the less expensive carrier are given priority. Calls only route to the more expensive carrier if the first trunk is unavailable.

Configure route groups

This procedure adds or updates route groups.

Prerequisites:

- You must define one or more gateway or SIP trunks before you add a route group.

Note: Each gateway or gateway and port combination can only belong to one route group and can only be listed once within that route group. All gateways in a route group must have the same route pattern. The pattern is assigned to the route list containing the route group (not the route group itself).

Route groups are optional. If a proposed route group only contains one gateway or one gateway and port combination and that route group is not to be included in a route list, the route group is not needed.

Perform these steps:

- Log in as Provider, Reseller or Customer administrator.
- Go to (Cisco UCM) **Route Groups**.
- Choose an option:**
 - Add new route group?** Click **Add**. Go to step 4.
 - Edit an existing route group?** Click the group to be updated, edit the fields as required, then click **Save** to save the edited route group.
- In the **CUCM** drop-down, select the Cisco Unified Communications Manager corresponding to the route group.
- 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.

- Select Distribution Algorithm options for the route group. The default value is Circular.

Option	Description
Top Down	Allows UCM to distribute a call to idle or available members starting with the first idle or available member of a route group to the last idle or available member of a route group. This option is mandatory if you want to prioritize the order of devices.
Circular	Allows UCM to Communications Manager to distribute a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which the UCM most recently extended a call. If the nth member is the last member of a route group, UCM distributes a call starting from the top of the route group.

- Click the Plus icon (+) to open the **Members** box.

8. Choose an option:

- Add a device to the route group? Go to Step 9.
- Modify the priority of a device? Go to Step 10.
- Remove a device from the route group? Select the relevant device, and click the Minus sign (-). Ensure you leave at least one device in the route group.

8. To add a device to the route group:

- a. From the **Device Name** drop-down menu, choose the device where the route group is added.

Note: When adding a SIP trunk or gateway, all ports on the device are selected.

- b. For Device Selection Order, indicate the order in which to prioritize multiple devices. A lower selection order indicates higher priority. This field requires an integer value. The default is no setting. The device selection order, if specified, overrides the position of the device in the list.
 - c. To add another device to the route group, click the Plus icon (+) at **Members**, then repeat this step for each device you want to add.
10. If no device selection order is specified, you can change the priority of a device by moving the device up or down in the list by clicking the arrows on the right side of the **Members** box. Using the Up arrow, move the device higher in the list to make it a higher priority in the route group, or using the Down arrow, move the device lower in the list to make it a lower priority in the route group.

Note: The Top Down distribution algorithm must be selected in Step 6 to prioritize the order of devices.

11. Click **Save**. The new route group displays **Route Group** list.

Delete a route group

To delete a route group:

1. Log in as Provider, Reseller or Customer administrator.

Warning: When deleting a route group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to delete a route group at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

2. Go to **Route Groups**.
3. From the list of trunks, select the route group you wish to delete.
4. Click **Delete**, then click **Yes** to confirm.

4.28. Configure route lists

4.28.1. Route lists

Tip: *Use the Action search to navigate Automate*

Overview

Route lists are made up of route groups and are associated with route patterns. A route list associates a set of route groups with a route pattern and determines the order in which those route groups are accessed. The order controls the progress of the search for available trunk devices for outgoing calls.

A route list can contain only route groups. Each route list should have at least one route group. Each route group includes at least one device, such as a gateway, that is available. Based on device type, Cisco Unified Communications Manager (Cisco UCM) can choose some, or all, ports as resources in each route group. Some devices, such as digital access, only allow you to choose all ports.

You can add a route group to any number of route lists.

Configure route groups

This procedure adds route lists and adds, removes, or changes the order of route groups in a route list.

Pre-requisites:

- Configure the route groups.

Perform these steps:

1. Log in to as Provider, Reseller or Customer administrator.

Note: When configuring a route list as a provider or reseller, ensure that you select a valid customer or site under your customer in the hierarchy node breadcrumb at the top of the view.

2. Go to **Route Lists**.
3. **Choose an appropriate option:**
 - **Add a new route list?** Click the Plus icon (+) to add a new record, then go to Step 4.
 - **Edit an existing route list?** Choose the list to be updated by clicking on its box in the leftmost column, then click **Edit** to update the selected route list. Go to Step 5.
4. Complete at minimum, the mandatory *Route lists configuration*.
5. To add a route group to this route list, click + on the right side of the **Route Group Items** box and complete at minimum, the mandatory *Route Group settings*.
6. To remove a route group from this route list, click - on the right side of its row in the **Member** box.
7. To change the priority of a route group, move it up or down in the list by clicking the arrows on the right side of the **Member** box. Using the Up arrow, move the group higher in the list to make it a higher priority, or using the Down arrow, move the group lower in the list to make it a lower priority.

8. To save a new or updated route list, click **Save**.

Route lists configuration

Field	Description
CUCM *	Select a Cisco UCM for the route list. Mandatory.
Name *	<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 Cisco UCM 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 UCM in the group (which is the Primary UCM).</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 settings

Field	Description
Route Group *	Choose the route group. This field is mandatory.
Selection Order	Indicate the order in which to prioritize multiple routes. A lower selection order indicates higher priority. This field requires an integer value. The default is no setting.
Use Calling Party's External Phone Number Mask *	Choose On from the drop-down list if you want the full external phone number to be used for calling line identification (CLID) on outgoing calls. Choose Off or Default if you do not want to use the full external phone number for CLID on outgoing calls. You may also configure an External Phone Number Mask on all phone devices. This field is mandatory.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the Digit Discards field is blank, the Prefix Digits field is blank, the Calling Party Transformation Mask field is blank, and Use Calling Party's External Phone Number Mask is set to Off or Default , no calling party transformation takes place.
Calling Party Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Party Number Type	Choose the format for the number type in calling party directory numbers. Cisco UCM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non national type numbering plan. Choose one of the following options: <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco UCM sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialling a user by using a shortened user number.

Field	Description
Calling Party Numbering Plan	<p>Choose the format for the numbering plan in calling party directory numbers. Cisco UCM sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco UCM sets the numbering plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.
Called Party Discard Digits	Choose the discard digit instructions that you want to be associated with this called party transformation pattern.
Called Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Called Party Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character +, and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Called Party Number Type	<p>Choose the format for the number type in called party directory numbers. Cisco UCM sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco UCM sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user by using a shortened user number.

Field	Description
Called Party Numbering Plan	<p>Choose the format for the numbering plan in called party directory numbers. Cisco UCM sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco UCM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco UCM sets the numbering plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

4.29. Configure date time groups

4.29.1. Date time groups

Tip: *Use the Action search to navigate Automate*

Overview

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

UCM automatically configures a default Date Time Group, called `CMLocal`, which syncs to the active date and time of the operating system on the server where UCM is installed. You can change the settings for `CMLocal`, as required. Normally, adjust server Date and Time to the local time zone date and time.

Tip: For a worldwide distribution of Cisco Unified IP phones, create one named Date Time Group for each of the time zones in which you deploy endpoints.

Add date time groups

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to a customer or site level.
3. If prompted, select the NDL that contains the Cisco Unified CM on which you are configuring the Date Time Group.
4. Go to **Date Time Groups**.
5. Click the Plus icon (+) to add a new record, then, provide configuration details:

Field	Description
Group Name	Enter the name that you want to assign to the new Date Time Group. This field is mandatory.
Time Zone	Choose the time zone for the group that you are adding. This field is mandatory.
Separator	Choose the separator character to use between the date fields. This field is mandatory.
Date Format	Choose the date format for the date that displays on the Cisco Unified IP Phones. This field is mandatory.
Time Format	Choose a 12-hour or 24-hour time format. This field is mandatory.
Selected Phone NTP References	To ensure that a phone that is running SIP gets its date and time configuration from an NTP server, select the phone NTP references for the Date Time Group.

6. Click **Save**.

4.30. Configure locations

4.30.1. Locations

Tip: *Use the Action search to navigate Automate*

Overview

Locations are used to implement call admission control in a centralized call-processing system. Call admission control enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between the locations.

Important: Locations are different to sites. Locations are used by CUCM to manage call admission control. Sites are used by VOSS Automate to logically group resources.

Add locations on CUCM

This procedure adds CUCM locations.

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to a customer or site level.
3. If prompted, select the NDL that contains the CUCM on which you are configuring the location.
4. Choose an option:
 - Logged in as Provider or Reseller admin? Go to (CUCM) **Locations**.
 - Logged in as Customer admin? Go to (Advanced) **Locations**.
5. Click the Plus icon (+) to add a new record.
6. On the **Location Information** tab, fill out the name of the location.
7. Select the **Intra-Location** tab, and complete at minimum, the mandatory *Intra-Location settings*.
8. Select the **Between Locations** tab, and complete at minimum, the mandatory *Between Locations settings*.
9. Select the **RSVP Settings** tab, and complete at minimum, the mandatory *RSVP Settings*.
10. Click **Save**.

Intra-Location settings

Field	Description
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Valid values are 0 to 2147483647, where 0 means unlimited bandwidth. This field is mandatory. Note: To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on this link.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Valid values are 1 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 settings

Field	Description
Location	Select a location from the list. This field is mandatory.
Weight	Enter the relative priority of this link in forming the Effective Path between any pair of Locations. The Effective Path has the least cumulative Weight of all possible paths. Valid values are 0-100. This field is mandatory.
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Valid values are 0 to 2147483647, where 0 means unlimited bandwidth. You can also select Unlimited Bandwidth. This field is mandatory.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. You can also select Unlimited Bandwidth or None. Setting the value to None means you cannot make video calls between this location and other locations. This field is mandatory.
Immersive Video Bandwidth	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link between this location and other locations. For video calls, the immersive video bandwidth does not include overhead. Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. You can also select Unlimited Bandwidth or None . Setting the value to None means you cannot make immersive video calls between this location and other locations. This field is mandatory.

RSVP Settings

Field	Description
Location	To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane. This field is mandatory.
RSVP Setting	<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.

4.31. Configure device pools

4.31.1. Device pools

Tip: *Use the Action search to navigate Automate*

Overview

Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains system, device, and location-related information.

After adding a new device pool, you can use it to configure devices, such as Cisco Unified IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, and CTI route points.

Add or manage device pools

1. Log in to the Admin Portal as Provider, Reseller, or Customer administrator.
2. Go to **Device Pools**.
3. Choose an option:

Add new device pool

- Click **Add**.
- Choose the network device list (NDL) where you want to add the new device pool.

Note: You won't need to choose a NDL if you're adding the device pool at a site. In this case, you will use the NDL associated with the site.

- Click **OK**.
- On the **Device Pool Settings** tab, at **Device Pool Name**, fill out the device pool name as **RSMSimPhone_DP**.
- From the **Cisco Unified CM Group** drop-down, choose **RSMSimPhone**.
- On the **Roaming Sensitive Settings** tab, from the **Date/Time Group** drop-down, choose the appropriate date/time group.
- From the **Region** drop-down, choose **AR_RSMSimPhone**.
- From the **SRST Reference** drop-down, choose **Disable**.

Edit a device pool

- Click on the relevant device pool in the list.
- Go to step 4.

Delete a device pool

- In the list view, select the checkbox adjacent to the **Name** column for the device pool you want to remove.
- Click **Delete**.

4. To configure or update device pool properties, click through the tabs on the page and fill out at least the mandatory fields:
 - Device Pool Settings tab
 - Local Route Group Settings tab
 - Roaming Sensitive Settings tab
 - Device Mobility Related Information tab
 - Geolocation Configuration** tab
 - Incoming Calling Party Settings tab

- Incoming Called Party Settings tab
- Caller ID for Calls from This Phone tab
- Connected Party Settings tab
- Redirecting Party Settings tab

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

Associate a local route group to a device pool

This procedure associates a local route group with an existing device pool for each site.

This allows calls from a device that is tied to a device pool to go out on a specific route group based on the call type. For example, you can associate multiple local route groups such as Emergency Route Group, Primary Local Route Group (for site A), Secondary Local Route Group (for site A), Primary Local Route Group (for site B), and Secondary Local Route Group (for site B).

Local Route groups allow you to specify different route groups for each site (site A and site B) for the respective device pool. Also, you can define a separate call routing option for emergency calls when you associate the Emergency Route Group with a different route group. Hence you can easily define separate call routing options for emergency calls and PSTN calls.

1. Log in as Provider, Reseller, or Customer administrator.

Warning: When associating a local route group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to associate a local route group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.

2. Go to **Device Pools**.
3. Click the device pool to be associated.
4. From the **Cisco Unified CM Group** drop-down menu, select a specific Cisco Unified Communications Manager group or leave the Cisco Unified CM Group as Default.
5. Configure setting in the **Local Route Group Settings** tab/panel:
 - a. In the grid, from the **Local Route Group** drop-down menu, select the local route group.
 - b. In the grid, from the **Route Group** drop-down menu, select the route group or gateway.
6. Save the new local route association.

Device pools configuration settings

Device Pool Settings

The table describes the device pool settings and values on the Device Pool Settings tab/panel:

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

The table describes the device pool settings and values on the Local Route Group Settings tab/panel:

Option	Description
Local Route Group	From the drop-down, choose the name of the local route group to associate with this device pool.
Route Group	From the drop-down, choose the value for the local route group to associate with this device pool.

Roaming Sensitive Settings

The table describes the device pool settings and values on the Roaming Sensitive Settings tab/panel:

Option	Description
Date/Time Group *	Choose the date/time group to assign to devices in this device pool. The date/time group specifies the time zone and the display formats for date and time. Default value: None
Region *	Choose the Unified CM region to assign to devices in this device pool. The Unified CM region settings specify voice codec that can be used for calls within a region and between other regions. Default value: None
Media Resource Group List	From the drop-down list, choose a media resource group list. A media resource group list specifies a prioritized list of media resource groups. An application selects the required media resource (for example, a music on hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order defined in a media resource group list. Default value: None
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability. It works by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list, choose the appropriate location for this device pool. A location setting of None or Hub_None means that the locations feature does not track the bandwidth that the devices in this pool consume. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. Default value: None
Network Locale	From the drop-down list, choose the locale that is associated with phones and gateways. The network locale contains a definition of the tones and cadences that the phones and gateways in the device pool in a specific geographic area use. Make sure that you select a network locale that all of the phones and gateways that use this device pool can support. Note: If the user does not choose a network locale, the locale that is specified in the Unified CM clusterwide parameters as Default Network Locale applies. Note: Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. When a device is associated with a network locale that it does not support in the firmware, the device fails to come up. Default value: None

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 un-registers from SRST and re-registers 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

The table describes the device pool settings and values on the Device Mobility Related Information tab/panel:

Option	Description
Device Mobility Calling Search Space	Choose the appropriate calling search space to be used as the device calling search space when the device is roaming and in the same device mobility group. Default value: None
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. Default value: None
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls is attempted. Default value: None
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool. Tip: Before the call occurs, the device must apply the transformation by using digit analysis. Note: If you configure the Calling Party Transformation CSS as None for the device pool and you select the Use Device Pool Calling Party Transformation CSS check box in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing. Default value: None
Called Party Transformation CSS	This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. Note: If you configure the Called Party Transformation CSS as None , the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing. Default value: None

Geolocation Configuration

The table describes the device pool settings and values on the Geolocation Configuration tab/panel:

Option	Description
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that the devices in this device pool do not associate with a geolocation. Default value: None
Geolocation Filter	From the drop-down list, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for the devices in this device pool. Default value: None

Incoming Calling Party Settings

The table describes the device pool settings and values on the Incoming Calling Party Settings tab/panel:

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	UCM applies the prefix that you enter in this field to calling party numbers that use User for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word "Default" displays in the Prefix field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
Subscriber Strip Digits	Enter the number of digits, up to the number 24, that you want UCM to strip from the calling party number of user type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to globalize the calling party number of User calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None , the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Incoming Called Party Settings

The table describes the device pool settings and values on the Incoming Called Party Settings Configuration tab/panel:

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:</p> <p>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:</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>
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>UCM applies the prefix that you enter in this field to called numbers that use User for the Called Party Numbering Type. You can enter up to sixteen characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word "Default" instead of entering a prefix.</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>
Subscriber Strip Digits	Enter the number of digits, that you want UCM to strip from the called party number of user type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to transform the called party number of user called party number type on the device. If you choose None , no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Caller ID For Calls From This Phone

The table describes the device pool settings and values on the Caller ID For Calls From This Phone tab/panel:

Option	Description
Calling Party Transformation CSS	From the drop-down list, choose the CSS that contains the Calling Party Transformation Pattern that you want to apply to devices in this device pool. When UCM receives a call from a device in this device pool on an inbound line, UCM immediately applies the calling party transformation patterns in this CSS to the digits in the calling party number before it routes the call. This setting allows you to apply digit transformations to the calling party number before UCM routes the call. For example, a transformation pattern can change a phone extension to appear as an E.164 number.

Connected Party Settings

The table describes the device pool settings and values on the Connected Party Settings tab/panel:

Option	Description
Connected Party Transformation CSS	<p>This setting is applicable for inbound calls only. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. UCM includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages for SIP calls and in the Connected Number Information Element of CONNECT and NOTIFY messages for H.323 and MGCP calls. Make sure that the Connected Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool.</p> <p>Note:</p> <p>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>

Redirecting Party Settings

The table describes the device pool settings and values on the Redirecting Party Settings tab/panel:

Option	Description
Redirecting Party Transformation CSS	<p>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.</p> <p>Note:</p> <p>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.</p>

4.32. Configure Cisco UCM groups

4.32.1. Call Manager Groups

Tip: *Use the Action search to navigate Automate*

Overview

A Call Manager Group (Cisco UCM group), contains a list of up to three UCM servers (users). These servers are prioritized. The server marked with the lowest number (zero) serves as the primary UCM user for that group, and the other members of the group serve as secondary and tertiary (backup) UCMs.

Each device pool has one UCM group that is assigned to it. When a device registers, it attempts to connect to the primary UCM user in the group assigned to its device pool. If the primary UCM is unavailable, the device tries to connect to the next UCM listed in the group, and so on.

A single UCM user is usually assigned as primary for one UCM group, and as secondary / tertiary (if applicable) on other UCM groups.

The table describes the value of UCM groups for your system:

Benefit	Description
Redundancy	This feature enables you to designate a primary and backup UCM user servers for each group.
Call processing load balancing	This feature enables you to distribute the control of devices across multiple UCM users.

For systems with a UCM that includes multiple servers (users), you are likely to achieve better load distribution and redundancy.

Manage Call Manager Groups

This procedure adds a new UCM group, and edits and deletes an existing UCM group.

Prerequisites:

- Configure all UCM servers (users) that you want to assign as members of the Call Manager group.

Note: After configuring the Call Manager group, you can use it to configure device pools. Devices obtain their UCM group list setting from the device pool to which they are assigned.

Perform these steps:

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.

Note: For Shared Architecture deployment, ensure you sign in only as either Provider or Reseller admin as only these admins can add UCMs.

2. If you are adding a new instance, ensure the hierarchy path is set to the target node for the new instance.
3. Go to **Call Manager Groups**.
4. Choose an option:
 - To add a new UCM group, click the Plus icon (+), then go to step 5.
 - To edit an existing UCM group, click on the relevant option in the list to open its settings, then go to step 5.
5. Configure the UCM group:

Field	Description
Name (Mandatory)	Fill out the UCM group name.
Auto-registration Cisco Unified Communications Manager Group	<p>Select this checkbox if you want this UCM group to be the default UCM group when auto-registration is enabled. Leave unchecked (disabled) if you don't want devices to auto-register with this UCM group.</p> <p>Tip</p> <p>Each UCM cluster can have only one default auto-registration group. If you choose a different UCM group as the default auto-registration group, that is, you select the Auto-registration Cisco Unified Unified Communications Manager Group* checkbox for a different UCM group, the previously chosen auto-registration group no longer serves as the default for the cluster; the Auto-registration Cisco Unified Communications Manager* checkbox displays for the previously chosen group (the original default), and the checkbox gets disabled for the group that now serves as the default.</p>
Unified CM Group Items (Mandatory)	<p>Click the Plus icon (+) to add a UCM to the group. Repeat to add multiple UCM's to the group.</p> <p>You can delete UCMs added to to the Call Manager (UCM) group or re-order UCMs in the group.</p>
Priority (Mandatory)	Enter the priority number for this UCM in the group. The smaller the integer, the higher the priority.
Selected Cisco Unified Communications Managers	This field displays the UCMs in the Cisco UCM group.

6. Click **Save**.

New UCM groups now appear in the list view of Call Manager Groups. You can delete Call Manager Groups from the list if required.

Note: To verify that the UCM is deployed in Shared Mode:

- Go to UCM **Servers**.
- On the **Publisher** tab, verify that the Multi-Tenant field is set to *Shared*.

Related topics

- Cisco UCM group selection in the Core Feature Guide.
- Set up Cisco UCM servers in the Core Feature Guide.

4.33. Configure route partitions

4.33.1. Route partitions

Tip: *Use the Action search to navigate Automate*

Overview

A partition contains a list of route patterns (directory number (DN) and route patterns). Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.

Tip: Use concise and descriptive names for your partitions. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

Configure route partitions

If you're updating a partition, use the **Apply Config** button (as described in this procedure) to synchronize a partition with affected devices. When you apply the configuration to devices that are associated with the partition, all calls on affected gateways drop.

1. Log in as the Provider, Reseller, or Customer administrator.
2. Go to **Route Partitions**.
3. Choose the relevant hierarchy.
4. Choose an option:
 - To add a new route partition, click **Add**, then go to step 5.
 - To edit an existing route partition, click the line item in the table. Go to step 6.
5. In the pop-up, select from the drop-down the network device list (NDL) to which you are adding the route partition, and click **OK**.

Note: The NDL pop-up only appears when you are adding a new route partition. If you are updating an existing partition, go to step 6.

If you are adding the partition to a site hierarchy node, the NDL pop-up will not appear. You will go right to the route partitions add page using the NDL associated to the site.

6. On the **Route Partitions** page, modify the following fields as required.

Option	Description
Name (Mandatory)	<p>Enter a name for the new partition that you are creating. Ensure that each partition name is unique to the route plan. Partition names can contain a-z, A-Z, and 0-9 characters, as well as spaces, hyphens (-), and underscore characters (_).</p> <p>Note:</p> <p>The length of the partition names limits the maximum number of partitions that can be added to a calling search space (CSS). The CSS partition limitations table provides examples of the maximum number of partitions that can be added to a CSS with partition names of fixed length.</p>
Description	<p>Enter a description of the new partition that you are creating. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), angle brackets (<>), or brackets ([]).</p> <p>If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.</p> <p>Default value: None</p>
Time Schedule	<p>From the drop-down list box, choose a time schedule to associate with this partition. The associated time schedule specifies when the partition is available to receive incoming calls.</p> <p>This field is empty by default, which indicates that time-of-day routing is not in effect and the partition remains active.</p> <p>With the time zone value in the following field, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks incoming calls to this partition against the specified time schedule.</p>
Time Zone	<p>Choose one of the following options to associate a partition with a time zone:</p> <ul style="list-style-type: none"> • Use Originating Device Time Zone: If you choose this option, the system checks the partition against the associated time schedule with the calling device's time zone. • Time Zone: If you choose this option, choose a time zone from the drop-down list box. The system checks the partition against the associated time schedule at the time that is specified in this time zone. <p>These options all specify the time zone. When an incoming call occurs, the current time on the Cisco Unified Communications Manager gets converted into the specific time zone set when one option is chosen. The system validates this specific time against the value in the Time Schedule field.</p>

The following table provides examples of the maximum number of partitions that can be added to a CSS if partition names are of fixed length.

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86
...	...
10 characters	46
15 characters	32

7. Click **Save**. The route partition appears in the route partition list.

- To modify any of these properties, click the item in the list, make your changes, and click **Save**.
- To delete a route partition, select the checkbox to the left of the Name column in the group list, and click **Delete**.

4.34. Configure calling search spaces

4.34.1. Calling search spaces

Tip: *Use the Action search to navigate Automate*

Overview

A Calling Search Space (CSS) comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

Add and edit calling search spaces

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Go to **Calling Search Spaces**.
3. Choose the relevant hierarchy.
4. Choose an option:
 - To add a new calling search space, click **Add**, then go to step 5.
 - To edit an existing calling search space, click on the line item in the table. Go to step 6.
5. In the popup, select from the pull-down the network device list (NDL) to which you are adding the calling search space, and click **OK**.

Note: The NDL popup will only appear when you are adding a new calling search space. If you are updating an existing calling search space, go to Step 6.

If you are adding the calling search space to a Site hierarchy node, the NDL popup will not appear. You will go right to the Calling Search Spaces add page using the NDL associated to the site.

6. From the **Calling Search Spaces** page, modify the following fields as required.

Option	Description
Name (Mandatory)	Enter a name in the field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each calling search space name is unique to the system. Note Use concise and descriptive names for your calling search spaces. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a calling search space. For example, CiscoDallasMetroCS identifies a calling search space for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas. Default value: None
Description	Enter a description in the field. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). Default value: None
Route Partitions	Click the Add (+) button to add a partition to the calling search space. Repeat as necessary to add multiple partitions to the calling search space.
Partition Name	Click the drop-down list and select a partition to add to the calling search space. Click Add (+) to add another partition to the Route Partitions list. Repeat as necessary to add multiple partitions to the list. Click the Remove (-) button to remove a partition from the list. Click the up and down arrow buttons to change the order of a partition in the list.
Partition Index	Enter the priority number for this partition in the calling search space. The smaller the integer, the higher the priority.

The following table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length.

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86
...	...
10 characters	46
15 characters	32

7. Click **Save**. The calling search space appears in the list.

- To modify any of these properties, click the item in the list, make your changes, and click **Save**.
- To delete a calling search space, check the box to the left of the Name column in the group list, and click **Delete**.

Note: When selecting an existing CSS with a partition associated and cloning this instance for modification, the new CSS will by default show the partition populated with this associated partition.

4.35. Configure calling party transformation patterns

4.35.1. Calling party transformation patterns

Tip: *Use the Action search to navigate Automate*

Overview

Parameters on the **Calling Party Transformation Patterns** page provide appropriate caller information using the Calling Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

You use calling party transformation patterns with the calling party normalization feature.

Configure calling party transformation patterns

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Go to **Calling Party Transformation Patterns**.
3. Set the hierarchy path to the relevant level.
4. Choose an option:
 - To add a new calling party transformation pattern, click **Add**, then go to step 5.
 - To edit an existing calling party transformation pattern, click on the line item in the table. Go to step 6.
5. In the popup, select from the drop-down the network device list (NDL) to which you are adding the calling party transformation pattern, and click **OK**.

Note: The NDL popup will only appear when you are adding a new calling party transformation pattern. If you are updating an existing pattern, go to Step 6.

If you are adding the calling party transformation pattern to a Site hierarchy node, the NDL popup will not appear. You will go right to the Calling Party Transformation Pattern add tabs using the NDL associated to the site.

6. From the **Pattern Definition** tab, modify the following fields as required.

Option	Description
Pattern (Mandatory)	<p>Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and +, which represents the international escape character +.</p> <p>Note</p> <p>Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report.</p> <p>Default value: None</p>
Partition	<p>If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box.</p> <p>Note</p> <p>Configure transformation patterns in different non-null partitions rather than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, Cisco Unified Communications Manager ignores the patterns in null partitions.</p> <p>Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</p>
Description	Enter a description of the transformation pattern.
Numbering Plan	Choose a numbering plan.
Route Filter	<p>If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.</p> <p>The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.</p>
MLPP Preemption Disabled	Check this box to make the numbers in a transformation pattern non-preemptable.

7. From the **Calling Party Transformations** tab, modify the following fields as required.

Option	Description
Use Calling Party's External Phone Number Mask	Choose On from the drop-down list if you want the full external phone number to be used for calling line identification (CLID) on outgoing calls. Choose Off or Default if you do not want to use the full external phone number for CLID on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
Digit Discards	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the Digit Discards field is blank, the Prefix Digits field is blank, the Calling Party Transformation Mask field is blank, and Use Calling Party's External Phone Number Mask is set to Off or Default, no calling party transformation takes place.
Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. Note The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this route pattern. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling number.

Option	Description
Calling Party Number Type	<p>Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non national type numbering plan. Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user by using a shortened user number.
Calling Party Numbering Plan	<p>Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

8. Click **Save**. The calling party transformation pattern appears in the list.

- If you need to modify any of these properties, click the item in the list, make your changes, and click **Save**.
- To delete a calling party transformation pattern, select the checkbox adjacent to the **Name** column in the group list, then click **Delete**.

4.36. Configure called party transformation patterns

4.36.1. Configure called party transformation patterns

Tip: *Use the Action search to navigate Automate*

Overview

Parameters on the **Called Party Transformation Patterns** page provide appropriate caller information by using the Called Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

Configure called party transformation patterns

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Go to **Called Party Transformation Patterns**.
3. Set the hierarchy path to the relevant level.
4. Choose an option:
 - **Add a new called party transformation pattern?** Click **Add**, then go to step 5.
 - **Edit an existing called party transformation pattern?** Click on the line item in the table. Go to step 6.
5. In the popup, select from the drop-down the network device list (NDL) to which you are adding the called party transformation pattern, and click **OK**.

Note: The NDL popup will only appear when you are adding a new called party transformation pattern. If you are updating an existing pattern, go to Step 6.

If you are adding the called party transformation pattern to a Site hierarchy node, the NDL popup will not appear. You will go right to the Called Party Transformation Pattern add tabs using the NDL associated to the site.

6. From the Pattern Definition tab, modify the following fields as required.

Option	Description
Pattern (Mandatory)	<p>Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. Valid characters include the uppercase letters A, B, C, and D and +, which represents the international escape character +.</p> <p>Note</p> <p>Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report.</p> <p>Default value: None</p>
Partition	<p>If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the transformation pattern, choose <None> for the partition.</p> <p>Note</p> <p>Transformation patterns should be configured in different non- NULL partitions than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, the patterns in NULL partitions get ignored.</p> <p>Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</p>
Description	Enter a description of the transformation pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Numbering Plan	Choose a numbering plan.
Route Filter	<p>If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.</p> <p>The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.</p>
MLPP Preemption Disabled	Check this box to make the numbers in a transformation pattern non-preemptable.

7. From the **Called Party Transformations** tab, modify the following fields as required.

Option	Description
Digit Discards	Choose the discard digit instructions that you want to be associated with this called party transformation pattern.
Called Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Prefix Digits	<p>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.</p> <p>Note The appended prefix digit does not affect which directory numbers route to the assigned device.</p>
Called Party Number Type	<p>Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a user, by using a shortened user number.

Option	Description
Called Party Numbering Plan	<p>Choose the format for the numbering plan in called party directory numbers.</p> <p>Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

8. Click **Save**. The called party transformation pattern appears in the list.

- To modify any of these properties, click the item in the list, make your changes, and click **Save**.
- To delete a called party transformation pattern, select the checkbox adjacent to the **Name** column in the group list, and click **Delete**.

4.37. Configure CTI route points

4.37.1. CTI route points

Tip: *Use the Action search to navigate Automate*

Overview

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

Add a CTI route point

This procedure adds a CTI route point.

1. Log in as Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the site for which you want to configure CTI route points.
3. Go to **CTI Route Points**.
4. Choose an option:
 - To view the details on an existing CTI route point, click an entry in the list view.

Home / CTI Route Points / CTIRP32323

Common Device Configuration	
Calling Search Space	
Location *	Cu1Si1-Location
User Locale	
Media Resource Group List	
Network Hold MOH Audio Source	
User Hold MOH Audio Source	
Use Trusted Relay Point Required Field *	Default
Calling Party Transformation CSS	
Geolocation	
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 settings](#).
 6. In the **Line** section, click the Plus icon (+) to associate a line with the CTI route point. Complete at least the mandatory fields. See [CTI route points line settings](#).
 7. Click **Save**.

CTI route points settings

Option	Description
Device Name *	Enter a unique identifier for this device, from 1 to 15 characters, including alphanumeric, dot, dash, or underscores. This field is mandatory.
Description	Enter a descriptive name for the CTI route point. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool *	Choose the name of a Device Pool. The device pool specifies the collection of properties for this device, including Cisco UCM group, Date Time Group, Region, and Calling Search Space for autoregistration. This field is mandatory.
Common Device Configuration	Choose the common device configuration to which you want this CTI route point assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure common device configurations in the Common Device Configuration window.
Calling Search Space	From the drop-down list, choose a calling search space. The calling search space specifies the collection of partitions that are searched to determine how a collected (originating) number is routed.
Location *	<p>From the drop-down list, choose the appropriate location for this CTI route point. This field is mandatory.</p> <p>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.</p> <p>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.</p>
User Locale	<p>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:</p> <p>If no user locale is specified, Cisco UCM uses the user locale that is associated with the device pool</p>
Media Resource Group List	<p>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.</p> <p>If you choose <none>, Cisco UCM uses the Media Resource Group that is defined in the device pool.</p>

Option	Description
Network Hold MOH Audio Source	Choose the audio source that plays when the network starts a hold action. If you do not choose an audio source, Cisco UCM uses the audio source that is defined in the device pool. If the device pool does not specify an audio source, the system default is used.
User Hold MOH Audio Source	Choose the audio source that plays when an application starts a hold action. If you do not choose an audio source, Cisco UCM uses the audio source that is defined in the device pool. If the device pool does not specify an audio source, the system default is used.
Use Trusted Relay Point Required Field *	<p>Enable or disable whether Cisco UCM inserts a trusted relay point (TRP) device with this media endpoint. This field is mandatory. Choose one of the following values:</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 settings

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	This field is the line position on the device. If left blank, an integer is automatically assigned.
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)	This field provides the same information as the Display (Internal Caller ID) field, but limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the ASCII Display (Internal Caller ID) field.
Ring Setting (Phone Active)	<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)	<p>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:</p> <ul style="list-style-type: none"> • Use system default • Disable • Flash only • Ring once • Ring
Recording Option	<p>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:</p> <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	<p>This field determines the recording media source option on the line appearance. Choose one of the following options:</p> <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	<p>Use this field to configure the handset lamp illumination policy. Choose one of the following options:</p> <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	<p>Use this field to configure an audible message waiting indicator policy. Choose one of the following options:</p> <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 UCM 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.

4.38. Configure time periods and schedules

4.38.1. Time periods

Tip: *Use the Action search to navigate Automate*

Overview

A time period specifies a time range that includes a start time and end time. Time periods also specify a repetition interval either as days of the week or a specified date on the yearly calendar. You define time periods and then associate the time periods with time schedules. A particular time period can be associated with multiple time schedules.

Note: Automate provides one **All the time** time period, which is a special, default time period that includes all days and hours, and cannot be deleted.

Configure time periods

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node where you wish to configure the new time period.
3. Go to **Time Periods**.
4. **Choose an option:**
 - **Add a new time period?** Click **Add**, then go to Step 5.

- **Edit an existing time period?** Select the time period to be updated by clicking it in the list of time periods, then go to Step 6.

- To add a new time period, if the **Network Device List** popup window appears, choose the NDL for the time period from the drop-down menu. The window appears when you are on a non-site hierarchy node. If you are at a site hierarchy node, the NDL associated with the site is automatically used.

Note: The **Network Device List** drop-down menu displays only when adding a time period; it does not display when editing a time period.

- When adding or editing a time period, add or update a unique name for the time period in the **Name** field. This field is mandatory. Enter a name in the **Time Period Name** field.

Note: Time period name can comprise up to 50 alphanumeric characters. It can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Use concise and descriptive names for your time periods. The hours_or_days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, *office_M_to_F* identifies a time period for the business hours of an office from Monday to Friday.

- 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.

- 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

- a. From the **Start Month** drop-down menu, choose a month of the year on which this time period starts.
 - b. Enter a number from 1 to 31 in the **Start Date** field to define the day of the month on which this time period starts.
 - c. From the **End Month** drop-down menu, choose a month of the year on which this time period ends.
 - d. Enter a number from 1 to 31 in the **End Date** field to define the day of the month on which this time period ends.
 - For weekly time intervals, choose a Start Day on Mon and End Day of Fri for a time period starting on Mondays and ending on Fridays.
 - For weekly time intervals, choose Start Day and End Day values of Sat to define a time period that applies only on Saturdays.
 - For yearly time intervals, choose Start Month value of Jan and Start Date of 15, and End values of Mar and 15 to choose the days from January 15 to March 15.
 - For yearly time intervals, choose Start and End values of Jan and 1 to specify January 1 as the only day during which this time period applies.
9. Click **Save** to save the new or updated time period.

Next steps: Associate time periods with time schedules. See “Configure Time Schedules”.

Note: You can't delete time periods if they're used by any time schedules. Before deleting a time period that is currently in use, perform either or both of these tasks as appropriate:

- Assign a different time period to any time schedule that is using the time period that you want to delete.
 - Delete the time schedules that are using the time period that you want to delete.
-

4.38.2. Time schedules

Tip: *Use the Action search to navigate Automate*

Overview

A time schedule includes a group of time periods. Time schedules are assigned to partitions to set up time-of-day call routing. Time schedules determine the partitions where calling devices search when they are attempting to complete a call during a particular time of day. Multiple time schedules can use a single time period.

Configure time schedules

This procedure assigns a time period to a time schedule.

Prerequisites:

- Configure a time period. You can only assign the time period to a time schedule after you have configured a time period.

Note: Automate provides one 'All the time' schedule. The 'All the time' schedule is a special, default time schedule that includes all days and hours, and cannot be deleted.

Perform these steps:

1. Log in to the Admin Portal as a Provider, Reseller, or Customer administrator.
2. Set the hierarchy path to the node where you want to create the new time schedule.
3. Go to **Time Schedules**.
4. **Choose an action:**
 - **Add a new time schedule?** Click the Plus icon (+) to add a new record, then go to Step 5.
 - **Edit an existing time schedule?** Select the time schedule to be updated by clicking it in the list of time schedules. Go to Step 6.
5. If the **Network Device List** popup displays, select the NDL for the time schedule from the drop-down. This dialog displays when you're on a non-site hierarchy. If you're at a site hierarchy, the NDL associated with the site is automatically used.

Note: The **Network Device List** drop-down displays only when you're adding a time schedule; it doesn't display when editing a time schedule.

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

Note: The name can comprise up to 50 alphanumeric characters. The name of the time schedule can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

7. (Optional) Enter a description for the time schedule in the **Description** field.
8. Click the Plus icon (+) to open the **Time Periods** form.
9. From the **Time Period** drop-down, choose a time period for the time schedule.
10. Repeat Steps 8 and 9 to add another time period to the time schedule.

Note:

- If multiple time periods are associated with a schedule where the time periods overlap, time periods with Day of Year settings take precedence over time periods with Day of Week settings. Day of Year is applicable when Year Start value is set and the End value is left blank.

Example: If a Time Period configured for January 1 is configured as No Office Hours and another time period is configured for the same day of the week (for example, Sunday to Saturday) as

08:00 to 17:00, the time period for January 1 is used. In this example, No Office Hours takes precedence.

- Time interval settings take precedence over No Office Hour settings for the same day of the year or day of the week.

Example: One time period specifies for Saturday as No Office Hours. Another time period specifies Saturday hours of 08:00 to 12:00. In this example, the resulting time interval specifies 08:00 to 12:00 for Saturday.

- If multiple time periods are associated with a schedule where the time periods overlap, time periods with Day of Week settings take precedence over time periods with Range of Days settings. Range of Days applies to when Year Start and End values are set, even if they are configured for the same day.

Example: If a Time Period configured for Day of Week (for example, Sunday to Saturday) is configured as No Office Hours and another time period is configured for January 1 until December 31 as 08:00 to 17:00, the time period for Day of Week is used. In this example, No Office Hours takes precedence.

11. To save the new time schedule, click **Save**, or to update time schedule, click **Update**.

12. Repeat Steps 3 to 11 to configure another time schedule.

Next steps

You can't delete time schedules that partitions are using. Before deleting a time schedule that is currently in use, perform either or both of the following tasks:

- Assign a different time schedule to any partitions that are using the time schedule that you want to delete.
- Delete the partitions that are using the time schedule that you want to delete.

Warning: Before deleting a time schedule, ensure that you're deleting the correct time schedule. You cannot retrieve deleted time schedules. If you accidentally delete a time schedule, you must rebuild it.

4.39. Clone a Cisco UCM device model

4.39.1. Clone an instance of a Cisco UCM device model

Tip: *Use the Action search to navigate Automate*

To save time, make a copy of an existing instance of a device model rather than adding a new one. To do this, use the clone operation. When you create a clone, give it a new unique name and modify other device model fields as needed before saving.

Note: You can clone an instance of a device model to the same Cisco UCM or to a different Cisco UCM.

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

Perform these steps:

1. Log in as provider, reseller, or customer administrator.
2. Go to **{device_model_type}**.
3. From the device model list, select the instance to be cloned.
4. Click **Action > Clone**.
5. Depending on the device model, do one of the following:
 - When prompted, choose the NDL that contains the target Cisco Unified CM.
 - choose the target UCM from the **CUCM** drop-down menu.
6. At the **Name** field, fill out a unique name for the new instance of the device model.
7. Modify other fields, as required.

For further details about these fields, see the corresponding topic on configuring a new instance of the device model. For example, if you are cloning a SIP trunk, see under [SIP trunks](#) for the SIP trunk field descriptions.

8. Click **Save** to save the cloned instance.

The new instance appears in the list. The new instance is created on the target UCM.

4.40. Load balancing

4.40.1. Introduction to load balancing

Cisco Unified Communications Manager (Cisco UCM) groups provide both call-processing redundancy and distributed call processing. You can distribute devices, device pools, and UCMs among the groups to improve redundancy and load balancing in your system.

A UCM group specifies a prioritized list of up to three UCMs. The first UCM in the list serves as the primary UCM for that group, and the other members of the group serve as secondary and tertiary (backup) UCMs.

Each device pool has one UCM group that is assigned to it. For example, Group 1 points to Device Pool 1, Group 2 points to Device Pool 2, and Group 3 points to Device Pool 3. When a device registers, it attempts to connect to the primary (first) UCM in the group that is assigned to its device pool. If the primary UCM is unavailable, the device tries to connect to the next UCM listed in the group, and so on.

Load balancing is a manual process on Cisco UCM, requiring you to perform the following tasks:

1. Add new, custom UCM groups and device pools.
2. Synchronize the groups and device pools into Automate.
3. Choose the appropriate group and device pool in the user management or phone configuration for the site. To create more than one configuration for a site, create at least two UCM groups, then associate a device pool to the appropriate UCM group.

To determine if load balancing is required for your network, you can check the current device traffic load in Cisco UCM, via System > Device Pool menu. When you click on the device configuration information for a specific device pool, the Device Pool Information field lists the number of members in the Device Pool. Compare different device pools to see if the members are evenly divided between pools.

To perform load balancing, see “Load Balancing Using Site Default Device Pool”.

4.40.2. Load balancing using site default device pool

Tip: *Use the Action search to navigate Automate*

This procedure load balances using the default site device pool and updates the default device pool to point to the appropriate Cisco Unified Communication Manager (Cisco UCM) group.

Note: A default device pool is created for each site when the site dial plan is deployed for the Type 1 through Type 4 dial plan schema groups.

Since you're using the default device pool, you don't need to create any additional device pools directly on CUCM. Using this configuration, redundancy is gained within a site while load balancing is gained across multiple sites. Since there is one device pool per site, all devices at a site home to the same sequence of CUCMs, providing failover redundancy. Devices in different sites home to different sequences of CUCMs, providing load balancing across the sites.

The default site device pool is not created until the Type 1 to 4 site dial plan has been deployed, which updates the Site Defaults to use the default device pool. If the site dial plan has not been deployed, you will not see a site default device pool in the form Cu<customerId>Si<siteId>-DevicePool.

In Automate you can determine the default device pool for a site in the site **Defaults** page.

Perform these steps:

1. Log in as Provider, Reseller, or Customer administrator.
2. Choose the relevant site.
3. Follow the steps outlined in *Create a Site Dial Plan* if you have not already done so; the Create a Site Dial Plan procedure creates the default site device pool instance.
4. Log in to Cisco Unified Communications Manager and create one or more UCM groups.

Note: See Cisco Unified Communications Manager Administration Guide.

5. In Automate, perform a sync operation of the UCM via the **Data Sync** page.

This sync updates the Automate cache and makes the UCM groups that were added directly on Cisco Unified Communications Manager available to Automate.

6. Associate a UCM group to a device pool and choose a UCM group other than the default group in the **Call Manager Group** drop-down list. See “Associate a CUCM Group to a Device Pool”.

Note: To verify that the phone or user uses the device pool as expected, open a user's settings in Automate, then select the required **Device Pool Name** setting from the drop-down under the **Phones** tab.

4.40.3. Associate a UCM group to a device pool

Tip: *Use the Action search to navigate Automate*

This procedure associates a Cisco UCM group with an existing device pool for each site.

This allows calls from a device that is tied to a device pool to go out on a specific UCM group based on the call type.

Note: You cannot use this procedure to add or delete device pools.

1. Log in as Provider, reseller or Customer administrator.

Warning: When associating a UCM group, ensure that you choose a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to associate a UCM group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.

2. Go to **Device Pools**.
3. Click the device pool to be associated.
4. From the **Unified CM Group** drop-down, choose a specific CUCM group or leave the **Unified CM Group** as **Default**.
5. Save the new UCM group association.

4.41. Update the USA device-based routing dial plan

4.41.1. Update the USA device-based routing dial plan

Tip: *Use the Action search to navigate Automate*

This procedure updates the United States country dial plan that was first deployed in an earlier version of Automate, if you're using device-based routing.

Update the calling search spaces (CSS) for each customer that uses the United States dial plan. Update one customer-level CSS and one site-level CSS for each USA site.

Note: Perform this procedure only once (the first time you upgrade Automate).

1. Log in to Cisco Unified Communications Manager (UCM).
2. Go to **Call Routing > Class of Control > Calling Search Space**.
3. Find the calling search space where the CSS Name ends with USADP-DBRDevice-CSS.

Note: Records for each of your USA sites appear in the following format: Cu<customerId>Si<siteId>-USADP-DBRDevice-CSS.

4. Edit each calling search space to include the pre-device-based route selection partition instead of the device-based route selection partition:
 - a. Remove the following partition: Cu<customerId>-USADP-DBRteSel-PT.
 - b. Add the following partition: Cu<customerId>-USADP-PreDBRteSel-PT.
 - c. Click **Save**.
5. Find the calling search space where the CSS Name ends with USADP-DBRteSel-CSS.

Note: Records for each of your USA sites appear in the following format: Cu<customerId>Si<siteId>-USADP-DBRteSel-CSS.

6. Edit this calling search space to include the device-based route selection partition instead of the line-based route selection partition:
 - a. Remove the following partition: Cu<customerId>-USADP-LBRteSel-PT.
 - b. Add the following partition: Cu<customerId>-USADP-DBRteSel-PT.
 - c. Click **Save**.
7. After updating all calling search spaces, log in to Automate and perform a CUCM import operation:
 - a. Log in to Automate as provider or customer administrator.
 - b. Go to **Perform Publisher Actions**.
 - c. Select Action Import, App Type CUCM Device and select the appropriate CUCM cluster.
 - d. Click **Save**.

4.42. Sharing lines across sites

4.42.1. Shared line across sites

Overview

The ability to have shared lines across sites allows lines to be shared across sites, and is accomplished by introducing the concept of an “inventory site”, in addition to “real sites”:

- The inventory site is used to provision the shared lines first
- Then the real sites make use of the shared lines by assigning them to phones

Devices are only provisioned on real sites (not in the inventory site).

The “shared lines” feature also supports *hunt groups* and *call pickup groups* across sites by leveraging the *inventory site* to provision all of the lines to be included in the hunt group or call pickup group.

Lines used in the hunt groups and call pickup groups that are provisioned in the inventory site can span multiple real sites; that is, they’re used by devices on the real sites. The key requirement is that all the lines

to be used by a given hunt group or call pickup group must be configured in the inventory site, along with the hunt group and call pickup group itself.

The “shared line across sites” deployment model is 100% backward compatible with the previous directory number (DN) and line configuration. Existing deployments are not impacted when the system is upgraded, and all existing dial plan configuration procedures are supported. The deployment configuration shown in [Example of shared line across sites](#) is optional and is only required when sharing lines across sites.

Tip: If a line is potentially shareable, it is recommended that you create the line in the inventory site, even if it won't be shared across sites immediately.

The system does not support the ability to move a line from a real site to an inventory site, so to convert a line from *site-local* to *cross-site shared*, the line would need to be deleted from the real site and recreated in the inventory site.

Note: See the Glossary for descriptions of the following terms related to *shared lines across sites* functionality:

- Directory Number (DN)
 - DN Inventory
 - E.164 Number
 - E.164 Inventory
 - Line / Line Relation
 - Line Appearance
 - Class of Service (CoS)
 - Directory Number Routing (DNR)
 - E.164 Associations
-

Limitations of shared lines across sites

When considering using shared lines across sites, consider the following limitations:

- A new inventory site is required for each new combination of network device list (NDL) and Country (a “site group”); that is, lines configured at the inventory site are specific to the NDL and Country defined for that site.
- All real sites that reference lines in an inventory site must be defined with the same NDL and Country. Ensure that this requirement is met, as it is not enforced in Automate.
- Shared lines can't span countries or NDLs. This is necessary because Cisco UCM doesn't support shared lines across clusters. The country must be consistent so that line CoSs (defined in the inventory site) are correct for each device referencing the line (defined in the real site). Ensure that the correct association is made between inventory sites and real sites, as it is not enforced in Automate.
- When configuring a phone or user at a real site, any reference to a DN that does not exist in the inventory site results in a new line being created at the real site as it did prior to this Cisco HCS release. If the inventory site doesn't exist, or a line hasn't been configured in the inventory site first, the system behaves as it did in previous Cisco HCS releases (backwards compatible).

- If a line can be potentially shared, create it in the inventory site before referencing it by any devices. If the DN is used in a device before it's configured in the inventory site, the line is created in the real site and may not have the desired CoS or other configuration desired for a shared line.
- When a line has been created (either at the inventory site or a real site), it can't be moved. To move the line, delete it and re-add it. For example, if you forget to define the line at the inventory site first and configure a device with a line, the line is created at the real site. You would need to delete the line from the real site and add it to the inventory site, then reassign it to the phone.
- A site admin logged in to a real site is not able to see the line configuration that exists at the inventory site. A custom admin (or above) can view the line configuration at all of the sites.
- The "shared lines across sites" functionality only works when using a *flat* dial plan since other dial plans have site location codes in the DN that won't make sense if the DN is shared by multiple sites. The default Automate template bundle includes a *Type 4 flat dial plan*. Other, non-site-specific custom dial plans can be used.
- Self-provisioning does not work for DNs defined at the customer level.
- Although an admin can delete inventory sites, this is not recommended. If an inventory site is deleted, all hunt groups, call pickup groups, voicemail pilot associations, and lines that are part of the inventory site are deleted. If there are devices on the "real" sites that reference these lines, they will no longer reference these lines as they will have been deleted. The customer-level DN inventory is still intact, though no lines are associated with these DNs because they are deleted when the inventory site is deleted. The hunt groups and call pickup groups are self-contained to the inventory site and are therefore deleted as part of the deletion of the inventory site.
- When the inventory site is deleted, this deletes all shared lines, Classes of Service, DNR, and any other configuration added at that site. The shared lines are removed from all devices on "real" sites that may have referenced them.
- If an emergency number is dialed from any shared line, the number displayed on the other end should be the Emergency Call Back Number of the corresponding site.

Example of shared line across sites

Phones are always configured on *real sites*, and can use both shared and *site-local* lines. For example, each phone can have one *site-local* line (for example, 1000), and one *cross-site shared* line (for example, 9000). The following is a summary of the configuration that resides at each hierarchy type:

a. Customer hierarchy

- **DN inventory** - for the lines to be shared across sites.

Note: The DN inventory is visible across all sites under the customer. Allowing DN Inventory to be configured at the customer hierarchy node is an enhancement for the Shared Line Across Sites feature. Note that DN inventory can only be created at the customer hierarchy node when a non-SLC-based customer dial plan has been deployed. A transaction error is sent if the administrator attempts to create customer level DN inventory with an SLC-based dial plan.

b. Inventory site, includes:

- **Line relations** - for the DNs to be shared across sites.
- **Directory Number Routing (DNR)** entry for the line relations configured at this site to make the DNs inter/intra-site dialable.
- **E.164 inventory** - for the line relations configured at this site.

- **E.164 associations** - for the line relations configured at this site.
- **Line Class of Service (CoS)** - for the lines configured at this site. CoS is discussed in more detail in [Class of service for shared line across sites](#).
- **Short codes** - for the line relations configured at this site.

c. Real site, includes

- **DN inventory** - for lines to be used only at this site. Note that these DNs can be shared by multiple phones within the site.
- **Users** - configured via **Users** page or **Quick Add User**.
- **Line relations** - for the DNs configured at this site. These line relations do not have to be configured first; they are configured automatically any time a phone, extension mobility profile, or remote destination profile references a line that doesn't exist in the inventory site.
- **Directory Number Routing (DNR)** - for each of the line relations configured at this site.
- **E.164 inventory** - for lines created at this site.
- **E.164 associations** - for lines created at this site.
- **Device Class of Service (CoS)** - to be used for the phones configured at this site.
- **Phones** - these phones can reference lines that were defined in the inventory site or the Real Site where the phone exists.
- **Extension mobility** - these profiles can also reference lines that were defined in the inventory site or the Real Site where the phone exists.
- **Single Number Reach** - these profiles can reference lines that were defined in the inventory site or the Real Site where the profile is defined.

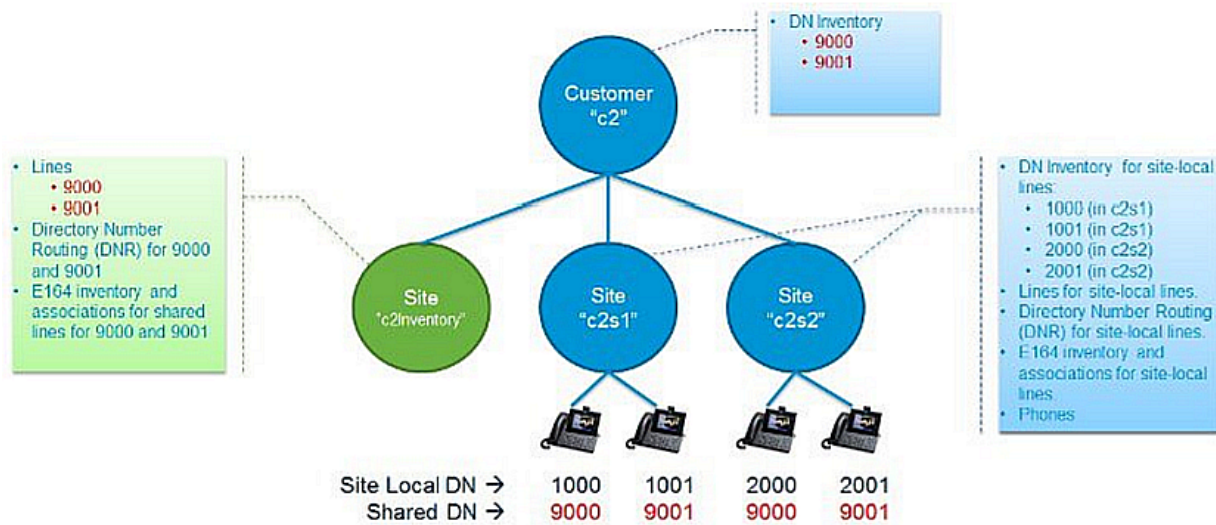
Fields in Automate that reference DNs, such as the **Pattern** field in the **Line** tab of a phone, are in a drop-down list of DN inventory. The drop-down list of DNs includes inventory defined at the customer level, combined with the inventory defined at the current site context. The administrator can choose either a cross-site shared DN or a site-local DN.

Diagram showing shared line across sites configuration

The image provides a basic *shared line across sites* configuration:

- Uses one inventory site ("c2Inventory") and two real sites ("c2s1" and "c2s2")
- Shows two shared DNs (9000 and 9001 shown in red) and four site-specific DNs (1000 and 1001 at c2s1, 2000 and 2001 at c2s2).
- The inventory for the shared DNs are provisioned at the *customer* hierarchy to make them visible to all sites under the customer. This allows the sites to configure the associated line and assign the line to a device.
- The inventory for the non-shared-across-sites DNs is still configured at the real sites (in blue) as it was in previous Cisco HCS releases.

Note that both shared DNs and non-shared DNs can co-exist for the same customer.



Configure shared line across sites

Tip: Use the Action search to navigate Automate

The steps for configuring shared lines across sites is generally the same as with conventional lines. This section highlights the differences.

- **Conventional, site-local lines:** Lines can be configured automatically as part of the phone, user, or Quick User workflows. Lines don't need to be configured separately first
- **Lines to be shared across sites:** Lines must be configured first in the inventory site, then referenced from phone, user, or Quick User workflows.

Configure shared line across sites at customer

The customer configuration is similar except that you create DN inventory at the customer hierarchy for lines you would like to share (or potentially share) across sites.

1. Configure the Cisco UCM and Cisco Unity Connection (CUC) devices. These can be at the customer level (dedicated) or above (shared).
2. Configure the customer normally (for example, c2).
3. Configure the Network Device List (NDL) for the customer (for example, c2Ndl) that will be used for your site group (NDL/Country combination).
4. Deploy the customer dial plan.

This must be a flat dial plan (for example, Type 4) since shared lines across site dictates that DNs cannot be site-specific. The Type 4 dial plan does not impose site-specific structure (in other words, site location codes). When configuring the customer dial plan, ensure that the Site Location Code check box is unchecked.

5. Configure the DN inventory to be used across sites for shared lines (via the **Directory Number Inventory**). Note that you should leave the site drop-down list empty to create the inventory on the Customer hierarchy node.

Configure shared line across sites at inventory site

The *inventory site* is only needed if you want to configure shared lines across sites. If you do not have this requirement you do not need an inventory site and configuration is exactly as it is done normally. Most of the inventory site configuration is the same as configuration for a real site (for example, deploy site dial plan, configure DN inventory, and so on). The areas that are unique to the inventory site are provided in Steps 1, 3, and 5.

1. Configure the inventory site and specify the NDL and Country, for example, c2InventorySite. A different inventory site is needed for each NDL/Country combination (site group). If the customer only has one NDL and one Country, they only need one inventory site.
2. Deploy the site dial plan (Type 4 will automatically be used based on the customer dial plan that was deployed).
3. Create the new Classes of Service to be used as the default line CSS and update the Site Defaults procedure for the inventory site.

See [Class of service for shared line across sites](#).

4. Configure Directory Number Routing (DNR) for the shared lines (via **Directory Number Routing**).
5. Create line relations for each shared line (via **Line**).
6. Create E.164 inventory (via **Add E164 Inventory**).
7. Associate E.164 to DN (via **E164 Associations (N to N)**).
8. Configure Hunt Groups that use shared lines (via **Hunt Groups**).
9. Configure Call Pickup Groups that use shared lines (via **Call Pickup Groups**).

Configure shared line across sites at real sites

Configuration at the real sites is almost exactly the same as in past Cisco HCS releases. The major difference is that the Shared Lines Across Sites exist at the inventory site and therefore any configuration associated with those lines (CoS, DNR, E.164 associations, and so on) exists at the inventory site.

1. Configure the real site (for example c2s1, c2s2, and so on). Use the same NDL and Country as the inventory site (same site group).
2. Deploy the site dial plan on each of the real sites (again, the customer dial plan enforces that the flat dial plan is used).
3. Create DN inventory for an DNs that will be used only at this site.
4. Create Directory Number Routing (DNR) for any DNs created at this site.
5. Create E.164 inventory and associations for an DNs created at this site.
6. Create Device Class of Service if needed. See [Class of service for shared line across sites](#).
7. Create Line Class of Service if needed for your site-specific lines. Refer to [Class of service for shared line across sites](#).
8. Configure users and phones (via **Quick Add User**, or **Phones**).
 - a. When configuring normal lines (lines that aren't shared across sites), select a line from the local site DN inventory, not the customer-level DN inventory. The line is created at the local site as normal; you can configure line CoS, DNR, E.164 associations at this site as normal. Note that this includes shared lines that are only shared within the site.

- b. When configuring a shared line across sites, select a customer-level DN from the drop-down list. Remember, the line should be configured at the inventory site first.
9. Configure site-specific Hunt Groups that use lines local to the real site.
10. Configure site-specific Call Pickup Groups that use lines local to the real site.

Dial plan type for shared line across sites

The *shared lines across sites* functionality only works if you're using a flat dial plan (Type 4), or a custom, non-site-specific, dial plan. This is because other dial plans (Types 1 to 3) have site location codes in the DN that don't work if the DN is shared by multiple sites.

If you're using predefined dial plans, ensure the **Site Location Code** checkbox is clear (disabled) when deploying the customer dial plan.

Class of service for shared line across sites

Class of Service (CoS) refers to a Calling Search Space (CSS) that is specifically used to define call routing and feature processing for a line or a phone.

Several CSSs are defined when a customer and site dial plan are deployed. Some of these are only used internally (don't select these CSSs in the CSS drop-downs when configuring a line or phone).

Class of Service CSSs are listed on the **Class of Service** page. A few example CoSs are predefined when a site dial plan is deployed, but the intent is for the administrator to create their own CoSs to meet the desired call routing and feature processing behavior. Below is a summary of Class of Service as it pertains to Shared Lines Across Sites feature.

Class of service is used in two places in Automate:

- Line calling search space (via the **Lines** page, Directory Number Basic Information tab, Calling Search Space)
- Device calling search space (via User Management GUIs, Phones page or Users page, Calling Search Space Name setting)

Additionally, CoS can provide line-based routing (LBR) or device-based routing (DBR). For each call made from a phone, the device CSS of the phone is combined with the line CSS of the line from which the call is being made, and the features and routing for the call are processed based on the combined list of partitions of these two CSSs. The default set of CoSs provided when a site dial plan is deployed includes a device CoS for emergency dialing only, and several line CoSs for feature processing, national dialing, and international dialing and that support either DBR and LBR. The following table shows the default allocation of feature and routing duties between the two sets of CoSs.

Feature	Default Device CoS	Default Line CoS
Emergency call routing	yes*	-
Intrasite routing	-	yes
Intersite routing	-	yes
Local PSTN call routing	-	yes**
National PSTN call routing	-	yes
International PSTN call routing	-	yes
Feature processing	-	yes

Table: Default Class of Service for Shared Line Across Sites Feature

* Emergency call routing is dependent on the country configured for the site. The country is used to route to the correct emergency number for that country (for example, 911 routes to 112 in the United Kingdom). Emergency call routing is assigned to the Device CoS because it is location-dependent, and must be tied to the site where the phone/user actually resides.

** Local call routing is dependent on local area codes defined in the site dial plan. The local area codes configured in the site dial plan allow dialing local dialing (for example 7-digit dialing in the United States).

As shown in the table above, routing is weighted heavily toward the line CoS because when the CoS is assigned to the line, it applies equally to the phone, extension mobility, and single number reach, which all typically share the same line configuration and provide similar dialing behavior for a given user. However, this assumes that the lines and devices are all constrained to individual sites. When we open up lines to be shared across sites, the site-specific configuration becomes more important in order to determine what to put in the device CoS versus the line CoS.

Class of Service (CoS) management for Shared Lines Across Sites is heavily dependent on the customer's specific deployment scenario. The distribution of work between the device CoS and the line CoS depends on the type of country dial plan, and the dialing behavior the customer wants.

For example, if the country dial plan is flat and closed like the Swiss dial plan, meaning that the user numbers are not variable length and there is no site-specific area codes (only national dialing), then most of the routing can occur in the line CoS because there is not much site-specific dialing behavior.

However, if the country dial plan uses area codes and the customer wants a local dialing experience (ability to dial a shorter number such as 7-digit dialing in the United States, and relying on the dial plan to fill in the local area code), then local call routing must be in the device CoS because the device context is needed to determine which area codes to apply to the dialed number. Feature processing partitions can almost always stay with the line CoS since there is usually no geographic dependencies for the feature processing. The exception to this is Time of Day (TOD) routing which may vary depending on the site.

The table provides details for determining how to distribute routing and feature processing between the line CoS and device CoS.

Feature	Line CoS	Device CoS
Emergency call routing	-	Emergency routing should always be location-specific
Intrasite routing	Always using the PreISR route partition	-
Intersite routing	Always using the PreISR route partition	-
Local call routing	When full E.164 number is always dialed for offnet calls, for example, national dial plans with no local call routing	When site-specific area codes and/or variable length user numbers (local dialing behavior) are defined
National call routing	If local dialing is line-specific, national dialing should be line-specific.	If local dialing is device-specific, national dialing should be device-specific.
Toll-free call routing	If local dialing is line-specific, toll-free dialing should be line-specific.	If local dialing is device-specific, toll-free dialing should be device-specific.
International call routing	If local dialing is line-specific, international dialing should be line-specific.	If local dialing is device-specific, international dialing should be device-specific.
Service call routing	If local dialing is line-specific, service number dialing should be line-specific.	If local dialing is device-specific, service number dialing should be device-specific.

To speed up the process of configuring lines and phones when you create new Classes of Service, set the site-specific default line CSS and site-specific default device CSS (**Site Management > Defaults**). These fields appear in the following tabs:

- **Device Defaults > Default CUCM Device CSS**
- **Line Defaults > Default CUCM Line CSS**

Call forward considerations for shared line across sites

As the administrator, you can create the Call Forward CSS as a CoS for a particular deployment scenario. Considerations must be made based on whether the local, national, and/or international dialing is configured on the device CoS or line CoS.

Be aware that if the Call Forward CSS allows national and local PSTN routing, you may need to consider call forward scenarios when a line is not associated to a device and PSTN dialing is in the device CoS.

Phone, user, and Quick User for shared line across sites

Phones and users should only be created at *real* sites and not at *inventory sites*. However, the system workflows don't enforce this rule, but will help facilitate ongoing management of the configuration data for the customer.

Lines referenced in the **Phone** screen, the **Users** screen, or the **Quick Users** screen are created automatically if they have not already been provisioned in the inventory sites and pushed to Cisco UCM. This is acceptable as long as you intend for these lines to be only referenced within one site. If a line gets created on a *real* site that you intended to share across sites, it is recommended that you delete the line, and recreate it in the *inventory* site.

Relevant fields for *shared lines across sites* on the **Phone** screen are:

- **Phone** tab: On this tab you specify the Calling Search Space Name (that is, the device-based routing CoS, which is by default the emergency routing CSS). Depending on choices made above in the Class of Service section, you might chose a different CSS here.
- **Lines** tab: On this tab you select the DN (Pattern) from the drop-down list, and configure the *E.164Mask* used for line presentation. The **DN** drop-down includes DNs from the Customer DN inventory combined with the current site DN inventory.

At the time of writing, the *E.164Mask* is a free-form field and is not tied to the *E.164* inventory; it must be manually entered.

The **Route Partition Name** field is automatically populated with the correct directory number partition based on the Pattern (DN) chosen. Similar fields exist in the **User** tabs.

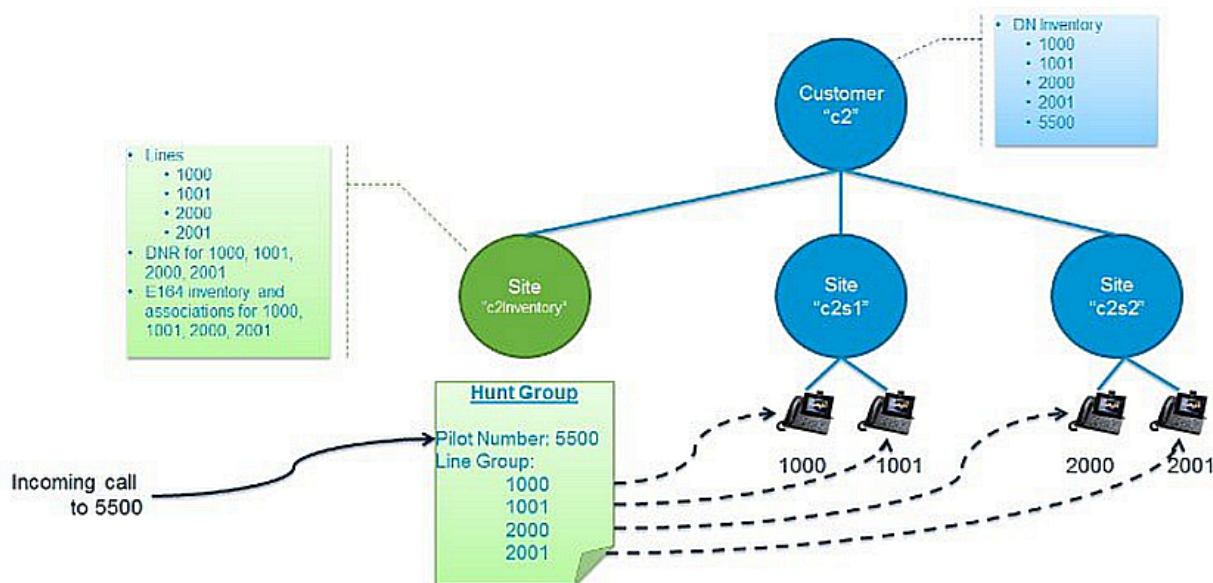
Hunt groups and call pickup groups for shared line across sites

Hunt groups and call pickup groups can be set up in either the *inventory site* or in the *real sites*, with the following conditions:

- **Inventory site:** When configured in the *inventory site*, the hunt groups and call pickup groups can include any line created in that site, but not from other sites.
The recommended setup is to use the *inventory site* if your hunt group or call pickup group needs to include lines from multiple sites.
- **The real sites.** When configured in the *real site*, the hunt groups and call pickup groups can include lines from the *real site*, but not from other sites.

Example scenario

The image provides an example of a hunt group that uses lines spanning multiple sites.



In this example, the hunt group includes the following lines:

- 1000
- 1001
- 2000
- 2001

These lines are *not* shared across sites, but to include them all in one hunt group, they must all be configured at the *inventory site* so that they can all be grouped under a single hunt pilot number, 5500.

Note:

- The hunt pilot directory number (DN) inventory is at the customer level.
- Once the hunt pilot is assigned, that DN becomes unavailable for other uses:
 - It can't be assigned to a device as a line
 - It can't be used for another service pilot number

Handling voicemail to secondary shared lines

To handle voicemail to secondary shared lines, create a separate user for each shared line at the Inventory Site level, then enable the voice mailbox for that user so that it can be managed by all shared lines.

This approach:

- Offers the ability to differentiate between voice mail deposited for primary and secondary lines
- Provides separate message waiting indication (MWI) notifications for voice mail in the phone's primary and secondary line
- Allows all configuration to be done in Automate. There are no separate manual configurations required in Cisco Unity Connection (CUC) or Cisco Unified Communications Manager (UCM).

Note: One additional license is required for the shared line user mailbox.

4.42.2. Inventory site

Tip: *Use the Action search to navigate Automate*

Overview

An inventory site is the same as any site, except that it is designated (**Inventory Site** checkbox is enabled) as the repository for lines to be shared across sites. It is deployed in the same way as any other site.

The inventory site is created on the **Site** page. It requires an NDL and a country, and requires a site dial plan to be deployed.

Note: There is no enforcement of configuration ensuring that, for example, only lines are configured at the Inventory Site and not phones. It is the responsibility of the administrator to ensure the proper procedures and conventions are followed as documented in this guide. Therefore, it is important to ensure a good understanding of how the Inventory Site is to be used, and how the Inventory Site configuration relates to the configuration of the “real sites”.

There are several caveats and restrictions that must be followed when using the Inventory Site as summarized below. Detailed configuration procedures are provided later in this document. For the purposes of this discussion, the term *Site Group* is used to describe an Inventory Site combined with the “real sites” which use the shared lines defined in the Inventory Site.

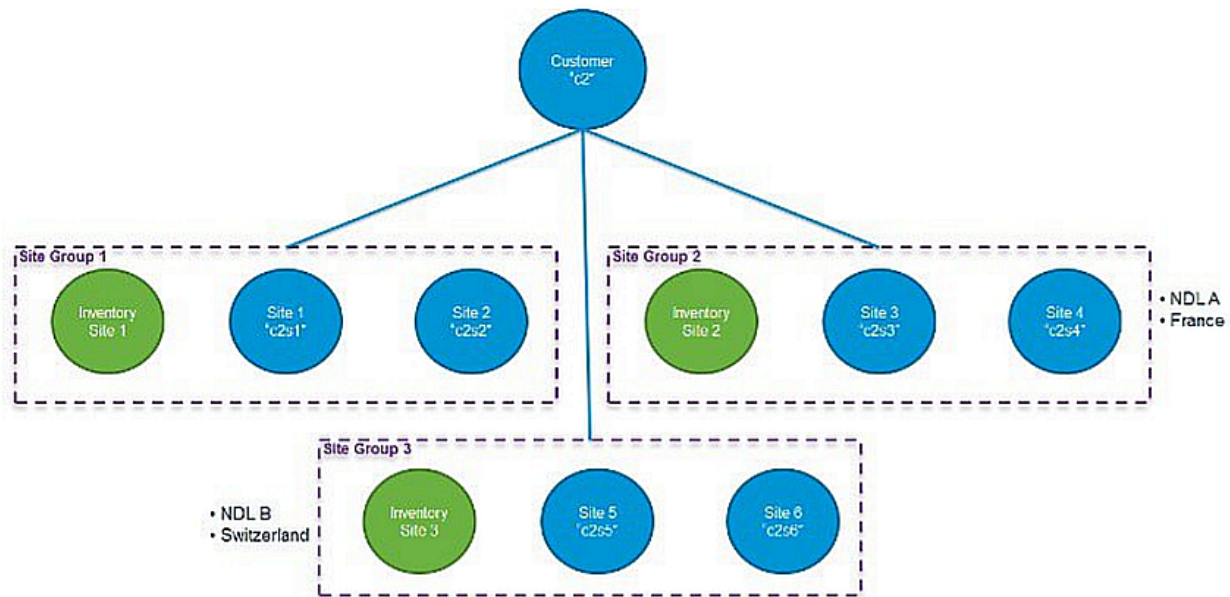
All sites in a site group must conform to the following rules:

- The sites must be configured with the same NDL and country. Any site that has the same NDL and country as the Inventory Site can participate in the same site group. In fact, the NDL and country settings are what defines the site group.
- Shared lines configured in the Inventory Site of a site group can only be used by other sites in the same group, not in other groups. This means that shared lines cannot span NDLs, and cannot span countries.

Tip: If a line is potentially shareable, we recommend that you create the line in the Inventory Site, even if it will not be shared across sites immediately. The system does not support the ability to move a line from a real site to an Inventory Site, so to convert a line from site-local to cross-site shared, the line would need to be deleted from the real site and recreated in the Inventory Site.

Inventory site diagram

The diagram shows a customer with three site groups:



4.42.3. Site short codes

Site short codes work the same for deployments that use shared lines across sites as they do for “real site” deployments. That is, short codes can be added to a site to allow shorter, convenient numbers to be dialed that are transformed into longer directory numbers. Normally, short codes are added to real sites that contain devices in order to allow users of those devices to dial shorter numbers to reach existing directory numbers.

Because the inventory site doesn’t contain devices, but only line inventory, site codes don’t need to be added to the inventory site. Short code translation patterns are created on a site’s Allow Internal (AIInt) route partition.

4.42.4. Configure tail end hop off

Note: The following task is applicable only if you are using Automate 10.6(2) or later.

Follow these steps to manually configure Tail End Hop Off (TEHO) in Cisco Unified CDM:

1. Configure route-group:
 - a. Select the hierarchy up to customer level. For procedures, see Configure Route Groups.

Note: While adding a new route group, enter a name and then select the sip_trunk added to the remote LBO site (for example, RouteGroup: TEHO-RG, Device: L1LBO-SIP).

2. Configure route-list:

Select the hierarchy up to customer level. For procedures, see Configure Route Lists.

Note: While adding a new route list, enter a name and then add three route groups (for example, RouteList: TEHO-RL, 1stRouteGroup: TEHO-RG, 2ndRouteGroup: SLRG-Natl, 3rdRouteGroup: RG-AGGR).

3. Configure route-pattern:

- a. Log in as Provider or Reseller Administrator.
- b. Select the hierarchy up to customer level.
- c. Go to **Route Patterns**.
- d. Click the Route Pattern from the list.
- e. Go to Action, and then click **Clone**.
- f. In the **Pattern Definition** tab, select the CUCM.
- g. Edit the Route Pattern name.
- h. Select the Route List that is configured when configuring the route list for TEHO (for example, RoutePattern: **[0-3]0[236-9]1.608!, RouteList: TEHO-RL). In this route pattern, 608 is the area code for the remote location).

5. Advanced management

5.1. Macros

5.1.1. HCS dial plan macros in Automate

Macros can be used in Automate to dynamically add site IDs, customer IDs, and other types of information when customizing dial plan schemas and Class of Service. Macros increase ease of use and reduce error.

Macros are evaluated within the context of a particular hierarchy node based on the scope specified in the schema group binding, for example, site, customer, provider.

The correct syntax for a macro is the word “macro” followed by a period (.), followed by the named macro.

Add double curly brackets ({{ }}) around the entire macro combination.

For example, {{ macro.HcsDpCustomerName }} is the macro combination created using the first named macro in the table below. Note that there are no spaces in a named macro.

This table provides a list of named macros - see also the named macros in the Automate documentation index:

Named Macro	Description
HcsDpCustomerName	Name of the customer (as specified when you create your customer)
HcsDpCustomerId	Systemwide, unique internal customer ID generated when you create a customer
HcsDpSiteName	Name of the site (as specified when you create a site under a customer)
HcsDpSiteId	Systemwide, unique internal site ID generated when you create a site
HcsDpUniqueCustomer PrefixMCR	Default unique Cisco HCS customer prefix in the form 'Cu{{ macro.HcsDpCustomerId }}
HcsDpUniqueSite PrefixMCR	Default unique HCS site prefix in the form 'Cu{{ macro.HcsDpCustomerId }}Si {{ macro.HcsDpSiteId }}
HcsDpSiteCountryMCR	Returns the country associated with a specific site
HcsDpSiteCountryIso	Returns the ISO 3166-1 alpha-3 three-letter country code associated with the country that is associated with a specific site
HcsDpPstnBreakout	Returns the PSTN prefix digit for the country that is associated with a specific site
HcsDpSiteAreaCode InLocal-DialingMCR	Returns True if a specific site requires area code for local PSTN dialing
HcsDpSiteNatTrunk PrefixMCR	Return the national trunk prefix associated to a particular site
HcsDpDefaultSite Device-PoolMCR	Default Cisco HCS site device pool Cisco Unified Communications Manager element name
HcsDpDefaultSite LocationMCR	Default Cisco HCS site location Cisco Unified Communications Manager element name
HcsDpDefaultSite RegionMCR	Default Cisco HCS site region Cisco Unified Communications Manager element name

The table lists macros that can be used to loop through the area codes specific for a particular site when adding translation patterns:

Named Macro	Description
HcsDpSiteAreaCodeMCR	Returns list of area codes associated with a specific site
HcsDpSiteAreaCode Item_AreaCodeMCR	Return the area code attribute from the area code list item
HcsDpSiteAreaCode Item_LocLenMCR	Return the local number length attribute from the area code list item

Related Topics

- Macro Evaluate Function in the Advanced Configuration Guide
- Create an Evaluation Macro in the Advanced Configuration Guide
- Macro Evaluator in the Advanced Configuration Guide

5.2. Auto-cloning of dial plan schemas and schema groups to the Provider hierarchy node

5.2.1. Auto-cloning of dial plan schemas and schema groups to the provider hierarchy node

All existing dial plan schema and schema groups are cloned automatically from the System Administration level in Automate 10.x/11.5(x) to the Provider hierarchy node when the following events occur:

- You create a new provider
- You perform an upgrade from a previous version of Automate

New dial plan schema files and schema groups are also cloned automatically to existing Provider hierarchy nodes when the following events occur:

- You load or import a country dial plan template that introduces additional dial plan schema files or schema groups at the System Admin level, the new additional schema files are cloned automatically to any existing Provider hierarchy nodes.
- New dial plan schema or schema groups are created using native GUI, REST API, native bulk loader, imported JSON files, or using the app install template, the new schema and schema groups are cloned automatically to existing Provider hierarchy nodes.

The cloned version at the Provider level has the same name and is an exact replica of the dial plan schema or schema group at the System Admin level except that the Description field in the **General** tab of the schema indicates that it is the Cloned instance version.

Note: The auto-cloning mechanism does not clone a schema or schema group to the Provider level if there is already one at the Provider level with the same name.

Auto-cloning of the dial plan schema and schema groups to the Provider level ensures that any dial plan schema and schema group changes you make to existing Cisco templates are not lost when a Cisco template upgrade is introduced. As a Provider, you can also add your own schemas and schema groups at the Sys Admin level and be confident that these will be cloned down to the Provider level and not be overwritten by upgraded Cisco templates.

Your dial plan schema changes are retained because when you deploy new customers and sites, the system searches up the hierarchy node tree to find the first instance of a particular template name to use for the deployment.

For example, when deploying the Customer Call Screening feature schema for a customer, the system searches up the hierarchy node tree for the first instance of the CustomerCallScreening-Feature-V1-SCH. It will find two instances of CustomerCallScreening-Feature-V1-SCH:

1. CustomerCallScreening-Feature-V1-SCH (at the Provider level - e.g. sys.hcs.p1)

2. CustomerCallScreening-Feature-V1-SCH (at the System Administration level - e.g. sys-hcs)

Because the schema names are identical and the Provider hierarchy node is found first, the Provider level CustomerCallScreening-Feature-V1-SCH schema is used to deploy the customer. Any customizations you made to the CustomerCallScreening-Feature-V1-SCH schema at the Provider level are retained if the template at the System Administration level gets updated by an upgrade.

5.3. Create schemas

5.3.1. Dial plan schemas

This procedure configures a customized group of related dial plan elements in Cisco Unified Communications Manager (Cisco UCM), including time periods, time schedules, partitions, calling search spaces, translation patterns, calling and called party transformations, CTI route points, route lists, route patterns, and SIP route patterns.

Note: When configuring a dial plan schema using this procedure, the elements are only available on the UCM after the dial plan schema is placed in a dial plan schema group (refer to Create Schema Groups), and once the group is associated with a customer (refer to Associate Custom Schemas to Customers).

It is strongly recommended that all dial plan entries in a dial plan should be unique.

Perform these steps:

1. Log in to Automate as a Provider or Reseller administrator.
2. Go to **Dial Plan Schema**.
3. To add a new custom schema, click **Add**.
4. On the **General** tab, enter a unique name for the schema, and (optionally) add a description.
5. On the **Time Periods** tab, click the Plus icon (+) to open the form for time period information, and fill out required details:
 - Define a name and (optionally) a description for the time period.
 - At **Time of Day Start** and **Time of Day End**, choose a start and end time.
 - (Optional) At **Start Day**, **End Day**, **Start Month**, and **End Month**, choose the day and month characteristics of the time period, as required.
 - (Optional) Fill out values for **Start Day of the Month** and **End Day of Month**.
 - Click **OK**.
6. On the **Time Schedules** tab, click the Plus icon (+) to open the form to add time schedule information, and fill out details for the schema:
 - Enter a name and a description for the time schedule.
 - At **Time Periods**, click the Plus icon (+) to add a time period name, and click **OK**.
7. On the **Partitions** tab, click the Plus icon (+) to open the form for adding partition details, then enter a partition name and description, and provide the time schedule.

Note: You can use macros to add partition information. For more information on using macros as part of the Partition Names, Descriptions, or Time Schedules, see Macros.

8. On the **Calling Search Spaces** tab, click the Plus icon (+), then fill out CSS details for the schema:

Note: You can use macros to add calling search space (CSS) details.

- Enter a CSS name and (optionally) a description.
 - At **Partition Usage**, enter a reason for the CSS.
 - If this CSS is used in a class of service, select the **Class of Service CSS** checkbox.
 - To add more detail about the partitions for this CSS, click the Plus icon at **Partitions**, then add a route partition name and an index.
 - Click **OK**.
9. On each of the following tabs, click the Plus icon (+) to open the editing form, and fill out the relevant details for the schema.
- Translation Patterns tab
 - Calling Party Transformation Patterns tab
 - Called Party Transformation Patterns tab
 - CTI Route Points tab
 - Route Lists tab (to add route lists)
 - Route Patterns tab (to add route patterns)
 - SIP Route Patterns tab (to add SIP route patterns)
10. Click **Save** to create the new dial plan schema.

Next steps

- Create schema groups to add dial plan schemas to a schema group.

5.4. Clone dial plan schemas

5.4.1. Clone dial plan schemas

Tip: *Use the Action search to navigate Automate*

This procedure copies one of the default dial plan schemas (or a previously customized schema) to use as a starting point when creating a new dial plan schema.

1. Log in to Automate as Provider or Reseller administrator.
2. Go to **Dial Plan Schema**.

- From the list of dial plan schemas, choose the one to be cloned, by clicking on its box in the leftmost column. For more information on the default dial plan schemas, refer to Default Dial Plan Schemas.

Note: There may be duplicate dial plan schemas in the list because some of the dial plan schemas may have been auto-cloned to the Provider hierarchy node. For more information, see Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node.

- Click **Action > Clone**.
- From the **General** tab, enter a new unique name for the cloned dial plan in the Dial Plan Name field.
- If desired, add a description of the new cloned dial plan schema in the Description field.
- Modify or add time periods, time schedules, partitions, calling search spaces, translation patterns, calling party transformation patterns, called party transformation patterns, CTI route points, route lists, route patterns, and SIP route patterns as desired by clicking on the appropriate tab.
- Click **Save**. The new dial plan schema appears in the list of Dial Plan Schemas.

5.5. Modify site defaults

5.5.1. Site defaults

Tip: *Use the Action search to navigate Automate*

Overview

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

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

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

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

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

Configure site defaults

This procedure displays and updates site defaults.

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

Note:

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

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.

Site defaults settings

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

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

- [General Defaults tab](#)
- [Device Defaults tab](#)
- [Line Defaults tab](#)
- [User Defaults tab](#)
- [CUC Defaults tab](#)
- [HotDial Defaults tab](#)
- [Overbuild Defaults tab](#)
- [Move Filter Criteria tab](#)
- [MS Teams tab](#)
- [Webex tab](#)

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 (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 user), the phone type you choose must support the protocol you wish to use (SIP or SCCP). If the phone type does not support the protocol, the protocol defaults to the protocol value set up in the site defaults (if the phone type supports the default protocol).
Default CUCM Device Profile Button Template	Standard 9971 SIP

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:</p> <p>For Quick Add User, set the following value in the E164 Mask field of the relevant phone, device profile and remote destination profile configuration template {{ macro.SDD_QAS_E164Number_MCR }}. See the "Reference CUCM Phone Template" CFT for an example configuration.</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).

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

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

CUC Defaults tab

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

Cisco Unity Connection Localization in the Core Feature Guide.

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

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

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

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

The table describes the settings on this tab:

Field	Description
Include Site for Overbuild	Defines whether the site is included in the overbuild.
Create Internal Number Inventory at Customer	<p>Defines whether to create the internal number inventory only at the site level, or only at the customer level.</p> <p>When set to True (checkbox selected), the internal number inventory is created only at the customer level, and will be used by all sites belonging to that customer.</p> <p>The default is False.</p> <p>CAUTION: If overbuild has already been run for a site and the internal number inventory has been created for the site, if <i>Create Internal Number Inventory</i> is enabled and you run overbuild for the same site, a duplicate set of internal number inventory is created at the customer. The same applies if Create Internal Number Inventory at Customer is enabled when the overbuild is run for the site, if it is then disabled and overbuild is run again, a duplicate set of internal number inventory is created at the site.</p>
Additional Device Pools	<p>By default, if a site is included for overbuild, the Default CUCM Device Pool on the General Defaults tab must match the device pool of phones that have been imported in order for these and their related objects to be moved to the site at which the Site Defaults Doc exists.</p> <p>The Run Overbuild tool uses the device pool to determine the devices and models to move to the site where the site defaults are defined. You can however add additional device pools, so that more than one device pool from those of the imported phones can be moved to the same site.</p> <p>Additional device pools are selected from the Device Pool Name drop-down, as instances of the Additional Device Pools group control.</p> <p>The names of the additional device pools can be renamed to the Default Device Pool name (as defined on the General Defaults tab) if Replace with Default Device Pool is selected.</p>
Overbuild Device Control	<p>Options are:</p> <ul style="list-style-type: none"> • Move all devices - when True, all matching and related imported devices are moved to the site. • Limit moved devices - when True, options display to choose devices to import to the site (as on Run Overbuild page)

Related topics

- Overbuild for Microsoft in the Core Feature Guide

Move Filter Criteria tab

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

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

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

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

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

Related topics

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

MS Teams tab

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

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

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

The table describes settings on this tab:

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

Webex tab

The table describes settings on this tab:

Option	Description
Webex Location ID	<p>The Webex location to which the site is mapped. Webex locations, numbers and users with location ID matching this site, will be synced to it.</p> <p>This dropdown allows selection of Webex locations at higher hierarchies.</p>
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 user and Webex App user have the same email address • User does not already have Jabber clients • CUCM calling behavior is not yet configured for the Webex App user <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 UC Manager Profile (device/spark/CallingProfile).</p>
Webex User Model Filter Criteria	<p>Allows you to select predefined model filter criteria for use with the Webex user. Requires that you set up the model filter criteria so that it appears in this drop-down. You can use this option to move the user to the site when running a data sync.</p>

Related topics

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

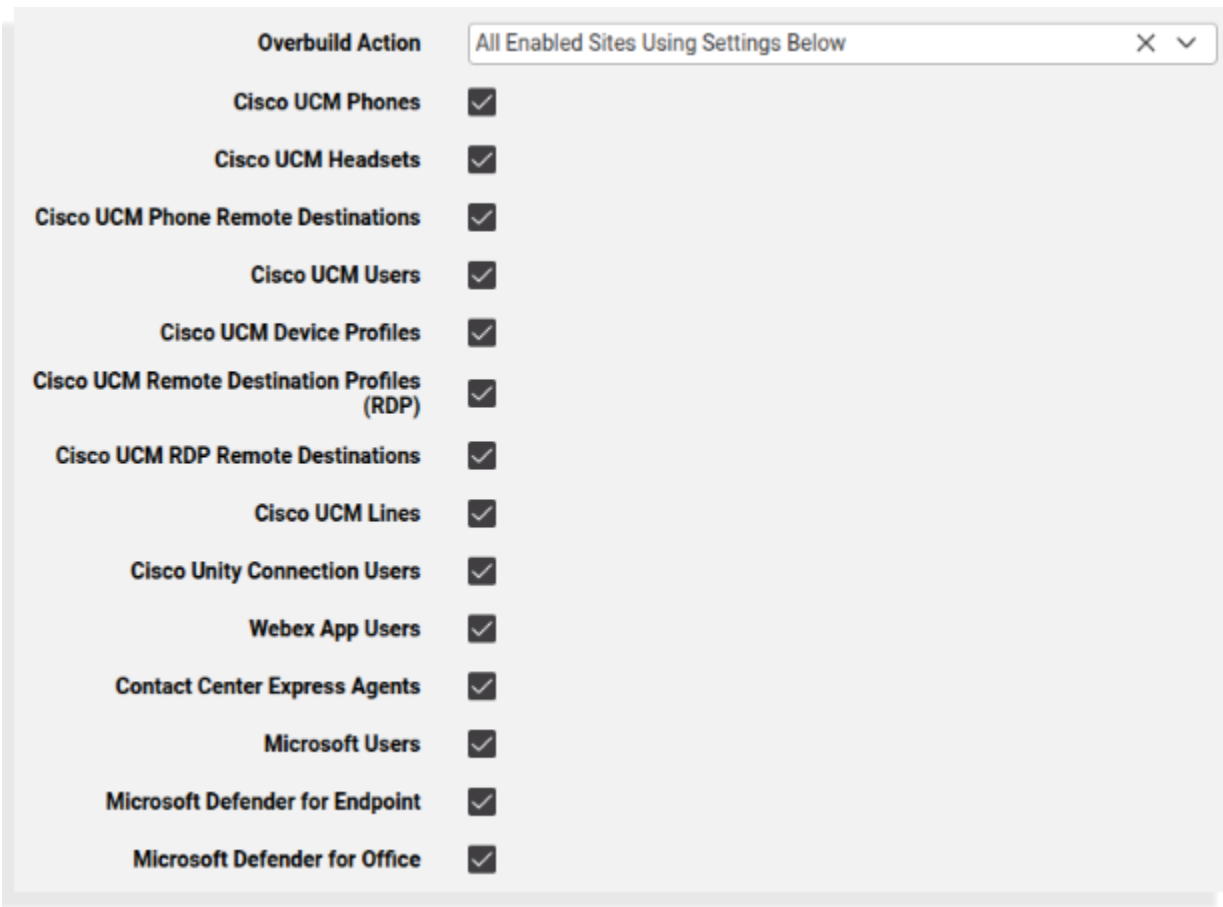
5.5.2. Run overbuild

Tip: *Use the Action search to navigate Automate*

Overview

The *Run Overbuild* tool imports objects.

Note: To access the Run Overbuild tool, go to **Run Overbuild**.



Overbuild action

The table describes options available for **Overbuild Action** on the **Run Overbuild** page

Overbuild action	Description
All Enabled Sites Using Settings Below	<ul style="list-style-type: none"> • Includes all devices selected on the form. • Includes all sites that have their site defaults doc configured to include the site in overbuild • An internal number inventory is created at customer level when Create Internal Number Inventory at Customer setting is selected, else, it's created at the site (if lines are included). • Device pools are from the General Defaults tab in the Site Defaults, and additional device pools are from the Overbuild Defaults tab. • The devices that display when Limit Move Devices is selected on the Overbuild Defaults tab are ignored. Runs Overbuild for all sites, and uses the devices selected on the Run Overbuild page. <p>When Run Overbuild executes with this option, it applies to all sites and uses devices selected on the Run Overbuild page.</p> <p>Run Overbuild devices supersede the devices selected in Limit Move Devices.</p>
All Enabled Sites Using Site Defaults Doc Overbuild Settings	<ul style="list-style-type: none"> • Hides and ignores selected devices on the Run Overbuild page. Moves all selected devices (when Limit Moved Devices is selected on the Overbuild Defaults tab in the Site Defaults) • Includes sites that are included for overbuild in their Site Defaults doc. • Creates internal number inventory at Customer level (when Create Internal Number Inventory at Customer option is chosen, else at site level (if lines is selected)). • Device pools are from the General Defaults tab in the Site Defaults, and Additional Device Pools are used from the Overbuild Defaults tab in the Site Defaults.

Overbuild action	Description
Single Enabled Site Using Settings Below	<ul style="list-style-type: none"> • Overbuild is applied to the single site you choose. • The only sites available for selection are sites included for overbuild via their Site Defaults. • Includes all devices you choose on the page • Creates internal number inventory at Customer (if Create Internal Number Inventory at Customer option is selected); else, only at site (if Lines are included) • Device pools are from the General Defaults tab in the Site Defaults doc, and Additional Device Pools from the Overbuild Defaults tab. • Devices displayed when the Limit Move Devices option is selected on the Overbuild Defaults tab are ignored. Runs Overbuild for the selected site, and uses the devices selected on the Run Overbuild page. <p>When the Run Overbuild tool executes with this option, it applies to the selected site only, and uses devices selected on the Run Overbuild page. Run Overbuild devices supersede the devices selected in Limit Move Devices.</p>

Available device types

The available device types are shown in accordance with enabled services in Global settings (see: [Global settings](#)), for example:

- Cisco CUCM
- Cisco CUCX
- Cisco WebEx
- Cisco Webex App(Teams)
- Cisco UCCX
- Microsoft
- Defender for Office
- Defender for Endpoint

Available device types include:

- Phones
- Phone Remote Destinations
- Users (device/cucm/User)
- Device Profiles
- Remote Destination Profiles (RDP)
- RDP Remote Destinations

- Lines (a number inventory entry is also added for all device/cucm/Line) instances that are in the system at the customer or site level)
- CUC Users
- Webex App Users
- Pexip Users
- Contact Center Agents
- Microsoft Users
- Microsoft Defender for Endpoint
- Microsoft Defender for Office

Affected device models

The following device models are affected by the overbuild move:

- device/cuc/User
- device/cuc/UserPassword
- device/cuc/UserPin
- device/cuc/AlternateExtension
- device/cuc/ExternalServiceAccount
- device/cuc/SmtpDevice
- device/cuc/SmsDevice
- device/cuc/PagerDevice
- device/cuc/PhoneDevice
- device/cuc/HtmlDevice
- device/cuc/Callhandler
- device/cuc/CallhandlerMenuEntry
- device/cuc/CallhandlerTransferOption
- device/cuc/Greeting
- device/cuc/MessageHandler
- device/cucm/Phone
- device/cucm/User
- device/cucm/DeviceProfile
- device/cucm/RemoteDestinationProfile
- device/cucm/RemoteDestination
- device/cucm/Line
- device/pexip/Conference
- device/spark/User
- device/uccx/Team

- device/uccx/Skill
- device/uccx/ResourceGroup
- device/uccx/Agent
- device/msexchangeonline/SafeAttachmentPolicy
- device/msexchangeonline/SafeLinksPolicy
- device/msexchangeonline/QuarantinePolicy
- device/mssecurity/Machine
- device/msgraphsecurity/Alert
- device/msgraphsecurity/Incident

Related topics

- Microsoft Defender for Office security management and policies in the Core Feature Guide
- Microsoft Defender for Endpoint security management and policies in the Core Feature Guide

Affected data models

The following data models are affected when moving a user during overbuild:

- data/User

Device types available for selection depend on the status of other device type check boxes. For example:

- The following device types are only available if you've selected **Phones**:
 - Dual-Mode Remote Destinations
 - Users
 - Lines
- The following device types are only available if you've selected **Users**:
 - Device Profiles
 - Remote Destination Profiles
 - CUC Users

Overbuild and failures

Overbuild workflows do not stop on any transaction failures and no transaction rollback takes place on errors. For example, device instance move operations to sites continue for all selected devices. Inspect the transaction log for errors.

In the Transaction log, sub-transactions of a successful overbuild workflow show their status as "Fail" if a model (such as a User) already exists. The sub-transaction logs also show details of the duplicate model and an "ignore error code" information message.

If a number already exists and the global setting *Prevent Duplicate Number* is enabled, the sub-transaction to create a duplicate of an existing number fails.

Related topics

- Prevent duplicate numbers in the Core Feature Guide

5.5.3. Overriding Cisco UCM group

Tip: *Use the Action search to navigate Automate*

The default Cisco UCM group is used when creating the default device pool for a site when using Cisco Dial Plan Schema Types 1*4.

This topic describes the steps for using a Cisco UCM group other than “Default” when deploying a site dial plan.

The steps allow you to override the Default UCM Group when deploying a site dial plan. The workflow that creates the default site device pool is hard-coded to use the *Default* CM Group when a site is created is as follows.

- HcsDpAddSiteSystemDataPWF
 - Entire Country Dial Plan
 - Dial Plan Schema Group (Type 1, 2, 3, 4, Shell)
 - Device Pool (Device Management)
 - Route List (Device Management)
 - Hunt List (User management)
 - Voice Mail Pilot Number Schema (VoiceMailService)
 - Route List (Sip Gateway)
1. Log in as Provider admin.
 2. Set the hierarchy to the provider level.
 3. Go to **Dial Plan Schema Group**.
 4. On the Site Defaults tab, set the macro for the Default CUCM Group from:

```
{{ macro.DEFAULT_CUCM_GROUP }} =
(( fn.is_site == True )) <{{ data.SiteDefaultsDoc.defaultcucmgroup }}><{{ fn.null }}>
```

to

```
{{ macro.DEFAULT_CUCM_GROUP }} =
(( fn.is_site == True )) <{{ data.SiteDefaultsDoc.defaultcucmgroup }}><Default>
```

Setting the macro to Default returns the value of Default CUCM Group from the SDD if evaluated at site hierarchy, else it returns Default. This setting pushes the new or customized UCM groups in any workflow at the site hierarchy.

Note: If you delete the Default UCM group from the Cisco UCM, deployment of the UCM group fails, which isn't at site hierarchy. In this scenario, change the macro `DEFAULT_CUCM_GROUP` implementation and modify the

```
{{ data.SiteDefaultsDoc.defaultcucmgroup }}><CUSTOM_GROUP NAME>
```

5.6. Create schema groups

5.6.1. Dial plan schema group

Tip: *Use the Action search to navigate Automate*

This procedure bundles a set of schemas to form a custom dial plan. You can clone one of default Type 1 to Type 4 schema groups to use as a starting point to create your own dial plan schema group.

1. Log in to Automate as Provider or Reseller admin.
2. Go to **Dial Plan Schema Group**.
3. From the list of dial plan schema groups, select the schema group to be cloned.

Note: There may be duplicate dial plan schema groups in the list because some of the dial plan schema groups may have been auto-cloned to the Provider hierarchy node. For more information, see *Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node*.

4. From the **General** tab, enter a new unique name for the cloned dial plan schema group in the Dial Plan Schema Group Name field.
5. Optionally, add a description of the new cloned dial plan schema group in the **Description** field.
6. Modify or add site defaults, core schemas, feature schemas, country schemas, or custom workflows as required by clicking on the appropriate tab as follows:
 - a. From the **Site Defaults** tab, modify site defaults. For more information on site defaults, refer to Modify Site Defaults.

Note: If a site defaults doc (SDD) for a site is based on `CUSTOMER_TEMPLATE`, then any empty values set under this tab will *not* result in empty values being set in the site dial plan. Values that are set on the **General** tab in the `CUSTOMER_TEMPLATE` will be applied instead.

- b. From the **Core Schemas** tab, modify the fields. Select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the hierarchical level for the core schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.

- c. From the **Feature Schemas** tab, modify the fields. Select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the hierarchical level for the feature schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the feature schema that will be triggered by the event. This drop-down list includes all default and created feature schemas from the Create Schemas procedure.
 - d. From the **Country Schemas** tab, modify the fields as required. For desired country schemas, select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the country dial plan from the Country Name drop-down menu. Select the hierarchical level for the country schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the country-specific schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.
 - e. From the **Custom Workflows** tab, modify event workflows. From the Dial Plan Event drop-down menu, select an event trigger for your workflow. Contact Advanced Services if you require an event trigger that is not in the list. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Workflow drop-down menu, select the custom workflow to execute when the dial plan event is triggered.
7. Click **Save**. The new dial plan schema group appears in the list of groups.

Related Topics

- Introduction to Cisco HCS Dial Plan in the Core Feature Guide

5.7. Associate custom schemas to customers

5.7.1. Associate custom dial plan schema group

Tip: *Use the Action search to navigate Automate*

This procedure bundles a set of schemas together to form a Type 1 to Type 4 dial plan that can be applied to a customer.

Note: You can use the default Type 1 to Type 4 schemas that are predefined and specify the Core Schemas, Feature Schemas, and Country Schemas for a customer.

1. Log in to Automate as Provider or Reseller admin.
2. Go to **Associate Custom Dial Plan Schema Group**.
3. From the list of default Type 1 to Type 4 dial plan schemas, choose the one to be customized for a customer, by clicking on its box in the leftmost column.
4. From the **General** tab, enter a new unique name for the dial plan schema group in the Dial Plan Schema Group Name field.
5. If desired, add a description of the new dial plan schema group in the Description field.

6. Modify or add site defaults, core schemas, feature schemas, country schemas or custom workflows for the customer as desired by clicking on the appropriate tab as follows:
 - a. From the **Site Defaults** tab, modify site defaults as required. For more information on site defaults, refer to *Modify Site Defaults*.
 - b. From the **Core Schemas** tab, modify the fields as required. For desired core schemas, select a trigger event from the **Dial Plan Schema Usage** drop-down menu, then select the hierarchical level for the core schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.
 - c. From the **Feature Schemas** tab, modify the fields as required. For desired feature schemas, select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the hierarchical level for the feature schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the feature schema that will be triggered by the event. This drop-down list includes all default and created feature schema from the Create Schemas procedure.
 - d. From the **Country Schemas** tab, modify the fields as required. For desired country schemas, select a trigger event from the Dial Plan Schema Usage drop-down menu, then select the country dial plan from the Country Name drop-down menu. Select the hierarchical level for the country schema in the Dial Plan Schema Scope drop-down menu. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Dial Plan Schema Name drop-down menu, select the country-specific schema that will be triggered by the event. This drop-down list includes all default and created schemas from the Create Schemas procedure.
 - e. From the **Custom Workflows** tab, modify any other schema you need that are not included in any of the previous schema group tabs. From the Dial Plan Event drop-down menu, select an event trigger for your custom schema. Contact Advanced Services if you require an event trigger that is not in the list. For a description of the trigger events, refer to Default Dial Plan Event Triggers. From the Workflow drop-down menu, select the custom workflow to execute when the dial plan event is triggered.
7. Click **Save**.

The new dial plan schema group is saved. The new dial plan schema group appears in the list of groups.

5.8. Default dial plan schemas

5.8.1. Default dial plan schemas

A number of default dial plan schemas are predefined in Automate. You can use the default schemas as templates when provisioning a site, or clone the default schemas to use as the basis for your own custom schemas.

The default dial plan schemas are located in (default menus) **Dial Plan > Dial Plan Schema**.

Note: In the tables below, Vx represents the schema version, where x is the version number.

Each dial plan schema in the tables are also automatically cloned to the Provider hierarchy node. For more information, see Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node.

Default Dial Plan Schemas

Schema Name	Description	When Deployed
CustomerCallScreening-Feature-Vx-SCH	<ul style="list-style-type: none">• Contains partitions, calling search spaces, and translation patterns necessary to implement the call screening feature used during Class of Service creation to block or allow calls based on call type (for example, International, National, Mobile, Service, PRS, Free Phone, PCS, SRS, Operator)• Deployed at the Customer hierarchy node	When the first site dial plan is created for a particular customer
CustomerFONet-Feature-Vx-SCH	<ul style="list-style-type: none">• Contains partitions, calling search spaces, and translation patterns necessary to implement the Forced OnNet feature used during Class of Service creation to block or allow calls based on call type (for example, International, National, Mobile, Service, PRS, Free Phone, PCS, SRS, Operator)• Deployed at the Customer hierarchy node	When the first site dial plan is created for a particular customer

Schema Name	Description	When Deployed
CustomerToDCLIPR-Feature-Vx-SCH	<ul style="list-style-type: none">• Contains partitions and translation patterns necessary to implement the Time of Day Calling Line Identification Presentation (CLIP)/Calling Line Identification Restriction (CLIR) feature used during Class of Service creation based on call type (for example, International, National, Mobile, Service, PRS, Free Phone, PCS, SRS, Operator)• Deployed at the Customer hierarchy node	When the first site dial plan is created for a particular customer
FACnCMC-Feature-Vx-SCH	<ul style="list-style-type: none">• Contains partitions and translation patterns necessary to implement the Forced Authorization Code (FAC) and Client Matter Code (CMC) feature used during Class of Service creation to enable or disable FAC and CMC based on call type (for example, International, National, Mobile, Service, PRS, Free Phone, PCS, SRS, Operator)• Deployed at the Customer hierarchy node	When the first site dial plan is created for a particular customer

HcsDefaultAddCustomerSchema	<p>Contains the following:</p> <ul style="list-style-type: none"> • Default time periods for a customer including All Day, Workday (08:00-18:00) and non-Workday (18:00-08:00) • Default time schedules for a customer including All Day, Works Hours (08:00-18:00), and After Hours (18:00-08:00) • Default customer partitions: <ul style="list-style-type: none"> – Pre-InterSiteRouting – InterSiteRouting – Directory Number – Allow Voice Mail – Mapping E164 to Directory Number – DN2DDI for RDPN, CGPN, CNPN – CDPN Transform Patterns – DN2DDI for Emergency – FMC – URI • Default customer calling search spaces: <ul style="list-style-type: none"> – Pre-InterSiteRouting – InterSiteRouting – Directory Number – Calling Party Transformation – Called Party Transformation – Redirected Transformation – Connected Transformation – Ingress from Central Break Out (CBO) – Ingress from Unity • Default Calling Party Transformation Pattern for DN2DDI4RCCN partition (wildcard match) to enable using the calling party's external phone number mask <p>Deployed at the Customer hierarchy node</p>	When the first site dial plan is created for a particular customer
-----------------------------	--	--

Schema Name	Description	When Deployed
HcsDefaultAddDnRangeSchema	Contains translation patterns necessary to route intersite calls based on number routing instance data provided by Directory Number Routing feature Deployed at the Site hierarchy node	When the first site directory number routing instance is added
HcsDefaultAddSiteShortCodeSchema	Contains translation patterns necessary to route site short codes based on data provided by Site Short Code feature Deployed at the Site hierarchy node	When a site short code is added
HcsDefaultAddSiteType1Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Also contains pre-InterSiteRouting, InterSiteRouting, and AllowInternal translation patterns for Type 1 Deployed at the Site hierarchy node	Deployed to Cisco UCM when a Type 1 site dial plan is created
HcsDefaultAddSiteType2Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Also contains pre-InterSiteRouting, InterSiteRouting, and AllowInternal translation patterns for Type 2 Deployed at the Site hierarchy node	Deployed to Cisco UCM when a Type 2 site dial plan is created
HcsDefaultAddSiteType3Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Also contains pre-InterSiteRouting, InterSiteRouting, and AllowInternal translation patterns for Type 3 Deployed at the Site hierarchy node	Deployed to Cisco Unified Communications Manager when a Type 3 site dial plan is created

Schema Name	Description	When Deployed
HcsDefaultAddSite-Type4Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Deployed at the Site hierarchy node	Deployed to Cisco UCM when a Type 4 site dial plan is created
HcsDefaultAddVoiceMailPilot-NumberSchema	Contains the Voice Mail pilot Calling Search Space and Voice Mail service route list Deployed at the Customer hierarchy node	Deployed to Cisco UCM when a voicemail pilot number is created for a customer

HcsDefaultAddVoice-MailE164NumberSchema	Contains the route pattern for an E164 format number associated with a Voice Mail pilot number Deployed at Site hierarchy node	Deployed to Cisco UCM when a voicemail pilot number with an accompanying E164 number is associated to a site
HcsDefaultLboSchema	Contains dial plan elements required for Local Break Out. Deployed at Site hierarchy node	Deployed to Cisco UCM when an LBO gateway is associated to a site

For each country shown in Predefined Country Dial Plans, there is a generic customer-level and a generic site-level country dial plan schema.

Note: The table below <CCC> represents the ISO Three Letter Country Code for the specific country.

Country Dial Plan Schemas

Schema Name	Description	When Deployed
HcsGenericCustomer<CCC>DP-Vx-SCH	Contains the customer-level country dial plan schema Deployed at the Customer hierarchy node	Deployed to Cisco Unified Communications Manager when the first Site Dial Plan for country <CCC> is deployed for a customer for Type 1 to 4 schema groups
HcsGenericSite<CCC>DP-Vx-SCH	Contains the site-level country dial plan schema Deployed at the Site hierarchy node	Deployed to Cisco UCM for each country <CCC> site that is deployed for Type 1 to 4 schema groups

5.9. Emergency and CLI settings

5.9.1. Emergency and CLI settings

Tip: *Use the Action search to navigate Automate*

Overview

Emergency and CLI settings provides a facility for mapping a site-specific CLI (Calling Line Identity) for emergency and non-emergency calls. This allows users to roam using extension mobility and still provide a site-specific emergency number appropriate to the site they have visited.

Note: To access this feature, go to **Emergency and CLI Settings**.

When deploying a Cisco HCS site dialplan, a site-specific emergency number is configured as a default emergency number for all devices at that site. This feature allows users making an emergency call from within their own site to present a CLI of their own individual DDI (Direct Dial In) instead of the site wide emergency CLI.

A CLI mapping and secondary CLI mapping can also be created using this feature. The behavior is controlled through settings that can exist at any hierarchy.

This feature allows a Provider administrator (or higher) to add up to three (3) new calling party transformation patterns to provide specific translation to a DDI for those DN's having a DDI mapping. The transformations are created and deleted when either '1 to 1' or '1 to N' number associations are created and deleted. See [Add E164 association \(N to 1 DN\)](#) and [Add an E164 association \(N to N DN\)](#)

Using the HCS dialplan schema, site wide mapping is provided using a wildcard match to a site specific prefix used only for emergency calls. An example is '*156*!'. This feature may be used to add more specific patterns such as '*156*81214000' in order that transformations to the E164 can take place. DN's that do not have a mode specific match fall back to the wildcard match as previously set, and therefore use the site wide emergency CLI.

Note: There is no requirement to use any schema. This feature can be used wherever transformations are required as part of DN association.

The supported transformation patterns are:

- **Emergency CLI** transformation
- **CLI** transformation
- **Secondary CLI** transformation

A data model contains settings for this feature. A default set of settings is created at the `sys.hcs` hierarchy, which disables all 3 patterns. These settings must be cloned and used at a lower hierarchy to provide the settings required for each hierarchy, that is clone them to the provider level for platform wide settings, or customer level for customer specific settings.

Each of the 3 patterns can be enabled or disabled independently. The following additional controls are available:

- Macro for defining the partition
- Macro for defining the E164 number format
- Macro for defining the DN (pattern) format

The following macros can be used as part of these settings:

- `EmergencyAndCLITransformations_SiteCountryCode` - returns the country code, e.g. 44
- `EmergencyAndCLITransformations_SiteCountryCodeWithPlus` - returns the country code with a plus, e.g. +44
- `EmergencyAndCLITransformations_NationalTrunkPrefix` - returns the trunk prefix, e.g. 0

Each of these macros is country aware and returns the settings appropriate to the site where the DN association is performed.

In addition to these macros, there is a set of pwf context variables that can be used in the settings macros:

- `pwf.e164_number` - the E164 number from the mapping transaction
- `pwf.dn_number` - the directory number from the transaction
- `pwf.sitePrefix` - the site prefix number as used for HCS emergency calling

Note: Only site level associations are supported, no support is provided for linked sites.

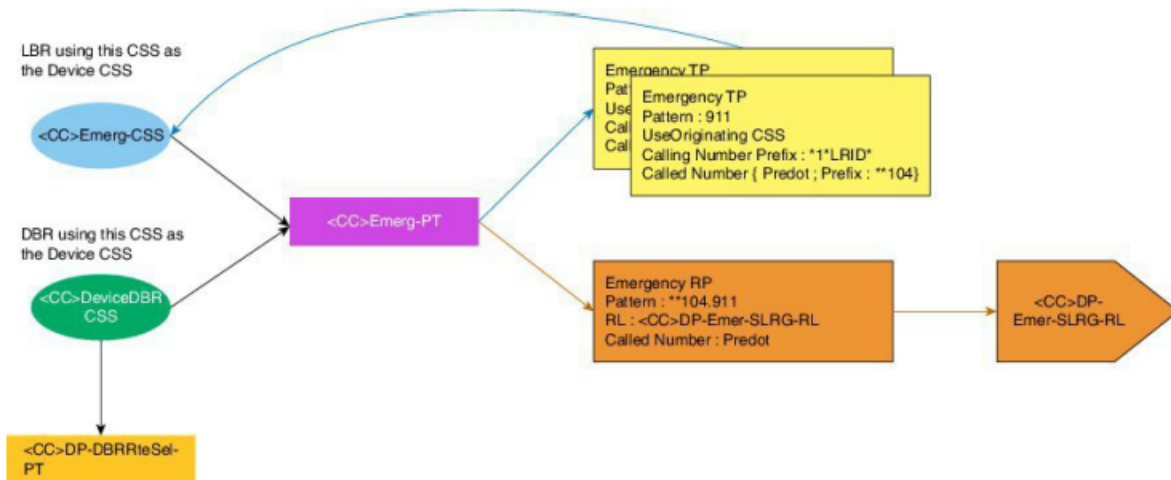
Emergency handling

Emergency handling is device-based. It uses the device pool local route group to handle call routing. When a phone has no Direct Inward Dial (DDI) or the phone has DDI but it is in a remote location, emergency handling uses the site's emergency number.

The implementation is as follows:

- An Emergency partition is created for each site.
- For Device-Based Routing (DBR), a DeviceDBR CSS is created and for Line Based Routing (LBR) an EmerCSS is created. Both CSSs are country and site specific and they contains the Emergency partition.
- Emergency Number translation patterns are added to the emergency partition when a site dial plan is added. This translation pattern leverages the UseOriginatingCSS, prefixes the called number with **104 and the calling number is prefixed with *1*LRID* to uniquely identify the calling site.
- An Emergency route pattern matching **104 is added to the emergency partition with the route list set to use the Device Pool Emergency Local Route Group.

The image illustrates Emergency Calling.



Provisioning emergency calls

Additional provisioning is not required for emergency calls since Automate provisions 911 as part of the United States country scheme, and 999/112 is provisioned as part of the United Kingdom country scheme. For more information, see “Emergency Handling”.

1. When creating a site dial plan, enter the emergency number in the **Emergency Number** field.

This is the Site Emergency Published Number; it is sent if the line that makes the emergency call does not have DDI. Then, if there is a callback, the Site Emergency Published Number is dialed.

2. Ensure that a Local Route group is set up with SLRG-Emer set to the Route group. Refer to “Associate Local Route Groups to a Device Pool”.

5.10. Default dial plan event triggers

5.10.1. Default dial plan event triggers

Tip: Use the Action search to navigate Automate

Overview

In Automate, you can use one of the default, pre-defined dial plan events to trigger a custom workflow as part of your dial plan schema group.

The default events are located on the **Custom Workflow** tab of the **Dial Plan Schema Group** page.

Default dial plan event triggers for custom workflows

Dial Plan Event	When Triggered	Notes
preAddSite	When a new site dial plan is deployed, before the Add Dial Plan workflow is executed	<p>For Type 1 to Type 4 schemas, this triggers a Cisco UCM bootstrap workflow that:</p> <ul style="list-style-type: none"> • Updates the CUCM cluster-wide “Local Route Group for Redirected Calls” service parameter to the value “Local route group of calling party” • Provisions the following clusterwide default local route group names to the CUC: SLRG-Emer, SLRG-FPHN, SLRG-Intl, SLRG-Local, SLRG-Mobl, SLRG-Natl, SLRG-Oper, SLRG-PCSN, SLRG-PRSN, SLRG-Serv, SLRG-SRSN <p>Items in the workflow are executed at the hierarchy node on which the target</p>
		<p>UCM cluster is added to the Automate system.</p> <p>Subsequent sites that are added trigger this workflow, but result in an operation that does nothing if these items have already been applied to the target CUCM cluster.</p> <p>The target cluster for this workflow is determined by the CUCM instance that is contained in the Network</p>
		<p>Device List Reference (NDLR) for the site on which this event was triggered.</p>

Dial Plan Event	When Triggered	Notes
addSite	After the Add Site Dial Plan workflow is executed and the context of the new site dial plan is passed	For Type 1 to Type 4 schemas, this triggers a workflow that adds a default location, region, and device pool at the site hierarchy node on which this event is triggered. The target cluster for this workflow is determined by the Cisco UCM instance that is contained in the NDLR for the site on which this event was triggered.
removeSite	Before the Delete Site dial plan workflow is executed and the context of the site dial plan is passed	For Type 1 to Type 4 schemas, this triggers a workflow that removes the default location, region, and device pool at the site hierarchy node on which this event is triggered. The target cluster for this workflow is determined by the CUCM instance that is contained in the NDLR for the site on which this event was triggered.

Dial Plan Event	When Triggered	Notes
addVoiceMailPilotNumber	When a new voice mail pilot number is added for a customer	<p>For Type 1 to Type 4 schemas, this triggers a Cisco UCM bootstrap workflow that:</p> <ul style="list-style-type: none"> • Creates the voice mail pilot on the target CUCM cluster • Creates a voice mail profile on the target CUCM cluster • Deploys a custom CUC schema to provision the following on CUC: <ul style="list-style-type: none"> – Direct routing rule and forward routing rules based on the new pilot number – The target CUC cluster for this workflow is determined by the CUM instance contained in the NDLR for the site on which this event was triggered <p>The target cluster for this workflow is determined by the UCM instance that is contained in the NDLR for the site on which this event was triggered.</p>
removeVoiceMailPilotNumber	When a voice mail pilot number is a customer	<p>The target cluster for this workflow is determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered.</p> <p>For Type 1 to Type 4 schemas, this triggers a workflow that</p> <ul style="list-style-type: none"> • Removes the voice mail profile and pilot number from CUCM • Undeploys direct and forward routing rules on CUC

Dial Plan Event	When Triggered	Notes
associateVoiceMailServiceTo-Customer	When voice mail service is associated to a customer	<p>The target Cisco UCM and CUC cluster for this workflow are determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered.</p> <p>For Type 1 to Type 4 schemas, this triggers a workflow that</p> <ul style="list-style-type: none"> • Deploys a SIP trunk to CUCM if voice mail service is partitioned or dedicated • Reset the SIP trunk • Deploys a route group to CUCM if voice mail service is partitioned or dedicated that contains the SIP trunk created in the previous step • Deploys a custom CUC schema to provision the port group, ports, route partition, calling search space (CSS), and the user template for voice mail service on the CUC
disassociateVoiceMailService-FromCustomer	When voice is disassociated from a	<p>The target UCM and CUC clusters for this workflow are determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered.</p> <p>For Type 1 to Type 4 schemas, this triggers a workflow that</p> <ul style="list-style-type: none"> • On CUCM, removes Voice Mail service route group and SIP trunk if dedicated or partitioned voice mail service • On CUC, deletes customer-specific route partition, css, user template, ports, and port group.

Dial Plan Event	When Triggered	Notes
addCustomer	When a customer dial plan is added	The target Cisco UCM and CUC clusters for this workflow are determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered. Currently not used for Type to Type 4 schemas
removeCustomer	When a customer dial plan is removed	The target UCM and CUCM clusters for this workflow are determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered. Currently not used for Type 1 to Type 4 schemas
updateCustomer	When a customer dial plan is updated	The target Cisco UCM and CUC clusters for this workflow are determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered. Currently not supported because customer dial plan updating is not supported
updateSite	When a site dial plan is updated	The target UCM and CUC clusters for this workflow are determined by the UCM and CUC instances that are contained in the NDLR for the site on which this event was triggered. Add the updateSite event with the HcsDpUpdateSiteAreaCode-sPWF workflow to update the site dial plan. Currently not supported because site dial plan updating is not supported

Dial Plan Event	When Triggered	Notes
addDnInventory	When an administrator provisions additional specific site	<p>The target UCM cluster for this workflow is determined by the UCM instance contained in the NDLR for the site on which this event was triggered.</p> <p>If a Type 1 or Type 3 dial plan is provisioned, this executes a workflow that creates directory numbers (DNs) where the extension is prefixed with the Site Location Code of the site on which the event was triggered.</p> <p>If a Type 2 dial plan is provisioned, this executes a workflow that creates DNs where the extension is prefixed with the Inter-site Prefix + Site Location Code of the site on which the event was triggered.</p> <p>If a Type 4 dial plan is provisioned, this executes one of the following workflows:</p> <ul style="list-style-type: none"> • Creates DNs where the extension is prefixed with + if the extension entered by the administrator is prefixed with + on the site on which the event is triggered, OR • Creates DN with no prefix; the extension on the site on which the event was triggered is used to create the DNs.
associateLboGateway	When a local gateway is associated with a site.	See associateLboGateway Custom Workflow for detailed information.
unassociateLboGateway	When a local gateway is disassociated from a site.	See unassociateLboGateway Custom Workflow for detailed information.

5.11. Correct calling presentation overwrite on calls forwarded to PSTN

5.11.1. Manual configuration to correct calling presentation overwrite on calls forwarded to PSTN

Tip: *Use the Action search to navigate Automate*

This procedure corrects the situation where calling presentation is incorrectly being overwritten on calls that are forwarded to the PSTN.

In HCS 10.6(1), the presentation setting is based on the following partitions used in the CoS CSS:

- Cu<CustID>-24HrsCLIP-PT or
- Cu<CustID>-WkHrsCLIP-PT or
- Cu<CustID>-24HrsCLIR-PT or
- Cu<CustID>-WkHrsCLIR-PT

Four scenarios are addressed:

- An IP Phone (line CoS CSS includes CLIP-PT) calls the PSTN. The Calling Number Presentation is set to 'Allowed' instead of using the default setting, which might be something else.
- An incoming PSTN Call with calling number presentation set to 'Restricted' is forwarded back to the PSTN where the last redirecting device has a line CoS CSS that includes CLIP-PT. The Calling Number Presentation is set to 'Allowed', and the incoming 'Restricted' is NOT honored
- An IP Phone (line CoS CSS include CLIR-PT) calls the PSTN. The Calling Number Presentation is set to 'Restricted' instead of using the default setting which might be something else.
- An incoming PSTN Call with calling number presentation set to 'Allowed' is forwarded back to the PSTN where the last redirecting device has a line CoS CSS that includes CLIR-PT. The Calling Number Presentation is set to 'Restricted', and the incoming 'Allowed' is NOT honored

The solution is to edit the CLIP-PT partition to not set the Calling Number Presentation to 'Allowed' and then to always use the CoS CSS containing the edited CLIP-PT partition for the Line Call Forward CSS.

1. Log in as the Provider administrator.
2. Go to **Dial Plan Schema**.
3. Select CustomerToDCLIPR-Feature-V2-SCH.
4. Export the schema.
5. Edit the exported schema.
6. Locate the structure that contains "pattern": "\+\\+030.!" and "routePartition": "{{pwf.HCSDpUniqueCustomerPrefixMCR}}-24HrsCLIP-PT".
7. Delete the lines containing "cgLinePresBit": "Allowed" and "cgNamePresBit": "Allowed".
8. Locate the structure that contains "pattern": "\+\\+030.!" and "routePartition": "{{pwf.HCSDpUniqueCustomerPrefixMCR}}-WkHrsCLIP-PT".
9. Delete the lines containing "cgLinePresBit": "Allowed" and "cgNamePresBit": "Allowed".

10. Import the json file back into Automate.
11. If there are deployed customers, then:
 - a. Log in as the Provider administrator.
 - b. Go to **Translation Patterns**.
 - c. Filter on Translation Pattern '++030.!' and if possible Partition ending with CLIP-PT.
 - d. Edit each pattern in the partition ending with CLIP-PT.
 - e. Click the **Calling Party Transformations** tab.
 - f. Change the Calling Line ID Presentation and Calling Name Presentation to 'Default'.
 - g. Click **Save**.
12. Use the CoS CSS that contains the edited CLIP-PT for the Line Call Forward CSS.

5.12. Global settings

5.12.1. Global settings

Tip: *Use the Action search to navigate Automate*

Overview

Administrators (Provider level and up) may configure global settings for customizations that apply at a specific hierarchy only or across all hierarchies in the system.

On each tabbed page in Global Settings, a read-only field below the choice drop-down displays the current setting for your system. Options are:

Inherit	The service is enabled/disabled based on the setting at the hierarchy above the current one.
Yes	The service is enabled at the current hierarchy.
No	The service is disabled at the current hierarchy.

To change inherited settings, see *Changing inherited settings*.

Update Global Settings

Global settings are configured on the tabs of the Global Settings page:

- *Number Inventory*
- *Number Inventory Alerting*
- *Microsoft Licensing Alerting*
- *Webex App*
- *Pexip Conference*

- Email
- Phones
- Voicemail
- User
- Flow Through Provisioning
- Enabled Services
- *Enabled Solutions*

Number Inventory

The table describes the global settings for the Number Inventory:

Field	Description
Enforce HCS Dialplan Rules	When enabled, dial plan workflows enforce HCS Rules when provisioning Customers, Countries, Site and so on. Default = Inherit . If your deployment uses a custom or specific dial plan that does not conform to the HCS rules, this setting should be set to No (False).
Prevent Duplicate Numbers	This setting displays only at hierarchies above site or or linked site levels, and only when Microsoft is enabled for your system (via the Enabled Services tab in Global Setting). When available, the setting is enabled only when <i>Enforce HCS Dialplan Rules</i> is set to <i>No</i> (disabled), else, the field is read-only. In Microsoft environments, defines whether to allow the creation of duplicate numbers at sites in Automate when syncing in and provisioning users, or when creating number ranges. Default is <i>No</i> (duplicate numbers are allowed). The system checks the setting for <i>Enforce HCS Dialplan Rules</i> before applying the <i>Prevent Duplicate Numbers</i> logic. When enabled, the system enforces unique number validation throughout the hierarchy.
Include the Number Inventory description in all number drop-downs	Defines whether descriptions for the numbers (which can be added when the number inventory is managed via Number Management), display along with the numbers in the drop-down lists. For example, let's say you have a number and its description as follows: <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 User). The default is No.
Include the Number Inventory vendor in all number dropdowns	Defines whether vendor names for the numbers show in number dropdown as an option. For example, a number 982017206 (which is from Microsoft vendor) will display as 982017206 [Microsoft] in the drop-down list.

Field	Description
Include the Number Inventory type in all number dropdowns	Defines whether number types for the numbers show in number drop-down as an option. For example, a number 982017206 (which is from Microsoft vendor and is of type OperatorConnect will display as 982017206 [OperatorConnect] in the drop-down list.
Enable Number Inventory Cooling	Defines the availability of numbers in the system when a phone, user, or service associated with the number is deleted, and the number is no longer associated with these entities. Options are: <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.
Enable Filters	Enables/disables custom number inventory filters at the current hierarchy. Shipped inventory filters can't be enabled or disabled as these reside at sys level. When enabled, custom and shipped inventory filters display in a drop-down list on forms such as Quick Add User, Onboard User (to add a user from a profile), Multi vendor service user move, Cisco Advanced User, Phones, Extension Mobility, and Single Number Reach. Options are: <ul style="list-style-type: none"> • Inherit (default): When set to True, custom inventory filters are enabled or disabled based on the setting defined at a higher level in the hierarchy. • Yes (True) Enables custom inventory filters at the hierarchy. When set to True, select the inventory filters to make available for selection in relevant drop-down lists, either shipped and custom inventory filters or all enabled inventory filters. You can view the available filters at a hierarchy via Manage Filters. When enabled, you can enable or disable specific filters at specific hierarchies via Manage Filters. • False (No) Custom and/or cloned shipped filters are disabled at the hierarchy.

Field	Description
Filter Group	<p>When Enable Filters is set to Yes, the selected filter defines the number inventory filters available in the the drop-downs for choosing a number inventory filter. Options are:</p> <ul style="list-style-type: none"> • Inherit • Shipped Enabled Filters • Custom Enabled Filters • All Enabled Filters (default) <p>When set to <i>Inherit</i>, the value displays for the filter group that will be used from a higher level in the hierarchy.</p> <p>Custom enabled filters will only display in the drop-downs if these exist and are enabled at the hierarchy you're working at.</p> <p><i>All Enabled Filters</i> includes all custom and shipped filters, provided they are enabled at the hierarchy you're working at.</p>

Home > Search Results > Global Settings

Number Inventory | Number Inventory Alerting | Microsoft Licensing Alerting | Webex App | Pexip Conference | Email | Phones | Voicemail | User

Enforce HCS Dialplan Rules	No
	No
Prevent Duplicate Numbers	Inherit
	No
Include the Number Inventory description in all number dropdowns	Inherit
	No
Include the Number Inventory vendor in all number dropdowns	Inherit
	No
Include the Number Inventory type in all number dropdowns	Inherit
	No
Enable Number Inventory Cooling	Inherit
	No
Number Inventory Cooling Duration (Days)	Inherit
	30
Enable Filters	Inherit
	Yes
Filter Group	Inherit
	All Enabled Filters

Related topics

- Number Cooling in the Core Feature Guide
- Number Cooling Auto Expiry Schedule in the Advanced Configuration Guide
- Manage Number Filters in the Core Feature Guide
- Prevent duplicate numbers in the Core Feature Guide

Number Inventory Alerting

This tab configures the global settings for number inventory alerting, which defines how alerts may be raised once the number inventory is running low.

The table describes the settings on this tab:

Field	Description
Enable Alert on Available Numbers	By default, this setting is set to Inherit . However, it will not inherit the setting from higher up the tree unless it is explicitly set to Yes or No . Inherit in this instance just means it is <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

Microsoft Licensing Alerting

The table describes the global settings for the Microsoft Licensing Alerting:

Field	Description
Enable Alert on Microsoft Licenses	When enabled, alerts will be raised and optionally emailed if the Microsoft license availability threshold is reached at the hierarchy. Default = Inherit . Note that this setting requires that Enable Microsoft User License Enforcement is enabled under the User tab. Refer to Availability Threshold Percentage below.
Availability Threshold Percentage	Defines a percentage of remaining Microsoft licenses at which an alert is raised. Percentages are available in the drop-down lists: 10, 15, 20, 25. Default = Inherit .
Enable Email Group	Defines whether an email group will receive alerts. Default = Inherit . If set to Yes at the hierarchy, the Alert Email Group drop-down list provides available email groups.
Alert Email Group	The selected email group to receive alerts for Microsoft licenses consumption above the defined threshold. Default = Inherit .

Related topics

- Microsoft License Management and Alerting in the Core Feature Guide
- Email in the Core Feature Guide

Webex App

This tab configures the global settings for Webex App.

The table describes the fields on this tab:

Field	Description
Retain a Webex App User when a subscriber is deleted	Defines whether to delete Webex App user when a user is deleted. Default is No .
Send notification when the Webex App Refresh Token expires	Defines whether a notification is sent when the Webex App refresh token expires for a specified customer. A SNMP trap and Webex App message is sent to recipients configured in the email group.
Webex App Refresh Token expires threshold (in seconds)	The max threshold (in seconds) for when to send a SNMP trap to the SNMP (if Send SNMP trap message when the Webex App Refresh Token expires is enabled). The default is 172800 seconds, which is two days.
Automatically apply default calling behavior on Webex App user data sync	Whether to apply default calling behavior (set up in Customer settings), to new Webex App users synced in to Automate. Default is No.
Generate and send Webex App User CSV file via Webex App message	Whether to generate a CSV file on create/update of Webex App user. Default is No. If enabled (Yes), the CSV file is sent via Webex App to a predefined list of recipients.
Email group containing recipients of the generated Webex App user CSV file	The group of recipients of the Webex App message with the generated CSV file. The email group is set up on the Email Groups menu.
Send manual Webex App Workspace configuration steps via Webex App message	Whether manual configuration steps (on Webex App Control Hub) are to be sent on create/update of a Webex App workspace. Default is No . If enabled, the steps are sent via a Webex App message.
Email group containing recipients of the manual Control Hub steps	Email group recipients of the Webex App message containing the manual configuration steps.
Quick Add Group for Hybrid Calling Workspace Unified CM users	The Quick Add Group to use when creating dummy CUCM users with line and device for Webex App workspace hybrid calling.
Enable Cisco Webex Contact Center Model References	Defines whether to enable retrieval and display of Cisco Webex Contact Center device model references from the Webex Control Hub. It is recommended that you enable this setting in the Global Settings only for any customer where you want to retrieve the reference details. This is to prevent a performance impact on customers where the setting is not required.

Related topics

- Quick Add Groups in the Core Feature Guide
- Email in the Core Feature Guide
- Email Groups in the Core Feature Guide
- Create Webex App Service in the Core Feature Guide

Pexip Conference

This tab configures the global settings for Pexip Conference.

The table describes the settings on this page:

Field	Description
Retain a Pexip Conference when a user is deleted	Defines whether the Pexip conference set up from the user interface is to be removed when the user is deleted. By default the setting is inherited from the hierarchy level directly above the current one.

Email

This tab configures the global settings for Email.

The table describes the settings on this page:

Field	Description
Allow welcome email to be sent to user after Quick Add User	Defines whether an email is sent to a user when added via Quick Add User. The default is No . When set to Yes , and a SMTP server is set up via Apps Management), then selecting the option to send an email when using Quick Add User, a welcome email is sent to the new user.

Related topics

- SMPT Server in the Core Feature Guide
- Email in the Core Feature Guide

Phones

This tab configures the global settings of phones for a site.

Note: These settings only apply to phones within the same site; both the re-added phone and the existing phone must be on the same site.

The table describes the phone global settings on this tab:

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).</p> <p>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 Quick Add User bulk load or when updating a user.</p> <p>When set to <i>Yes</i>, a system check verifies whether the phone exists and/or if it is already assigned (whether <code>ownerUserName</code> field is populated):</p> <ul style="list-style-type: none"> • If the phone exists and is assigned to a different user, the transaction fails. • If the phone exists and is unassigned, the existing phone is deleted, the phone is re-added, and is assigned to the user you're adding or updating. • If the phone exists and is already assigned to the user you're working with. The system performs an update.
Retain Desk Phones when Subscriber is deleted	<p>Defines whether a user's associated desk (hard) phones (phones prefixed with SEP or BAP) are deleted or retained when that user is deleted.</p> <p>When set to <i>Yes</i>:</p> <ul style="list-style-type: none"> • The deleted user's hard phones are retained. • The deleted user's soft phones (such as Jabber devices) are deleted. • An additional field displays (Update the Retained Desk Phone with Configuration Template), which allows you to define whether retained phones are updated via a CFT once the user is deleted. <p>Default is <i>Inherit</i> (set to <i>No</i>).</p> <p>This setting defines hard phone delete/retain behavior for any method of deleting a user, for example, delete user via the User's list view, or delete user in LDAP import, purge or sync (where delete or purge mode is automatic).</p> <p>You can view the hard phones associated with the user on the Phones tab in the user settings.</p>
Update the Retained Desk Phone with Configuration Template	<p>This field displays only when Retain Desk Phones when user is deleted is set to Yes (True).</p> <p>Defines whether to update retained hard phones via a configuration template (CFT) when the associated user is deleted.</p> <p>This feature ships with a default CFT (<code>RemoveOwnerFromPhoneCFT</code>), which clears the phone's Owner User ID if the phone is retained when deleting the associated user. You can choose a different CFT for the update step, if required.</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 page (Existing Phone tab, Device Name drop-down), and on Quick Add User, allowing you to search by phone description when choosing a phone from the drop-down. In the same way, when the additional information option is set to either <i>First Line</i> or <i>Description + First Line</i> , you can search for or choose phones based on this criteria.
Prevent Duplicate MAC Addresses for Cisco Phones	Options are Yes, No, Inherit. Default is <i>Inherit</i> . For any transaction adding a Cisco phone, if this setting is enabled, the transaction will fail with a message: Phone already exists with name: if any phone is found containing the same MAC address within all clusters in a customer or reseller.

Related topics

- Replace Phone in the Core Feature Guide.
- Quick Add User for Cisco UCM Users in the Core Feature Guide.
- User, Phones tab in the Core Feature Guide

Voicemail

This tab configures the global settings for voicemail.

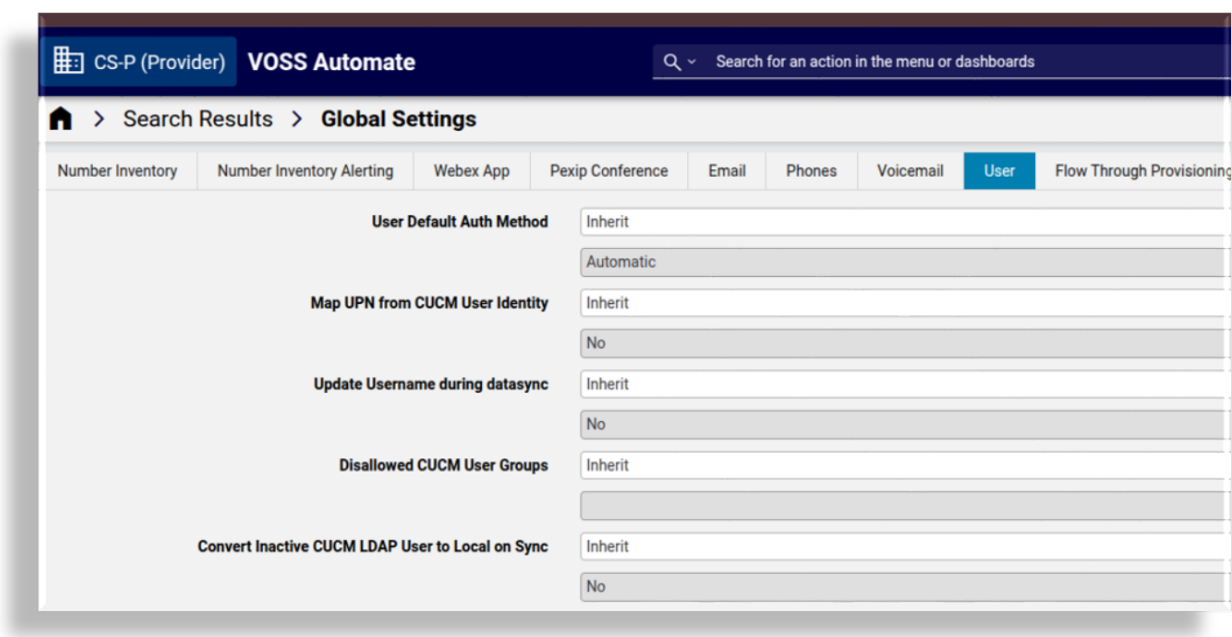
The table describes the settings on this tab:

Field	Description
Retain a (Cisco) Voicemail Account when a user is deleted by data sync only	Defines whether to retain a Cisco (UCM) user's voicemail account when the user is deleted. Default is Yes (true). When set to Yes, the CUCM user's voicemail account is retained when the user is deleted and user sync is executed.

User

This tab configures the global settings for users.

Note: When a user is either synced into or added manually on Automate, these settings apply by default. The settings can however be modified when adding a user via **User Management**.



The table describes the settings on this tab:

Field	Description
User Default Auth Method	The default authentication method to use when a user is synced in or added manually. The default is Local (inherited).
Map UPN from CUCM User Identity	Maps the Microsoft Azure UserPrincipalName (UPN) attribute to CUCM userIdentity attribute - used in Cisco-Microsoft hybrid configurations where the same user ID is on every user account (MS Teams, CUCM, etc.). If enabled, the CUCM user's userIdentity attribute is used for the import of MS teams CsOnlineUser and MS 365 Msol user instances. The default is No (inherited).
Update Username during data-sync	Defines whether to update the existing VOSS username when a new associated user is imported via a sync.
Disallowed CUCM User Groups	Defines the user groups (one or more) that admins will not be allowed to assign to user. This is to prevent users being incorrectly assigned elevated permissions to system resources that are reserved for users in the groups you specify here. Fill out the user group names in a colon-separated format, for example, <i>Standard CUCM SuperUser:MyGroupName</i>
Enable Microsoft User License Enforcement	Defines whether to Microsoft license allocation is enforced at hierarchy levels. Refer to the related topic below. Default is Inherit .
Convert Inactive CUCM LDAP User to Local on Sync	Defines whether to convert CUCM users that would normally be automatically deleted by the CUCM, to be converted into CUCM Local users during a data sync of CUCM. When disabled (default), users that have been in status "Inactive LDAP Synchronized User" for more than 24 hours are automatically deleted by the CUCM. These users and their services are then deleted from Automate on the next CUCM data sync. When enabled, users that have changed their status to "Inactive LDAP Synchronized User" are converted to "Enabled Local Users" on the next CUCM data sync. The data sync of the CUCM must occur within 24 hours of the users becoming inactive otherwise, CUCM will still delete them.
Retain User at Site after MS Off-board User	Defines whether to retain a user at a site instead of moving the user back to customer level when performing the task: Quick Offboard User. The default is No (inherited).

Related topics

- User Authentication Methods in the Core Feature Guide.
- Microsoft License Management and Alerting in the Core Feature Guide
- Convert user type CUCM-LDAP to CUCM Local in the Core Feature Guide.
- Microsoft User Management, Offboard User in the Core Feature Guide.

Flow Through Provisioning

This tab defines global settings for sync with flow through provisioning.

>

Search Results

>

Global Settings

Number Inventory

Number Inventory Alerting

Microsoft Licensing Alerting

Webex App

Pexip Conference

Email

Phones

Voicemail

User

Flow Through Provisioning

Enable Move & Flow Through Provisioning

Inherit

False

Enable Move & Provisioning (Add Sync)

Yes

No

Flow Through Provisioning Criteria (Add Sync)

Inherit

Enable Move & Provisioning (Update Sync)

Yes

No

Number Assignment Control (Update Sync)

Keep Existing Number

keep_existing

User Profile Control (Update Sync)

Inherit

Default

The table describes the settings on the Flow Through Provisioning tab/panel:

Field	Description
Enable Move & Flow Through Provisioning	Defines whether move and flow through provisioning is enabled. The default is No.
Enable Move & Provisioning (Add Sync)	Enabled only when Enable Move & Flow Through Provisioning is enabled. Defines whether move and flow through provisioning on <i>Add sync</i> is enabled. The default is No.
Flow Through Provisioning Criteria (Add Sync)	Enabled only when Enable Move & Flow Through Provisioning is enabled. Used <i>only</i> for adding and onboarding users. Defines the default criteria applied in an <i>Add sync</i> when moving and provisioning a user with flow through provisioning. The user is synced in, moved to a site, and provisioned with relevant serves in one step, based on the flow through provisioning criteria.
Enable Move & Provisioning (Update Sync)	Microsoft users only. Allows the system to automatically move an existing non-hybrid, Microsoft-only user, from one site to a new site, with their services and a new line, in a scheduled or manually triggered sync. When set to Yes, triggers display of these additional fields to apply controls for move using between sites, and provisioning in an update sync: <ul style="list-style-type: none"> • Number Assignment Control (Update Sync) • User Profile Control (Update Sync) <hr/> Important: Update syncs for move and flow through provisioning execute <i>only</i> on users that are already at Site level. These are users who have already been provisioned at a site and their settings on Azure have changed, therefore requiring a move to another site and, if relevant, changes to their provisioning at the new site. Users synced in at Customer level as Msol users aren't eligible for flow through provisioning. To move and automatically provision these users you can either purge them and sync them in again in an Add sync with flow through provisioning, or manually configure and move them. <hr/>
Number Assignment Control (Update Sync)	Displays only when Enable Move & Provisioning after Update Sync is set to Yes. Update sync only. Defines whether a user keeps their existing number or is assigned a new number when moved from one site to another site. Options are <i>Inherit</i> (from the hierarchy settings above this one), <i>Keep Existing Number</i> (default), or <i>Assign New Number</i> . Note that this is a global setting at the hierarchy where you're applying the setting so all users updated in this move and sync will either inherit settings, or keep their numbers, or be assigned new numbers.
User Profile Control (Update Sync)	Displays only when Enable Move & Provisioning after Update Sync is set to Yes. Update sync only. A single default profile used <i>only</i> in update syncs with flow through provisioning to apply criteria for moving the user. In an update sync, only this user profile applies for the move. The Flow Through Provisioning Criteria setting on this tab/panel applies only for <i>add</i> syncs.

Related topics

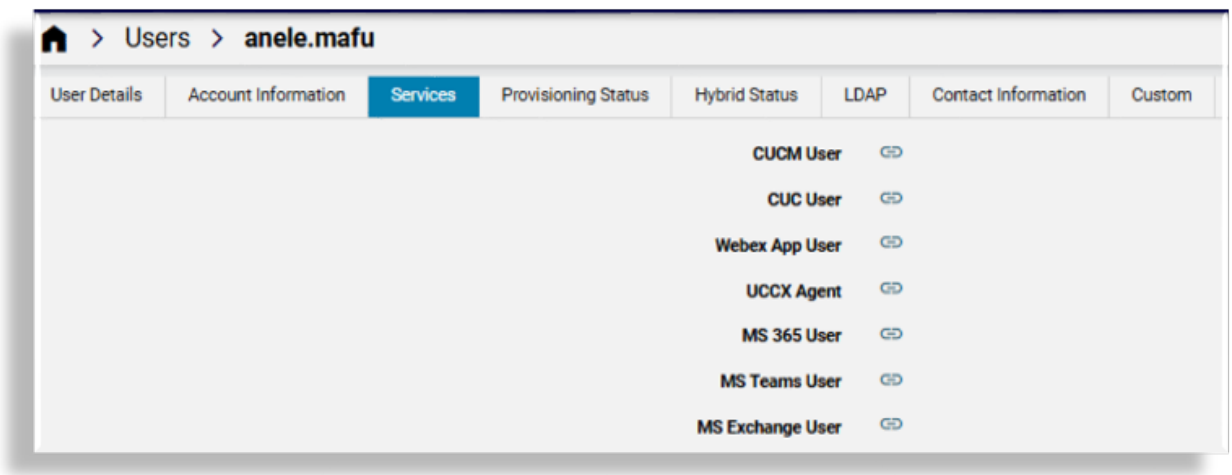
- Flow through provisioning (FTP) in the Core Feature Guide.
- Move Microsoft user and services in the Core Feature Guide.
- User profiles in the Core Feature Guide

Enabled Services

This tab defines the global settings for enabling/disabling services for different vendors, such as Cisco or Microsoft. Options are Inherit, or Yes/No (True/False).

ng	Webex App	Pexip Conference	Email	Phones	Voicemail	User	Flow Through Provisioning	Enabled Services
<div> <div> Enable Cisco CUCM <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Cisco CUCX <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Cisco WebEx <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Cisco Webex App(Teams) <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Cisco UCCX <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Cisco Broadworks <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Microsoft <input type="text" value="Yes"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Avaya <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Pexip <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Zoom <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Cisco / Microsoft Hybrid <input type="text" value="Yes"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Avaya / Microsoft Hybrid <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Cisco Webex Contact Center <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Cisco UCCE <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable VOSS Phones <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Session Border Controller <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Defender for Office <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Defender for Endpoint <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								
<div> <div> Enable Defender for Identity <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Defender for Cloud Apps <input type="text" value="Inherit"/> </div> <div> <input type="text" value="No"/> </div> </div>								
<div> <div> Enable Operator Connect <input type="text" value="Inherit"/> </div> <div> <input type="text" value="Yes"/> </div> </div>								

Services that are available to users and enabled on this tab display on the **Services** tab of the user's management page. When enabled, an admin can click the link to the service details to view and update the settings for that service. For services that the user isn't using, you can disable the service (select *No*) on this tab so that it won't display on their user management **Services** tab/panel.



When provisioning services from two or more vendors, the global setting is the first of a number of system verification checks. For example, when the **Enable Cisco CUCM** global setting is set to **Yes** (enabled), the administrator can provision a user with new CUCM services (such as a Cisco phone, Jabber, and extension mobility), only if the CUCM device check (server installed), entitlement profile check, and field display policy check all pass the verification check. In the same way, if for example, the **Enable Microsoft** global setting is set to **No** (disabled), and all other checks are set to enabled, existing Microsoft services can be viewed but new Microsoft services cannot be provisioned.

Note: By default, for new installs, the global setting for the following services are inherited from higher levels in the hierarchy (Inherit set to True/enabled):

- Cisco CUCM
- Cisco CUCX
- Cisco WebEx
- Cisco Webex App
- Cisco CCX

When upgrading to a version of the system that allows multi vendor and hybrid users, the default setting for services other than these 5 services is *Inherit* (False).

To provision services to new users (added after an upgrade), you will need to enable the vendor service in global settings.

The table describes services that can be enabled/disabled on this tab:

Setting	Description
Enable Cisco CUCM	Enables/disables Cisco CUCM services. The default is <i>Yes</i> . When set to <i>Yes</i> , allows an admin user to provision a user with new CUCM services, such as a Cisco phone, Jabber, and Extension Mobility, provided the server is installed, and the entitlement profile and field display policy pass a verification check.
Enable Cisco CUCX	Enables Cisco CUCX (Unity) services. The default is <i>Yes</i> .
Enable Cisco WebEx	Enables/disables Cisco WebEx services. The default is <i>No</i> .
Enable Cisco Webex App (Teams)	Enables/disables Cisco WebEx App (Teams) services. The default is <i>No</i> .
Enable Cisco UCCX	Enables/disables Cisco UCCX (Contact Center Express) services. The default is <i>No</i> .
Enable Cisco Broadworks	Enables/disables Cisco Broadworks services. The default is <i>No</i> .
Enable Microsoft	When enabled, allows provisioning of Microsoft services. The default is <i>No</i> .
Enable Avaya	Enables/disables Avaya services. The default is <i>No</i> .
Enable Pexip	Enables/disables Pexip services. The default is <i>No</i> .
Enable Zoom	Enables/disables Zoom services. The default is <i>No</i> .
Enable Cisco/Microsoft Hybrid	Enables/disables Cisco/Microsoft hybrid services. The default is <i>No</i> . When enabled, Automate allows for provisioning users and services from both Cisco and Microsoft devices, and makes available an admin user parent menu called Hybrid Cisco-Microsoft Management , and associated access profiles. For details, see <i>Hybrid Cisco-Microsoft Management</i> in the Core Feature Guide.
Enable Avaya/Microsoft Hybrid	Enables/disables Avaya/Microsoft hybrid services. The default is <i>No</i> .
Enable Cisco Webex Contact Center	Enables/disables Cisco Webex Contact Center services. The default is <i>No</i> .
Enable Cisco UCCE	Enables/disables Cisco UCCE services. The default is <i>No</i> .
Enable VOSS Phones	Enables/disables VOSS phones services. The default is <i>No</i> .
Enable Session Border Controller	Enables/disables Session Border Controller services. The default is <i>No</i> .
Enable Defender for Office	Enables Microsoft Defender for Office - security services for Office 365
Enable Defender for Endpoint	Enables Microsoft Defender for Endpoint - various devices
Enable Defender for Identity	Enables Microsoft Defender for Identity - for identity related threats
Enable Defender for Cloud Apps	Enables Microsoft Defender for Cloud - cloud security tools
Enable Operator Connect	Enables Microsoft Operator Connect for Providers in Automate. When set to <i>Yes</i> (enabled), displays Operator Connect settings in <i>Additional Apps</i>

Related topics

- Microsoft Defender for Office security management and policies

Enabled Solutions

This tab lists solutions that can be enabled in your system, provided you have the necessary licenses.

Note: As at the release of 25.3, the following solutions are available and enabled by default (provided you have the required licenses):

- **UC Automation:** Offers the same functionality as shipped in Automate pre-25.3.
- **Email:** Relevant for Microsoft customers using Automate for MS Exchange pre-25.3.

Deployment of the following solution capabilities is reserved for future development: UC Monitoring, UC Analytics, Security, License Management, Meetings Rooms

From 25.3, admins setting up a Microsoft tenant can add the tenant, select required solutions, and add the permissions for these solutions to a single application (app) registration directly in the customer tenant. When enabling two or more solutions, you will need to create your own app registration in this way, and add permissions to the app registration in the form of an uploaded certificate and/or a secret. Some solutions will require a certificate and others will need a secret.

Permissions required, by solution:

- UC Automation: Certificate
- Email: Certificate
- UC Monitoring: Secret
- UC Analytics: Secret
- Security: Certificate
- License Management: Certificate
- Meetings Rooms: Certificate

At the time of writing (25.3), shared central app registration can still be used provided you only have a single solution enabled; that is, *UC Automation* or *Email*.

Home

> Search Results

> Global Settings

< Exip Conference

Email

Phones

Voicemail

User

Flow Through Provisioning

Enabled Services

Enabled Solutions

Pull Sync Delete

Enable UC Automation Solution

Inherit

X

▼

Yes

Enable UC Monitoring Solution

Inherit

X

▼

No

Enable UC Analytics Solution

Inherit

X

▼

No

Enable Email Solution

Inherit

X

▼

Yes

Enable Security Solution

Inherit

X

▼

No

Enable License Management Solution

Inherit

X

▼

No

Enable Meeting Rooms Solution

Inherit

X

▼

No

Pull Sync Delete Thresholds

The Pull Sync Delete Threshold settings on the Enabled Services tab allow you to define the maximum number of items that may be deleted during a sync to protect against unwanted sync deletions. You can adjust the default values if needed. Sync will fail if the threshold is reached.

Setting	Description
Pull Sync Delete Threshold for CallManager	Blocks CallManager deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for LDAP	Blocks LDAP deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for MExchangeOnline	Blocks MExchangeOnline deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for MSGraph	Blocks MSGraph deletes if calculated number of local deletes exceeds the threshold. Default is 20.
Pull Sync Delete Threshold for MSTeamsOnline	Blocks MS-TeamsOnline deletes if calculated number of local deletes exceeds the threshold. Default is 20.
Pull Sync Delete Threshold for Spark	Blocks Spark deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for UnityConnection	Blocks UnityConnection deletes if calculated number of local deletes exceeds the threshold. Default is 50.
Pull Sync Delete Threshold for Zoom	Blocks Zoom deletes if calculated number of local deletes exceeds the threshold. Default is 50.

Related topics

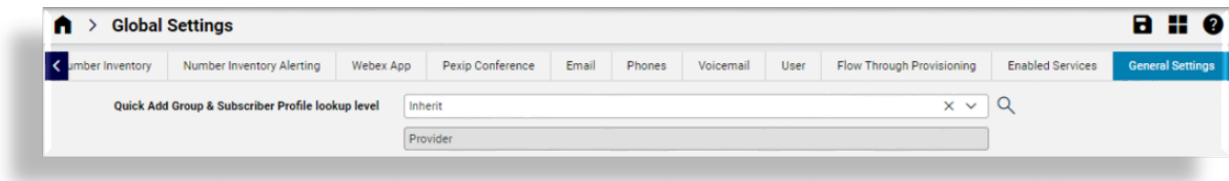
- Multi vendor users in the Core Feature Guide
- Role-based access for multi vendor users in the Core Feature Guide
- Configure multi vendor users in the Core Feature Guide
- Hybrid Cisco-Microsoft Management in the Core Feature Guide

General

This tab defines general global settings to manage system behavior.

The table describes services that can be enabled/disabled on this tab:

Setting	Description
Quick Add Group & User Profile lookup level	<p>Specifies the hierarchy level up to which Quick Add Groups and user profiles will be searched for. The default is Provider level. (sys and hcs levels are not available.)</p> <p>When a lookup level is set, selections of available QAGs and user profiles will be restricted upwards to this lookup level.</p> <p>If you have hybrid customers (customers using both Cisco and Microsoft, for example), you can create hybrid-specific user profiles for those hybrid customers, then set the lookup level for those customers to <i>Customer</i> level so that they will have available a hybrid user profile in the drop-down at that customer hierarchy.</p>



Changing inherited settings

- For numeric inherited values, for example, for “Number Inventory Cooling Duration (Days)” or “Webex App Refresh Token expires threshold (in seconds)”, you can overwrite the word “Inherit” with the required value, for example, 45, and save your changes. If the inherited value is already overwritten, for example, the value is already 45, then overwrite this value with the new value.
- For inherited values that are Yes/No (True/False), select an alternative from the drop-down (either Yes, No, or Inherit). This may change the current value.

5.13. Email

5.13.1. Add a SMTP server

Tip: *Use the Action search to navigate Automate*

This procedure adds a SMTP server at a hierarchy level.

Prerequisites:

- Enable email in the Global Settings (Email tab).

Perform these steps:

1. Log in to the Admin Portal.
2. Choose the relevant hierarchy.

Note: Configure the SMTP server at the hierarchy where you want to allow VOSS Automate to send email messages.

You may only set up one SMTP server at each hierarchy level. The SMTP server will be available at the current hierarchy and below. For example, for a SMTP set up at a specific customer, the sites below that customer can use that SMTP server.

3. Go to **SMTP Server**.
4. Click the Plus icon (+) to add a new SMTP server.
5. On the **SMTP Server** page, fill out details for the new SMTP server:

Field	Description
Name	The SMTP server name.
Description	A description for the email account.
Port	The port number.
Secure	Relevant only for SSL connections to the SMTP server. Select the checkbox (enable) to use the SSL protocol for connections to the SMTP server. Default is disabled (checkbox is left clear), for TLS and unsecure logins to the SMTP server.
Username	The username credential for establishing a connection to the SMTP server.
Password	The password credential for establishing a connection to the SMTP server.

6. Save your changes.

Related topics

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

5.13.2. Email

Tip: *Use the Action search to navigate Automate*

Overview

Provider administrators can test email messages and manage email templates, provided an email SMTP server is set up, and when emails are enabled via the **Email** tab of the *Global settings*.

Email functionality is available for the following:

Component	Description
Quick Add User - Cisco (QAS)	Enable email functionality via Global Settings > Email tab, then select a checkbox in QAS to send a welcome email to new users added via QAS.
Quick User - Microsoft	Enable email functionality via Global Settings > Email tab, then select a checkbox in Quick User to send a welcome email to new users added via Quick User.
File Transfer Destinations	Configured by high level system administrators to transfer audit data for licensing. See the Licensing and Data Export Guide.

Related topics

- *Add a SMTP server*
- *Global settings*

Send test email

On the **Send Test Email** page you can allow an email message to be sent to and from a specified email address, and select an email HTML template to test in the email body.

Email HTML templates

You can view and work with email templates on the **Email HTML Templates** page.

Email HTML templates contain placeholders for the email subject and body text, in HTML markup. The HTML markup can be:

- Previewed by using the **Preview** menu option in the editor
- Modified as required.

Default email templates

By default, the system provides the following email templates:

Note: When adding a HTML template from the list view, the **Name** can only be “Test Email Template”, “Quick Add User”, or “Number Inventory Alerting”.

Default email templates	Description
Test Email Template	This default template is read-only. You can't modify it or change its name. To use this template, you can clone it to your hierarchy and customize the clone.
Quick Add User	This default template is read-only. You can't modify it or change its name. To use this template, you can clone it to your hierarchy and customize the clone. You can use this template only if the setting is enabled via the Global Settings. Values from the Quick Add User input form can be used to populate the template by adding variables to the HTML template.
Number Inventory Alerting	This default template is read-only. You can't modify it or change its name. To use this template, you can clone it to your hierarchy and customize the clone. You can use this template only if the setting is enabled via the Global Settings. Values from Number Inventory Alert message can be used to populate the template by adding variables to the HTML template.

Quick Add User email template variables

Values from the **Quick Add User** page can be used to populate the Quick Add User email template by adding variables to the HTML template.

The table lists the available variables for the **Cisco** Quick Add User email template:

Field name on input form	Variable available in HTML
Username	{{ pwf.EMAIL.username }}
First name	{{ pwf.EMAIL.firstname }}
Last name	{{ pwf.EMAIL.lastname }}
One time password	{{ pwf.EMAIL.password }}
One time PIN	{{ pwf.EMAIL.pin }}
Access Code	{{ pwf.EMAIL.phone_access_code }}
Email	{{ pwf.EMAIL.email }}
Extension	{{ pwf.EMAIL.extension_number }}
Mobile Number	{{ pwf.EMAIL.mobile_number }}
Entitlement Profile	{{ pwf.EMAIL.entitlement_profile }}
Phone Type	{{ pwf.EMAIL.phone_type }}
Phone Names	{{ pwf.EMAIL.phone_names }}
Jabber Device Names	{{ pwf.EMAIL.jabber_names }}
Extension Mobility Name	{{ pwf.EMAIL.extensionmobility_name }}
External E.164 number	{{ pwf.EMAIL.e164 }}

Note: When sending the welcome email to users added via Quick Add User, if there is more than one E.164 number associated with the user's extension, only the primary E.164 number displays. If there are no E.164 numbers associated with the user's extension, then no E.164 number value displays.

The table describes the default variables for the **Microsoft** Quick user email template:

Field name on input form	Variable available in HTML
Username	{{ pwf.EMAIL.username }}
First name	{{ pwf.EMAIL.first_name }}
Last name	{{ pwf.EMAIL.last_name }}
One time password	{{ pwf.EMAIL.password }}
Email	{{ pwf.EMAIL.email }}
Extension	{{ pwf.EMAIL.line_uri }}
Mobile Number	{{ pwf.EMAIL.mobile_phone }}
Phone Number	{{ pwf.EMAIL.phone_number }}

Example user details you can add to your QAS HTML template:

```
<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
```

Email groups

You can manage a group of email recipients via the **Email Groups** page:

- Add a name and a description to create the group
- Add a list of email addresses

The email group is now available and can be selected where email groups are selected.

See for example [Global settings](#), for:

- Webex App email to specify recipients of generated CSV files.
- Number Inventory Alerting - email group to receive alerts.

Related topics

- *Add a SMTP server*
- *Global settings*

6. Basic call flow overview

6.1. Intra-site extension dialing

Within a site, users can make calls to other users by dialing only the extension part of the directory number. Although the lines are provisioned as (ISP)+SLC+Extension number, when the user dials only a subset of these digits, the dial plan treats the call as an intra-site call, and prefixes the called number with the ISP+SLC to route the call.

Note: Intra-site calls can also be dialed as ISP+SLC+Extension.

6.2. Multi-site customer with ISP included in SLC

The Intersite Prefix (ISP) is included as the first digit of the site code. Currently, Automate does not support the ISP as a separate component for the directory number construction. Without ISP in the DN, a CTI application such as Corporate Directory feature has problems; the DN returned from the Corporate Directory must be manually manipulated before a call can be placed. To work around this issue, Cisco recommends that the ISP be included as the first digit of a Site Location Code (SLC).

Site Customer with ISP in SLC

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	<ul style="list-style-type: none"> • Extension (for example, 4321) • Site Code + Extension (for example, 81134321) 	<ul style="list-style-type: none"> • Extension • Site Code + Extension 	Intra-Site Calls can be dialed as an extension or as Site Code + Extension. Similarly, the calling party number can be displayed either as an extension or as Site Code + Extension
Inter-Site Dialing	Site Code + Extension (for example, 82551234)	Site Code + Extension	The first part of the Site Code is an ISP
PSTN Dialing	<ul style="list-style-type: none"> • PSTN Prefix + PSTN Number (for example, 919722221234) • E.164 Number (for example, +19722221234) 	<ul style="list-style-type: none"> • (PSTN Prefix) + NN • (PSTN Prefix) + Local Number • E.164 Number (+CC NN) 	There are several alternatives for display. Some of the phones support E.164 dialing (including + sign). Some customers prefer to display the number as it would be dialed.
DN Format	Site Code + Extension (for example, 81134321)		The DN format applies to Cisco UCM, Cisco Unified IM and Presence Service, and Cisco Unity Connection

6.3. Multi-site customer with extension prefix and no ISP

In order to support inter-site calls without an Inter-Site Prefix (ISP), the first digit of site codes do not have match. The only requirement is that site codes should not conflict with extension or PSTN dialing. Customers use an extension prefix for intrasite calls.

Extension prefixes are useful when there is a conflict with PSTN Prefix or other Site Codes. They are also useful when you need to go from four- to five-digit dialing. This extension is still the last four digits of the E.164 number, but the last digit of an NXX code can be used as an extension prefix.

Multi-Site Customer with Extension Prefix and no ISP

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	<ul style="list-style-type: none"> Extension Prefix + Extension (for example, 51234) Site Code + Extension (for example, 2551234) 	<ul style="list-style-type: none"> Site Code + Extension 	Site Code = 255 Extension Prefix = 5 Number of extension digits = 4 Note: Even though the extension is dialed, the calling party number is displayed as a DN. Displaying the extension causes issues during Call Forwarding.
Inter-Site Dialing	Site Code + Extension (for example, 2551234)	Site Code + Extension	-
DN Format	Site Code + Extension (for example, 2551234)		-

6.4. Single Site Customer

Since this is a single site customer, it does not require a Site Code.

Single Site Customer

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	<ul style="list-style-type: none"> Extension (subset of DID number) (for example, 4321 or 54321 if extension prefix is used) Site Code + Extension for (example, 81134321) 	<ul style="list-style-type: none"> Extension 	<p>Even though a site code has been assigned, users are not aware of it.</p> <p>Note: Explicit extension prefix may not be required and it can be included as the first digit of the extension.</p>
DN Format	Extension (for example, 4321)		All extensions must be unique. If there are overlapping extensions, then the DN format of the extension only is not supported. Site Codes are required in this case. IPPBX configuration is done at the customer level.
Voice Mail	Voice Mail	Pilot number is also an extension (for example, 4000 or 54000 if using an extension prefix)	The Voice Mail setup cannot be a child of another location; it must have its own site code. If the extensions for the VM are reserved in the location, then the Dial Plan can be used to prefix the VM extension with the SLC so the user only dials the extension

6.5. Customer (single- or multi-site) without PSTN prefix

Most of the calls made by these customers are PSTN calls. The Cisco UCM interprets calls without any prefix as PSTN or off-net calls. To differentiate between PSTN and intra- or inter-site calls, a prefix is required.

Single or Multi-Site Customer without PSTN Prefix

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing (single site only)	<ul style="list-style-type: none"> Extension Prefix + Extension (for example, *4321) 	<ul style="list-style-type: none"> Extension Prefix + Extension 	Since any digit 0-9 is treated as a PSTN call, extension prefix or ISP is limited to only * or #. For a single site customer, the dialing plan for intra-site calls is just an extension prefix + extension.
Intra-Site and Inter-Site Dialing (Multi-Site)	ISP + Site Code + Extension (for example, *2551234)		<p>For a multi-site customer, it is recommended that extension dialing is not supported and all calls are dialed as ISP + Site Code + Extension.</p> <p>Note: ISP must not conflict with PSTN dialing and is therefore limited to * or #.</p>
PSTN Dialing	<ul style="list-style-type: none"> PSTN Number (for example, 19197221234) E.164 Number (for example, +19728134321) 	<ul style="list-style-type: none"> NN Local Number E.164 Number (+CC NN) 	There are several alternatives for display. Some of the phones support E.164 dialing (including + sign). Some customers prefer to display the number as it would be dialed.
DN Format	<ul style="list-style-type: none"> Extension(Single Site) (for example, 4321) Site Code + Extension (Multi-Site) (for example, 2554321) 		

6.6. Multi-site customer with ISP

In some cases, customers may require an independent inter-site prefix that is not included as the first digit of a site code. For example, for customers who wish to define ISPs per country.

Multi-Site Customer with ISP

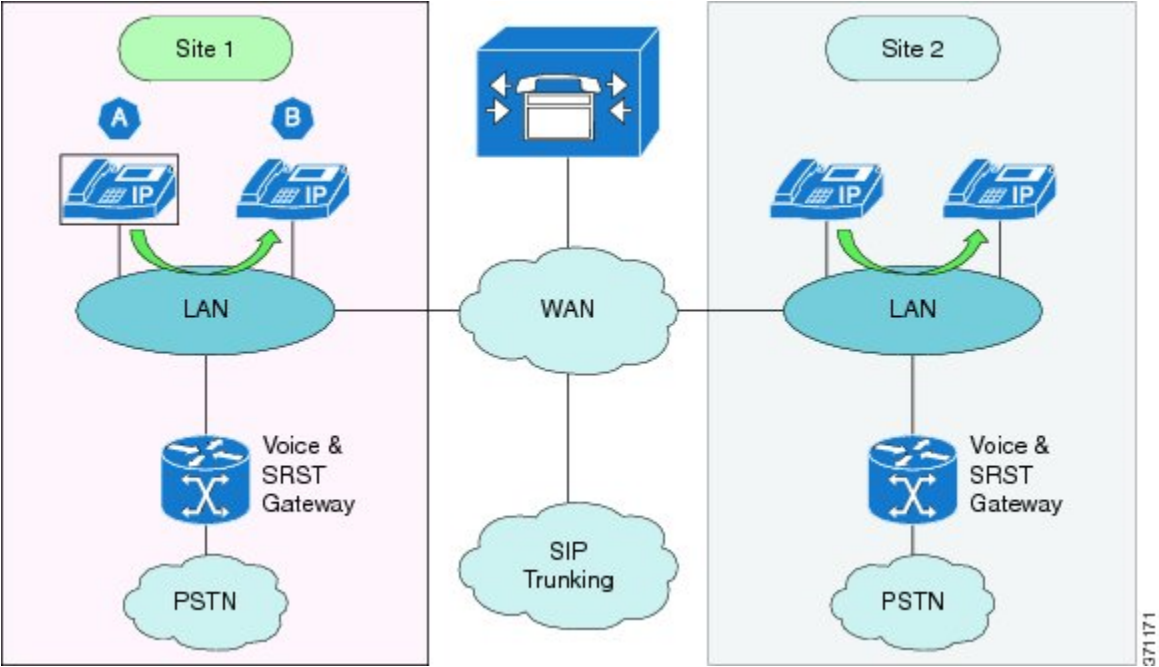
	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	<ul style="list-style-type: none"> Extension (for example, 4321 or 54321) ISP + Site Code + Extension (for example, 82554321) 	<ul style="list-style-type: none"> Extension ISP + Site Code + Extension 	Intra-Site Calls can be dialed as an extension or as an ISP+ Site Code + Extension. Similarly, the calling party number can be displayed either as an extension or as ISP + Code + Extension
Inter-Site Dialing	ISP + Site Code + Extension (for example, 81131234)	ISP + Site Code + Extension	Inter-Site - calls are dialed as ISP + Site Code + Extension
DN Format	Site Code + Extension (for example, 81134321) OR ISP + Site Code + Extension (for example, 82554321)	Site Code + Extension	The DN can be constructed with or without ISP

6.7. On-net call flows

6.7.1. Intra-site On-Net call

This call type occurs between two endpoints located at the same site. As shown in the following figure, media traffic is between the endpoints.

On-Net Call (intra-site)



Usage	<ul style="list-style-type: none">• Target numbering must follow the Numbering Plan described in this chapter• Target number can be a short code, extension, or ESP +Extension, DN or ISP + DN, depending on the enterprise internal numbering plan• Target number is used unless restricted by Class of Service• Codec is dynamically selected based on the endpoints used
Accessibility	User can perform On-Net call from any endpoint registered with Cisco UCM
Default Configuration Configuration Choices	Available to all users <ul style="list-style-type: none">• Feature availability cannot be changed• Codec preferences are configuration
Redundancy	Available to users without restrictions
Survivability	Available to users in fallback mode with the following exceptions: <ul style="list-style-type: none">• Phone must be registered to the SRST Gateway• Users must be able to make On-Net calls only to the same site users connected to the same SRST Gateway• No COS is available during survivability mode
Endpoint Types Supported	<ul style="list-style-type: none">• Cisco IP phones• Cisco ATA• Cisco VG

Examples

Case 1: DN = ISP+SLC+Extension
 Phone A (DN=8 300 4040)
 Dial 4050 (Phone B extension)
 as Phone A Connected Number shows 8 300 4040
 ↳ 4040

Phone B (DN=8 300 4050)
 On Answer, display shows 8 300 4040 -
 ↳ Calling Party Number

Case 2: DN = SLC+Extension; Extension
 ↳ Prefix is used for
 Extension dialing (for example 6)
 Phone A (DN=300 4040)
 Dial 6 4050 (Phone B extension)
 Phone A Connected Number shows 300 4050

Phone B (DN=300 4050)
 On Answer display shows 300 4040 -Calling
 ↳ Party Number

Case 3a: DN= Extension {Dialing with full
 ↳ DN}
 Phone A (DN=40404040)
 Dial 40404050 (Phone B extension)
 Phone A Connected Number shows 40404050

Phone B (DN=40404050)
 On Answer display shows 40404040 as the
 ↳ Calling
 Party Number

Case 3b: DN=Extension {Dialing with Short
 ↳ Code}
 Phone A (DN=40404040)
 Dial *4050 (short code for Phone B)
 Phone A Connected Number shows 40404050

Phone B (DN=40404050)
 On Answer display shows 40404040 as the
 ↳ Calling
 Party Number

6.7.2. Inter-site On-Net call

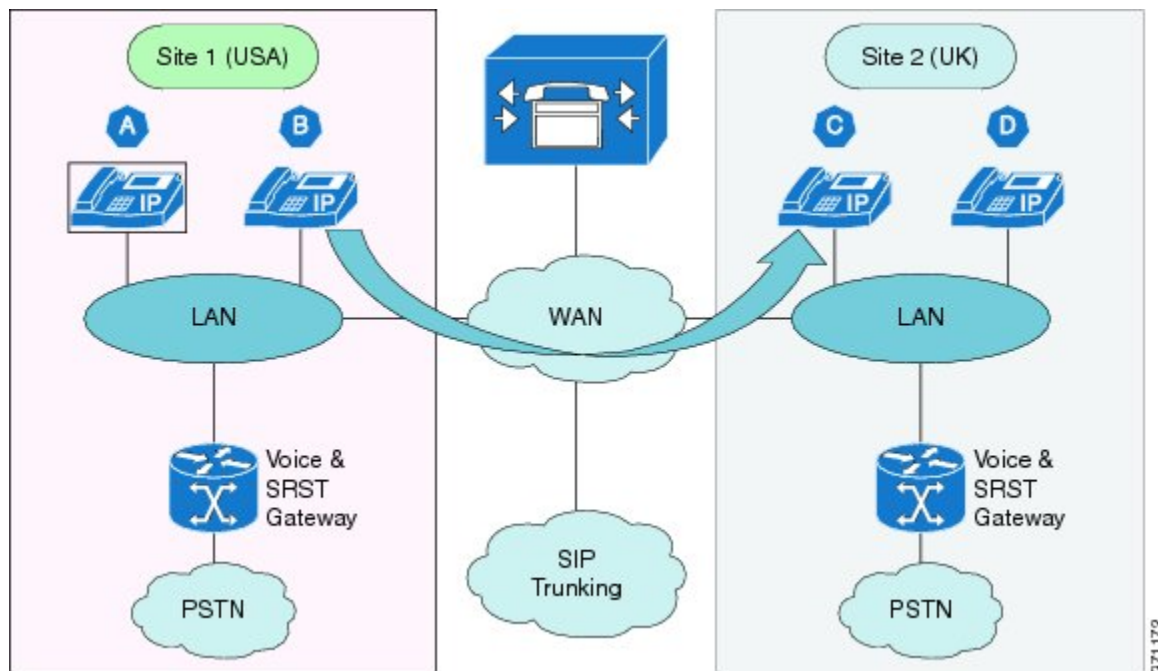
The deployment model supports multiple sites with overlapping extensions and inter-site calling by dialing the Site Location Codes prefixed with an inter-site prefix, and supports the following dialing capabilities:

- Inter-site dialing prefix
- Variable length extensions between sites with no post-dialing delay (PDD) cause by timeout

When the user dials a directory number of another user, the leaf cluster first examines the site code, and determines if the site code is for a site on the same cluster or another cluster. If the site is on the same cluster, the call is routed to the correct location and delivered to the phone. If the site code is for a site on a different cluster, routing is as described in the following section.

This call type occurs between two endpoints located on different sites. The sites can be on a different Cisco UCM that belongs to the same customer. As shown in the following figure, media traffic is between the endpoints.

On-Net Call (Inter-Site)



Usage	<ul style="list-style-type: none">• User can be located in the same or different countries (sites can be in different countries and or different Cisco UCM clusters)• Target numbering must follow the Numbering Plan described in this chapter• Target number can be either DN or ISP +DN depending on the enterprise internal numbering plan adopted. DN can be either just Extension for flat Dial Plan or SLC + Extension or ISP + SLC + Extension.• Any target number can be used unless restricted by Class of Service• Codec is dynamically selected based on the endpoints used
Accessibility	User can perform On-Net call from any endpoint registered with Cisco UCM
Usage Example	Reduces costs of Inter-site and International calls by sharing available bandwidth with Data Network
Default Configuration	Available to all users
Configuration Choices	<ul style="list-style-type: none">• Feature availability cannot be changed• Codec preferences are configuration
Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Endpoint Types Supported	<ul style="list-style-type: none">• Cisco IP phones• Cisco ATA• Cisco VG

Examples

Case 1: DN = ISP+SLC+Extension
 Phone B (DN=8 100 2345)
 Dial 8 200 6789 (for Phone C)
 Phone B Connected Number shows 8 200 6789

Phone C (DN=8 200 6789)
 On Answer, display shows 8 100 2345 -
 ↳ Calling Party Number

Case 2: DN = SLC+Extension; Extension
 ↳ Prefix is used for
 Extension dialing (for example 6)
 Phone A (DN=300 4040)
 Dial 300 4050 (Phone B extension)
 Phone D Connected Number shows 300 4050

Phone D (DN=300 4050)
 On Answer display shows 300 4040 -Calling
 ↳ Party Number

Case 3: DN= Extension {Dialing with full
 ↳ DN}
 Phone A (DN=40404040)
 Dial 40404050 (Phone D extension)
 Phone A Connected Number shows 40404050

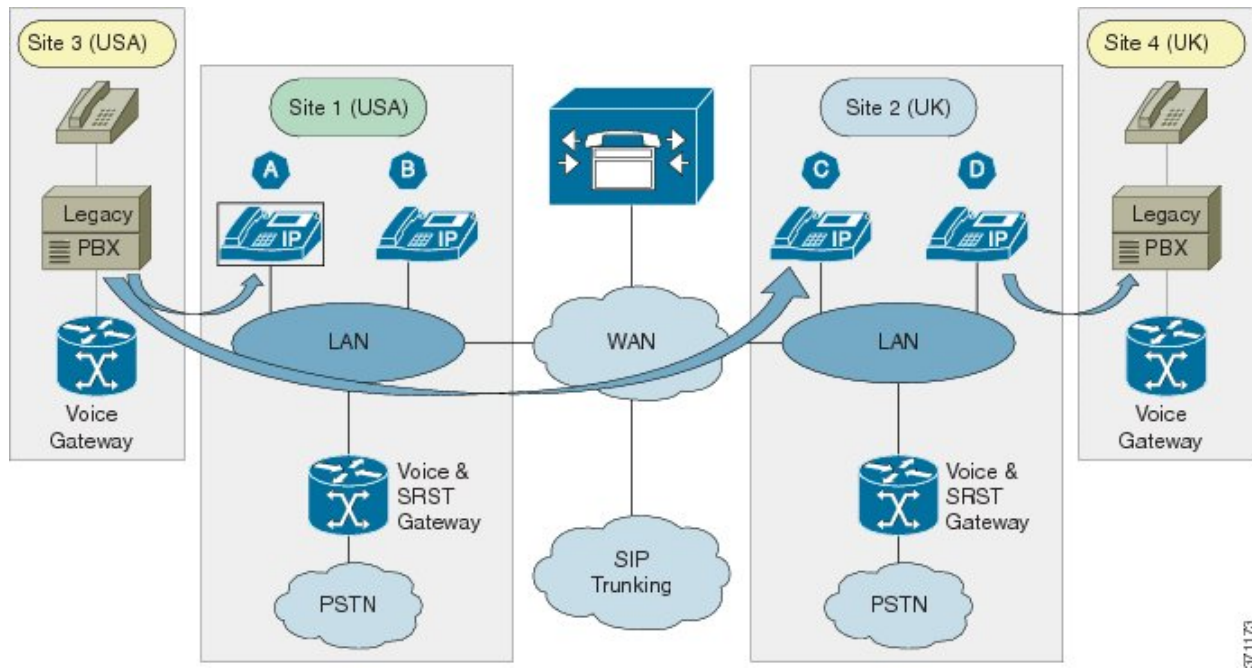
Phone D (DN=40404050)
 On Answer display shows 40404040 as the
 ↳ Calling
 Party Number

6.7.3. VoIP trunking On-Net Call

This call type occurs between endpoints connected to Cisco Unified Communications Manager (UCM) and a legacy PBX that is connected to a voice gateway. The call type includes:

- SIP/SCCP signaling traffic between the endpoint and the Cisco UCM
- SIP signaling traffic between the voice gateway and the Cisco UCM
- TDM signaling traffic between the Legacy PBX and voice gateway
- Media traffic between the endpoint and voice gateway

On-Net Call (VoIP trunking)



Usage	<ul style="list-style-type: none"> • Called number must follow the enterprise internal numbering plan requirement • Called number must be defined by ranges and not individual numbers • Called number can be either DN or ISP +DN depending on the enterprise internal numbering plan adopted. DN can be either just Extension for flat Dial Plan or SLC + Extension or ISP + SLC + Extension. • Voice codec used must be selected per site • Only voice calls can be made; video calls are not supported • Fax is supported as best effort only • MoH is provided in accordance with the site's MoH policy • Voice Gateway configuration is part of the solution • Voice Gateway redundant deployment is not supported • Enbloc signaling is between the Voice Gateway and Cisco UCM • Any target number can be used unless restricted by Class of Service • Codec is dynamically selected based on the endpoints used • Alternate call routing when the Legacy PBX or Voice Gateway is unreachable is not supported
Accessibility	<ul style="list-style-type: none"> • User can perform On-Net call from any endpoint registered with Cisco UCM • Legacy PBX connected using a Voice Gateway is considered to be similar to an Inter-Site call • User uses the same dialing behavior as Inter-Site On-Net Call
Usage Example	Enables the integration with the existing environment during the transition period of all users
Default Configuration	<ul style="list-style-type: none"> • Available to all users at all sites of the enterprise • Codec: Voice - G.729 and G.711 • Codec: Sample Size - 20ms/20Bytes and 20ms/160Bytes • Bandwidth: 8kbps and 64kbps

Configuration Choices	<ul style="list-style-type: none"> • Feature availability cannot be changed by site or user • Codec can be selected between G.711 and G.722 on a per-site basis
Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Endpoint Types Supported	<ul style="list-style-type: none"> • Cisco IP phones • Cisco ATA • Cisco VG
Example	<p>Example:</p> <p>Phone D (DN=8 200 6100)</p> <p>Dial 8 400 1234 to Legacy PBX</p> <p>Connected Number shows 8 400 1234</p> <p>Legacy PBX (Site 3)</p> <p>Dial 8 100 2123 to Call A</p> <p>Phone C (DN=8 100 2123)</p>

6.8. Off-net call flows

6.8.1. Local gateway (LBO)

This call type occurs in the following situations for an endpoint in a site that has Local Gateway (Local Breakout):

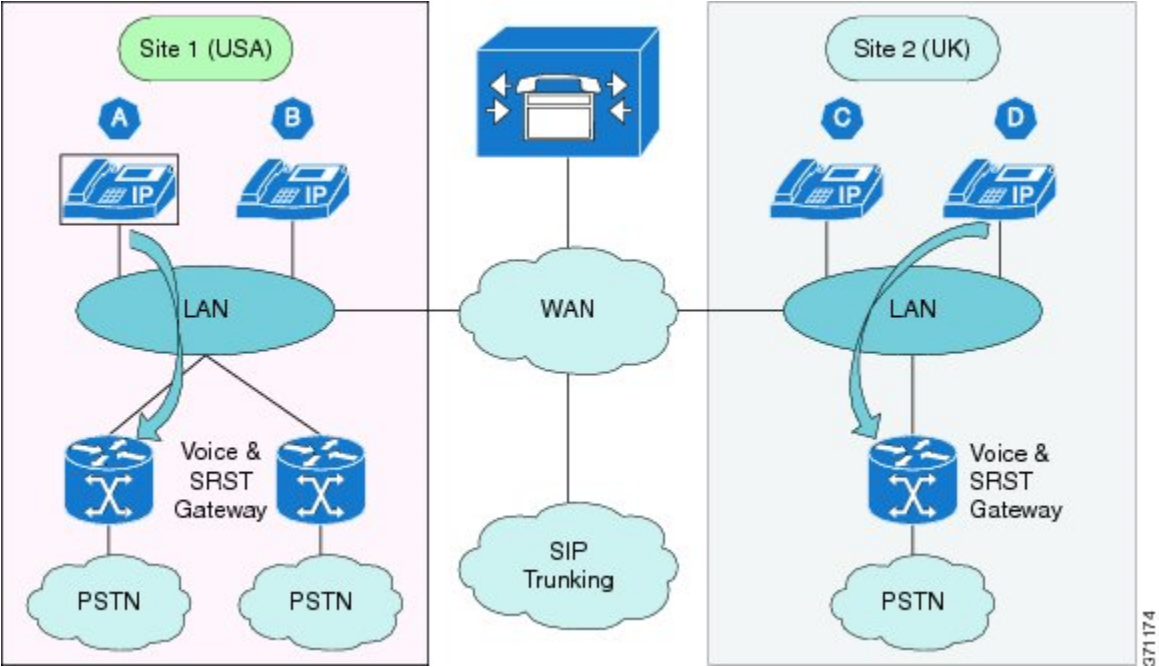
- When the endpoint places a call to reach a destination in the PSTN through the Local Gateway
- When the endpoint receives a call from the PSTN through the Local Gateway

The local gateway is used to connect to the PSTN locally. In this case, it must be possible on a per-call basis to select the Local Gateway breakout and there must be selectable per-site routing through the Local Gateway (that is, International, National, Service, and so on).

The call type includes:

- SIP/SCCP signaling traffic for the endpoint between the endpoint and Cisco UCM
- SIP signaling traffic for the Local Gateway between the Local Gateway and Cisco UCM
- Media traffic between the endpoint and local gateway

Off-Net Call (local gateway)



Usage	<ul style="list-style-type: none"> • Called number follows the Numbering Plan requirements • Called number can include an access code if necessary • Any target number can be used, unless it is restricted by Class of Service • Off-net dialing can be completed in two ways: <ul style="list-style-type: none"> – When PDD is unavoidable, user can wait for interdigit timeout or press # without waiting for interdigit timeout – E.164 numbering format is supported with + as the first digit • The calling number is one of: <ul style="list-style-type: none"> – DDI of the DN – Site Published PSTN number if the DN does not have a DDI, or – Site Published PSTN number regardless of the availability of DN DDI
Accessibility	User can perform Off-Net call from any endpoint registered with Cisco UCM
Usage Example	User can dial any PSTN number from their phone
Default Configuration	<ul style="list-style-type: none"> • Available to all users • DDI of the DN is sent if available; otherwise, Site Published PSTN number is sent • Codec depend on trunk bandwidth
Configuration Choices	<ul style="list-style-type: none"> • Feature availability cannot be changed • Can be configured to send only the Site Published PSTN number as the Calling Number PRI, BRI, and so on
Redundancy	Available to users without restrictions
Survivability	<p>Available to users in fallback mode, with the following restrictions:</p> <ul style="list-style-type: none"> • Phone must be registered to the SRST gateway • No COS is available during survivability mode

Endpoint Types Supported	<ul style="list-style-type: none">• Cisco IP phones• Cisco ATA• Cisco VG
Examples	<div>Case 1: Using Trunk Transformation CSS to →convert DN to DDI Phone A (DN=8 300 1234; External →Mask=+14085289001) Dial 9 12134225001 Local GW Trunk {uses Called, Calling, →Redirecting and Connected Transformation CSS} Outbound from CCM - CDPN = +12134225001; →CGPN=+14085289001 Inbound Connected Number +12134225001</div>

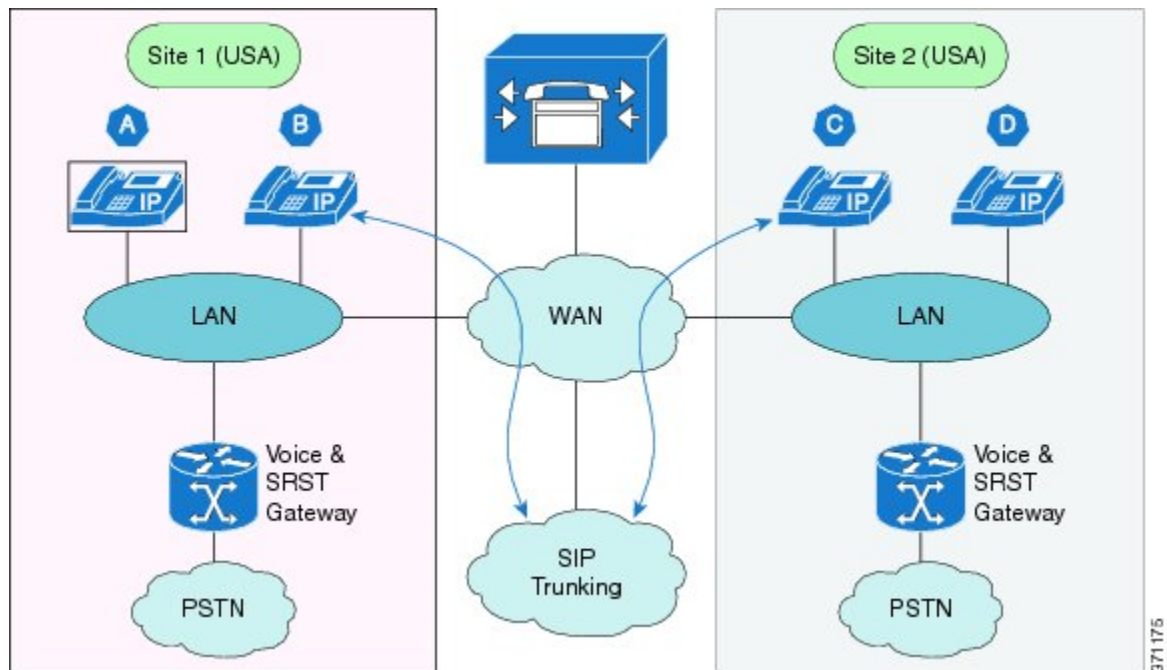
6.8.2. Aggregation (CBO)

This call type occurs when an endpoint located in a Site in one country wants to reach a destination in any country through Aggregation (Central Breakout). The cluster in which the site is located must have the source country dial plan. Routing is based on the source country. It is not possible for sites in a cluster to be in different countries.

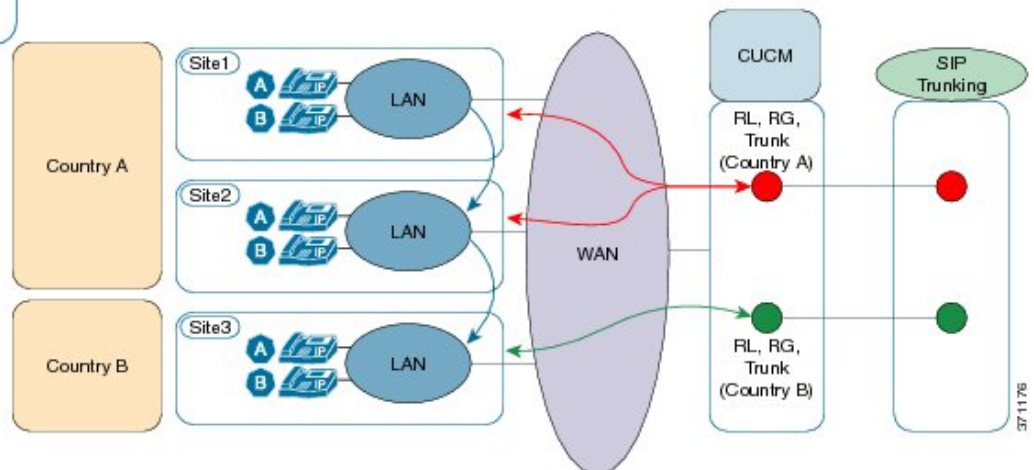
The call type includes:

- SIP/SCCP signaling traffic for the endpoint between the endpoint and Cisco Unified Communications Manager
- SIP signaling traffic for SIP trunking between the SIP trunking Session Border Controller (SBC) and Cisco Unified Communications Manager
- Media traffic between the endpoint and SIP trunk SBC

Off-Net Call (Aggregation)



Option 1 -
Source countries defined
per Customer per Cluster.
Destination countries can
be per source country
(i.e. origination based)



Usage	<ul style="list-style-type: none"> • Called number follows the Numbering Plan requirements • Called number can include an access code if necessary • Any target number can be used, unless it is restricted by Class of Service • Off-net dialing can be completed in two ways: <ul style="list-style-type: none"> – When PDD is unavoidable, user can wait for interdigit timeout or press # without waiting for interdigit timeout – E.164 numbering format is supported with + as the first digit • Forced On-Net is supported and optional. A forced on-net call will not reach the Session Border Controller. It is either within the same cluster or cross cluster • As shown in the figure (Option 1), each source country has its own SIP trunk to the Session Border Controller. Otherwise, all source countries share the same SIP trunk to the SBC. • The calling number is one of: <ul style="list-style-type: none"> – DDI of the DN – Site Published PSTN number if the DN does not have a DDI, or – Site Published PSTN number regardless of the availability of DN DDI • MoH is supported
Accessibility	User can perform Off-Net call from any endpoint registered with Cisco Unified Communications Manager
Usage Example	User can dial any PSTN number from their phone
Default Configuration	<ul style="list-style-type: none"> • Not available to all users; only by subscription to PSTN access • DDI of the DN is sent if available; otherwise, Site Published PSTN number is sent • Codec depend on trunk bandwidth
Configuration Choices	<ul style="list-style-type: none"> • Available by subscription to PSTN access • Can be configured to send only the Site Published PSTN number as the Calling Number PRI, BRI, and so on

Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Endpoint Types Supported	<ul style="list-style-type: none">• Cisco IP phones• Cisco ATA• Cisco VG
Examples	<div>Case 1: Using Trunk Transformation CSS to ↪convert DN to DDI Phone A (DN=8 300 1222; External ↪Mask=+14085289001) Dial 9 12134225010 Aggregation Trunk {uses Called, Calling, ↪Redirecting and Connected Transformation CSS} Outbound from CCM - CDPN = +12134225010; ↪CGPN=+14085289001 Inbound Connected Number +12134225010</div>

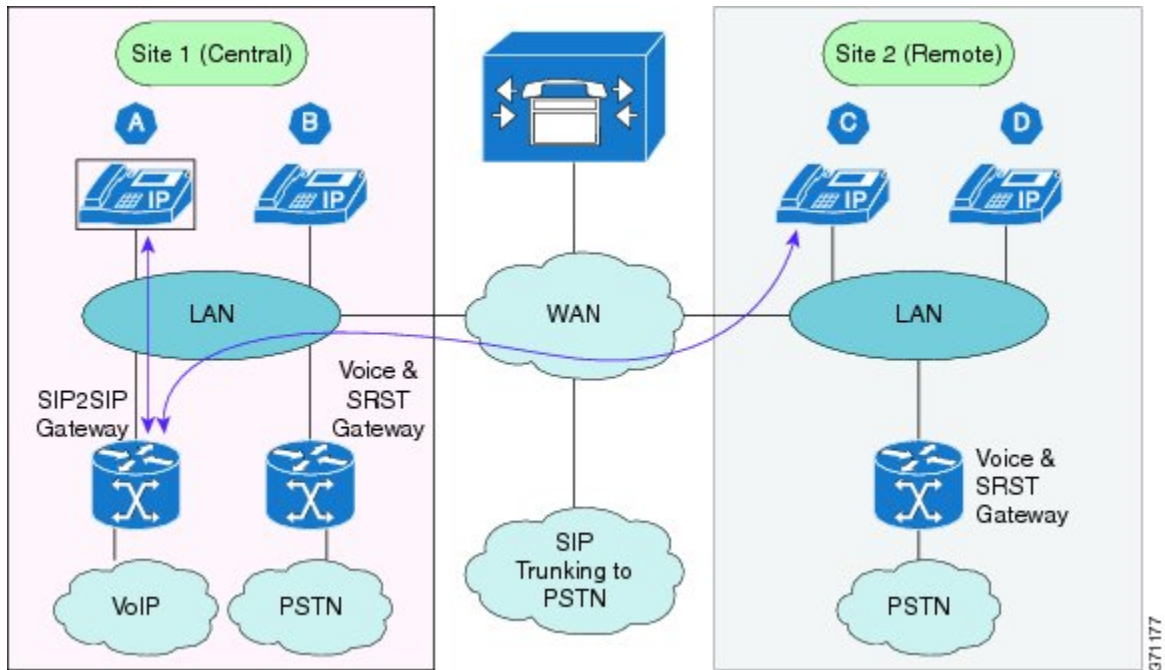
6.8.3. VoIP

This call type occurs when an endpoint located in a site wants to reach a destination on the PSTN through the Voice over IP (VoIP) provider. The cluster in which the site is located provides the source country dial plan and routing is based on the source country.

The call type includes:

- SIP/SCCP signaling traffic for the endpoint between the endpoint and Cisco Unified Communications Manager
- SIP signaling traffic is used for the SIP Gateway to the VoIP network and Cisco Unified Communications Manager
- SIP Gateway to the VoIP network can be PRI as well
- VoIP network can be connected through the Session Border Controller (not shown in the diagram)
- Media traffic between the endpoint and SIP trunk SBC

Off-Net Call (VoIP)



Usage	<ul style="list-style-type: none"> • Called number follows the Numbering Plan requirements • Called number can include an access code if necessary; the access codes can be either the same PSTN access code or a different access code • Any target number can be used, unless it is restricted by Class of Service • Off-net dialing can be completed in two ways: <ul style="list-style-type: none"> – When PDD is unavoidable, user can wait for interdigit timeout or press # without waiting for interdigit timeout – E.164 numbering format is supported with + as the first digit • Forced On-Net is supported and optional. • The calling number is one of: <ul style="list-style-type: none"> – DDI of the DN – Site Published PSTN number if the DN does not have a DDI, or – Site Published PSTN number regardless of the availability of DN DDI • MoH is supported
Accessibility	Users can perform Off-Net call from any endpoint registered with Cisco Unified Communications Manager through the VoIP network if they subscribe
Usage Example	Billing consolidation between domestic and international outgoing calls
Default Configuration	<ul style="list-style-type: none"> • Not available to all users; only by subscription to VoIP network access • DDI of the DN is sent if available; otherwise, Site Published PSTN number is sent • Codec preference depends on trunk bandwidth
Configuration Choices	<ul style="list-style-type: none"> • Feature availability by subscription to VoIP network access • Can be configured to send only the Site Published PSTN number as the Calling Number • Access code cannot be chosen by the user; it is defined by the provider • Automatic rerouting is not supported

Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Endpoint Types Supported	<ul style="list-style-type: none">• Cisco IP phones• Cisco ATA• Cisco VG
Examples	<div>Case 1: Uses different PSTN Access Prefix, →and Trunk Transformation CSS to convert DN to DDI Phone A (DN=8 300 1234; External, →Mask=+14085289001) Dial 0 12134225001 SIP2SIP GW Trunk {uses Called, Calling, →Redirecting and Connected Transformation CSS} Outbound from CCM - CDPN = +12134225001; →CGPN=+14085289001 Inbound Connected Number +12134225001</div>

6.9. Emergency call handling

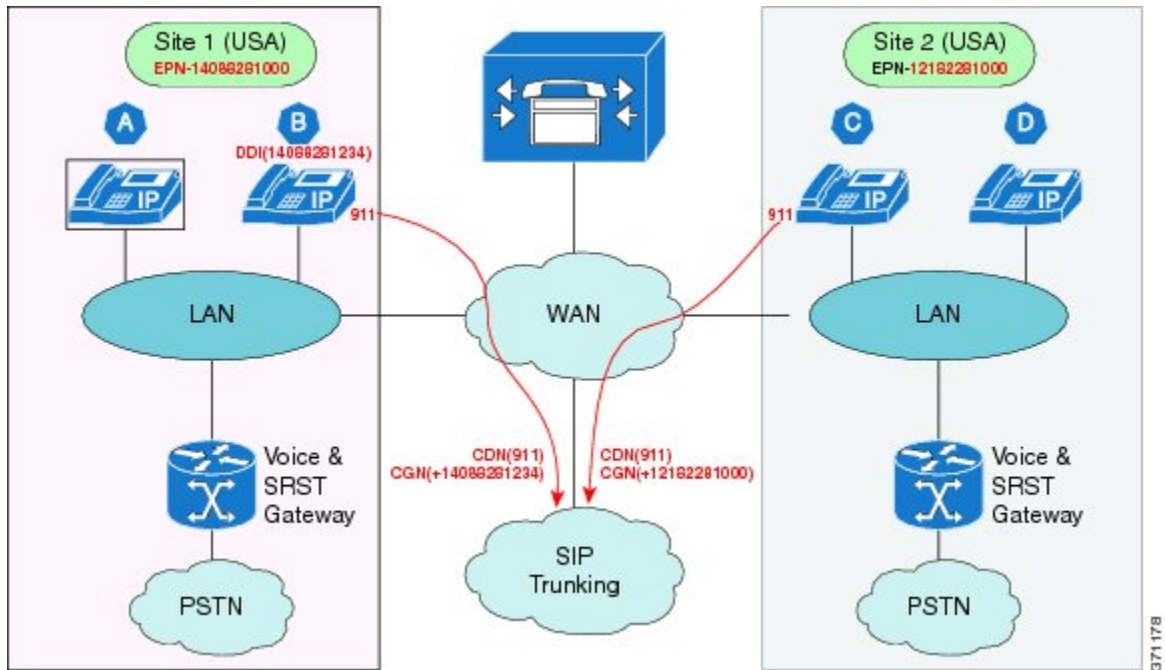
6.9.1. Non-CER through aggregation

This call type is the standard enhanced emergency call to the Emergency Service Center (for example, US Enhanced 911 or 911). If configured, the call is routed through Aggregation. Emergency Calling is provided, regardless of the Class of Service, as long as the phone is registered.

Non-CER through aggregation includes:

- SIP/SCCP signaling traffic for the endpoint is between the endpoint and Cisco UCM
- SIP signaling traffic for SIP trunking is between the SIP trunking Session Border Controller (SBC) and Cisco UCM
- Media traffic is between the endpoint and SIP trunk SBC

Emergency Call (Non-CER through aggregation)



Usage	<ul style="list-style-type: none"> • The Emergency number follows the Numbering Plan requirements • The Emergency number can include an access code if necessary • The Calling Party Number is one of: <ul style="list-style-type: none"> – DDI of the Line or Site Emergency Published Number if the line does not have a DDI – Site Emergency Published Number – For Extension Mobility where a user logs in to a Remote Site, the Site Emergency Publish Number is used • Emergency Calls are based on the device and not the line
Accessibility	User can perform Off-Net call from any endpoint registered with Cisco UCM
Usage Example	User can dial any PSTN number from their phone
Default Configuration	<ul style="list-style-type: none"> • Available to all registered phones • DDI of the DN is sent if available; otherwise, Site Emergency Publish Number is sent
Configuration Choices	<ul style="list-style-type: none"> • Can be configured to send only the Site Emergency Publish Number for all emergency calls
Redundancy	Available to users without restrictions
Survivability	Not available to users in SRST fallback mode
Class of Service	Available to all Classes of Service
Endpoint Types Supported	<ul style="list-style-type: none"> • Cisco IP phones • Cisco ATA • Cisco VG

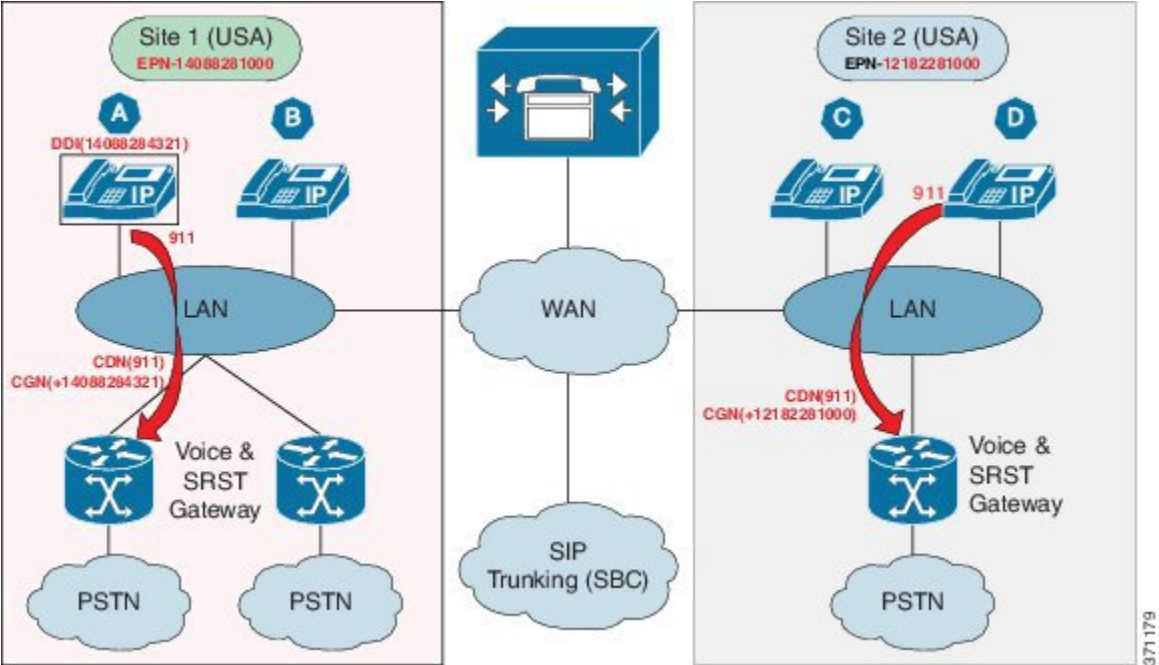
6.9.2. Non-CER through local gateway

This call type is the standard enhanced emergency call to the Emergency Service Center (for example, US Enhanced 911 or 911). If configured, the call is routed through the Local Gateway. Emergency Calling is provided, regardless of the Class of Service, as long as the phone is registered.

Non-CER through local gateway includes:

- SIP/SCCP signaling traffic for the endpoint is between the endpoint and Cisco UCM
- SIP signaling traffic for SIP trunking is between the local gateway and Cisco UCM
- Media traffic is between the endpoint and SIP trunk SBC

Figure 8. Emergency Call (Non-CER Through Local Gateway)



Usage	<ul style="list-style-type: none"> • The Emergency number follows the Numbering Plan requirements • The Emergency number can include an access code if necessary • The Calling Party Number is one of: <ul style="list-style-type: none"> – DDI of the Line or Site Emergency Published Number if the line does not have a DDI – Site Emergency Published Number – For Extension Mobility where a user logs in to a Remote Site, the Site Emergency Publish Number is used • Emergency Calls are based on the device and not the line • Emergency Call is configured to be routed through the Local Gateway
Accessibility	User can perform Off-Net call from any endpoint registered with Cisco UCM
Usage Example	User can dial any PSTN number from their phone
Default Configuration	<ul style="list-style-type: none"> • Available to all registered phones • DDI of the DN is sent if available; otherwise, Site Emergency Publish Number is sent
Configuration Choices	<ul style="list-style-type: none"> • Can be configured to send only the Site Emergency Publish Number for all emergency calls
Redundancy	Available to users without restrictions
Survivability	Not available to users in SRST fallback mode
Class of Service	Available to all Classes of Service
Endpoint Types Supported	<ul style="list-style-type: none"> • Cisco IP phones • Cisco ATA • Cisco VG

6.9.3. Cisco emergency responder

This call type uses the Cisco Emergency Responder (CER) to manage the emergency call. If configured, the call is routed through Aggregation or the Local Gateway. Each cluster has its own CER server. Emergency calling is provided, regardless of the Class of Service, as long as the phone is registered.

CER includes:

- SIP/SCCP signaling traffic for the endpoint is between the endpoint and Cisco UCM
- SIP signaling traffic for SIP trunking is between the SIP trunking Session Border Controller (SBC) and Cisco UCM

- Media traffic is between the endpoint and SIP trunk SBC

Usage	<ul style="list-style-type: none"> • The Emergency number follows the Numbering Plan requirements • The Emergency number can include an access code if necessary • The Calling Party Number is one of: <ul style="list-style-type: none"> – DDI of the Line or Site Emergency Published Number if the line does not have a DDI – Site Emergency Published Number – For Extension Mobility where a user logs in to a Remote Site, the Site Emergency Publish Number is used • Emergency Calls are based on the device and not the line
Accessibility	User can perform Off-Net call from any endpoint registered with Cisco UCM
Usage Example	User can dial any PSTN number from their phone
Default Configuration	<ul style="list-style-type: none"> • Available to all registered phones • DDI of the DN is sent if available; otherwise, Site Emergency Publish Number is sent
Configuration Choices	<ul style="list-style-type: none"> • Can be configured to send only the Site Emergency Publish Number for all emergency calls
Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Class of Service	Available to all Classes of Service
Endpoint Types Supported	<ul style="list-style-type: none"> • Cisco IP phones • Cisco ATA • Cisco VG

7. PSTN call processing and routing

7.1. Introduction to PSTN call processing and routing

7.1.1. Introduction to PSTN call processing and routing

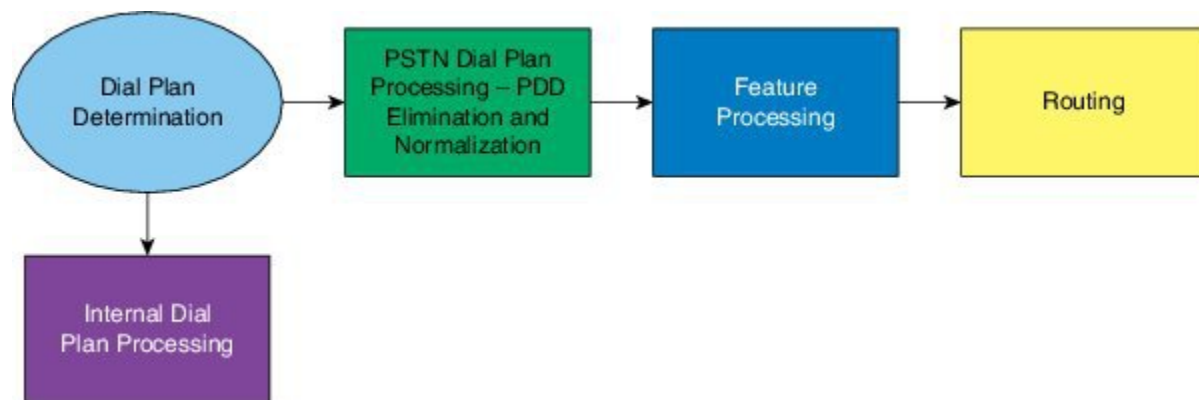
PSTN call processing and routing leverages two Automate 10.x/11.5(x) features:

- Calling Search Space (CSS) hierarchy
- Name Local Route Group

Call processing includes the following stages:

1. Dial plan determination (internal and PSTN dial plan)
2. Country dial Plan post-dialing delay (PDD) elimination, normalization, and call type classification (applies to PSTN calling only)
3. Feature processing - Forced On-Net, Origination Call Screening, Time of Day, Calling Line Identification Restriction (CLIR), Calling Line Identification Presentation (CLIP), Forced Authorization Code and CMC (applies to PSTN calling only)
4. Line or device based routing

Figure 1. Call Processing Stages

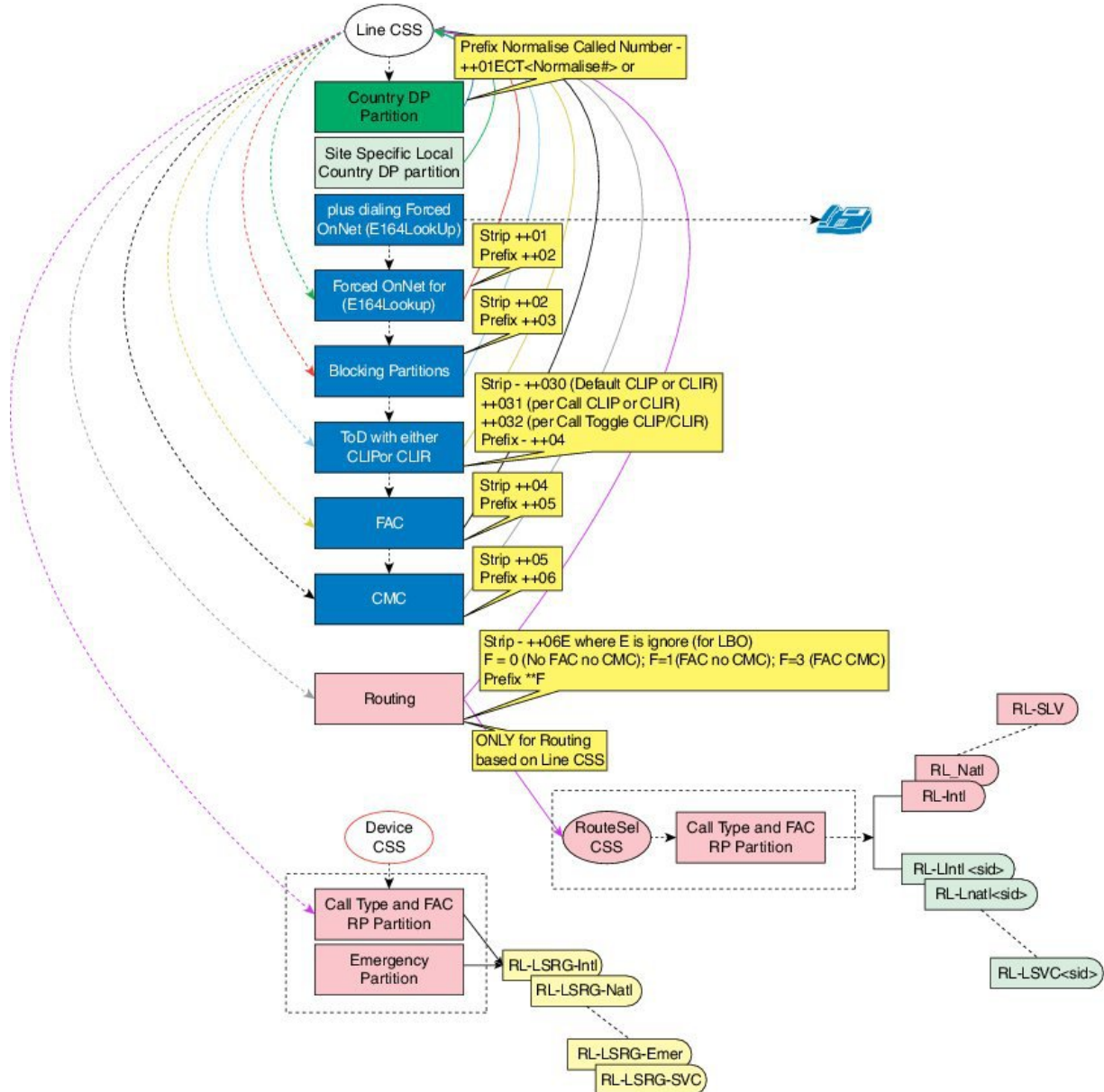


Features and routing are based on call type rather than dialed number. The biggest advantage of using call type classification is that most features are independent of the country dial plan. Adding a country dial plan defines the dialing behavior patterns, classifying them into different call types, and defining routing.

There are two caveats on using feature chaining and call type classification:

- In order to bypass a feature within a feature, a *nil* feature is implemented.
- For some features (for example FONet), call type classification must be de-classified and reclassified to handle the feature.

Figure 2. Call Processing Implementation



373379

7.2. Dial plan determination

7.2.1. Dial plan determination

This section covers PSTN call processing and routing. The first stage of call processing is the determination of which dial plan is applied against the incoming call.

It is assumed that there is a PSTN breakout code and the PSTN breakout code is used as a steering digit to direct the PSTN call processing. The PSTN breakout code is a single digit that is country-specific and customer-specific.

7.3. Country dial plan deployment

7.3.1. Country dial plan deployment overview

Each country dial plan deployed consists of a single partition containing all the patterns that handle the dialing behavior for that country. The partition is configured with the 'All Day' Time Schedule. The objective of each pattern in this partition is to eliminate Post Dialing Delay (PDD), normalize the Called Number, prefix the first feature code of the feature chain and set the Call Type to the normalized called number.

If there is Local Dialing behavior, then it is necessary to define a per-site local call handling partition. The patterns in this partition are built based on the following data collected from the user:

- Local Area Code if present and is or is not required for local dialing
- The number of digits for the Local (user) number.

The pattern objective is to eliminate PDD for local dialing, normalize the called number and prefix the first feature code. The local call traverses the feature chain like any other PSTN Call Type.

Besides defining the dialing behavior, it is also necessary to define per-country routing. In general, the routing is similar for every country except for the route list used. Hence it is a matter of copying an existing country routing defined and changing the route pattern route list name.

7.3.2. Predefined country dial plans

The table lists predefined country dial plans shipped with an early version of Automate. Additional country dial plans or updated versions of country dial plans may be made available between releases.

Country	ISO Three Letter Country Code
Australia	AUS
Austria	AUT
Belgium	BEL
Brazil	BRA
Canada	CAN
China	CHN
Cyprus	CYP
Denmark	DNK
Estonia	EST
Finland	FIN
France	FRA
Germany	DEU
Hungary	HUN
Italy	ITA
Luxembourg	LUX
Netherlands	NLD
New Zealand	NZL
Norway	NOR
Portugal	PRT
Puerto Rico	PRI
Russia	RUS
Spain	ESP
Sweden	SWE
Switzerland	CHE
Turkey	TUR
United Kingdom	GBR
United States	USA

Note: If you require a new country dial plan to be created, contact your VOSS representative.

7.3.3. Install country dial plan (.template file)

Tip: *Use the Action search to navigate Automate*

This procedure installs a new country dial plan using a **.template** file.

1. Extract the country dial plan **.template** file from the country dial plan package you downloaded from cisco.com.

2. Use *sftp* to transfer the country dial plan **.template** file to the platform user's media directory server.
3. Install the template with the `app template media/<template_file>` command.
4. Review the output from the `app template` command and confirm that the following message displays:
Script /opt/platform/admin/home/template_<random_number>/install_script completed successfully

Next steps

- If installation succeeds, add the new country dial plan to your customer dial plan.

7.3.4. Install country dial plan (.json file)

Tip: *Use the Action search to navigate Automate*

This procedure installs a new country dial plan using a .json file.

1. Log in as hcsadmin administrator.
2. Go to **Import**.
3. Browse to the .json file and select Import.
4. To monitor the status of the import, select **Administration Tools > Transaction**.

Next steps

- If the import succeeds, add the new country dial plan to your customer dial plan.

7.3.5. Add a country dial plan to a dial plan before deploying to a customer

Tip: *Use the Action search to navigate Automate*

By default, the USA and GBR country dial plans are associated with Type 1 through Type 4 dial plan schema groups. Use this procedure to associate another country dial plan with a dial plan schema group before deploying the dial plan to the customer.

1. Log in as the hcsadmin or Provider administrator.
2. Go to **Dial Plan Schema Group**.
3. Choose an existing dial plan schema group to clone, or create a new dial plan schema group.
If you choose an existing dial plan schema group, select **Action > Clone**. Update the Dial Plan Schema group Name on the General tab. For example, clone Cisco Type 4 Schema Group and give it the name "Cisco Type 4 Schema Group with France."
4. Click the **Country Schemas** tab.
5. Add the two schemas associated with the country dial plan to the dial plan schema group.
 - HcsGenericCustomer<Country>DP-V<version>-SCH: The schema template used to deploy the customer-level country dial plan elements for the target country.

- HcsGenericSite<Country>DP-V<version>-SCH: The schema template used to deploy the site-level country dial plan elements for the target country.

Provide the following mandatory information for the two schemas:

Field	Description
Dial Plan Schema Usage	Select Add Site for both schemas.
Country Name	Select the target country.
Dial Plan Schema Scope	Select Customer for the customer schema. Select Site for the site schema.
Dial Plan Schema Name	Select HcsGenericCustomer<Country>DP-V<version>-SCH for the customer schema. Select HcsGenericSite<Country>DP-V<version>-SCH for the site schema.

Note: Add more country dial plan schemas as needed by the customer.

6. Click **Save**.
7. Deploy the customized schema group to the customer.
 - a. Go to **Associate Custom Dial Plan Schema Group**.
 - b. Set the hierarchy path to the customer hierarchy node.
 - c. Click **Add**.
 - d. From the Dial Plan Schema Group drop-down, select The customized dial plan schema group with your Added country or countries.
 - e. Click **Save**.

Next steps

- Deploy your customer and site dial plans. When a site is created that targets the country you added to the customized dial plan schema group, the appropriate country dial plan schemas are deployed.

7.3.6. Add a country dial plan to a deployed customer dial plan

Tip: *Use the Action search to navigate Automate*

This procedure enables another country dial plan for a customer that already has a dial plan deployed.

1. Log in as a Provider administrator.
2. Go to **Associate Custom Dial Plan Schema Group**.

Make a note of which Dial Plan Schema Group is currently associated with the customer.

3. Set the hierarchy path to the customer hierarchy node for which you want to add country dial plan schemas.
4. Go to **Dial Plan Schema Group**.
5. Select the schema group currently associated with the customer.
6. Select **Action > Clone**.
7. Click the **Country Schemas** tab.
8. Add the two schemas associated with the country dial plan to the dial plan schema group.
 - HcsGenericCustomer<Country>DP-V<version>-SCH: The schema template used to deploy the customer-level country dial plan elements for the target country.
 - HcsGenericSite<Country>DP-V<version>-SCH: The schema template used to deploy the site-level country dial plan elements for the target country.

Provide the following mandatory information for the two schemas:

Field	Description
Dial Plan Schema Usage	Select Add Site for both schemas.
Country Name	Select the target country.
Dial Plan Schema Scope	Select Customer for the customer schema. Select Site for the site schema.
Dial Plan Schema Name	Select HcsGenericCustomer<Country>DP-V<version>-SCH for the customer schema. Select HcsGenericSite<Country>DP-V<version>-SCH for the site schema.

Note: Add more country dial plan schemas as needed by the customer.

9. Click **Save**. An instance of the schema group with the additional country dial plan schemas is created at the customer level. It has the same name as the schema group from which it was cloned. However, the schema group at the customer level is used rather than the instance at a higher hierarchy node.

Next steps

- Deploy the dial plan on the site that uses the new country dial plans.

7.3.7. Called party number as dialed feature

Tip: *Use the Action search to navigate Automate*

Overview

By default Cisco Type 1-4 dial plans route outbound PSTN calls with called party numbers in a +E.164 format. However, you can implement the As Dialed feature to instead route outbound calls using an ‘as-dialed’ format using a country’s national trunk prefix.

For example, for Great Britain, if the dialed number is 0 20 8824 9286, then called-party number in E.164 format is +44 20 8824 9286. If the ‘as-dialed’ format is enabled, then the called-party number is 0 20 8824 9286.

Note:

- Enabling sending called-party numbers ‘as dialed’ is done on a per-country and per-call type basis.
- This procedure applies to Cisco Type 1-4 dial plan schema groups.

The procedures to implement the Called-Party Number As Dialed feature vary depending on:

- The version of Automate
- Whether country-specific dial plans have been deployed to the customer

	Pre-VOSS-4-UC 10.6(2)	VOSS-4-UC 10.6(2) or later
Country Dial Plan not deployed for customer	1. Edit Country Dial Plan Schema (pre-10.6(2)) for Called-Party As Dialed Feature	1. Edit Country Dial Plan Schema (10.6(2) or later) for Called-Party As Dialed Feature
	2. Deploy Country Dial Plan	2. Deploy Country Dial Plan
Country Dial Plan deployed for customer	1. Edit Route Patterns for Called-Party As Dialed Feature	1. Edit Route Lists for Called-Party As Dialed Feature
	2. Edit Route Lists for Called-Party As Dialed Feature	

Edit country dial plan schema [pre-10.6(2)] for Called-Party as dialed feature

Modify the route patterns and route lists in the dial plan schema for each country dial plan to be deployed to the customer.

Important: Edit all route patterns with the following exceptions:

- Any route pattern that has the digits 04 (emergency), 05 (service), or 11 (operator) immediately before the dot.
- Any route pattern that has the digits 01 (international) immediately before the dot, unless the country code is specified immediately after the dot.
- Any route pattern that has an X (mask digit) immediately after the dot.

Edit all route lists with the following exceptions:

- Emergency
 - International
 - Operator
 - Service
-

Before you begin

To complete this procedure, you need to know the country code and country-specific trunk prefix.

1. Log in as Provider administrator.
2. Go to **Dial Plan Schema**.
3. Click the country dial plan schema you want to modify.
Select the country dial plan schema located closest to the customer hierarchy node.
Example: For Great Britain, select HcsGenericCustomerGBRDP-V5-SCH.
4. Select the **Route Patterns** tab.
5. For each route pattern, except for the ones noted previously:

a. In the Route Pattern field:

- If the route pattern contains the country code after the dot, move it to immediately before the dot.
- If the route pattern does not contain the country code, add it immediately before the dot.

Example: For Great Britain:

- Change **001.44! to **00144.!
- Change **002.! to **00244.!

b. In the Called Party Prefix Digits (Outgoing Calls) field, change the + to +<cc>, where <cc> is the appropriate country code.

Example: For Great Britain, change + to +44

6. Select the **Route Lists** tab.
7. For each route list, except for the ones noted previously, under Members, click **More...**

- a. If necessary, click + to expand the Members field.
 - b. For Called Party Discard Digits, select PreDot.
 - c. For Called Party Prefix Digits (Outgoing Calls), enter the appropriate trunk prefix for the country.
8. Click **Save**.

Edit country dial plan schema [10.6(2) or later] for Called-Party as dialed feature

Modify the dial plan schema for each country dial plan to be deployed to the customer.

Important: Edit all route lists with the following exceptions:

- Emergency
 - International
 - Operator
 - Service
-

Before you begin

To complete this procedure, you need to know the country code and country-specific trunk prefix.

1. Log in as Provider administrator.
2. Go to **Dial Plan Schema**.
3. Click the country dial plan schema you want to modify.
4. On the tabs bar, select **Route Lists**.
5. For the route list you want to update, under Members, click **More...**
6. If necessary, click + to expand the Members field.
7. For Called Party Discard Digits, select PreDot.
8. For Called Party Prefix Digits (Outgoing Calls), enter the appropriate trunk prefix for the country.
9. Click **Save**.

Edit route patterns for Called-Party as dialed feature

If pre-10.6(2) Country Dial Plans have been deployed, edit certain route patterns to place the country code before the dot in the patterns.

Important: Edit all route patterns for all country dial plans deployed for the customer with the following exceptions:

- Any route pattern that has the digits 04 (emergency), 05 (service), or 11 (operator) immediately before the dot.
- Any route pattern that has the digits 01 (international) immediately before the dot, unless the country code is specified immediately after the dot.
- Any route pattern that has an X (mask digit) immediately after the dot.

Before you begin

To complete this procedure, you need to know the country code for each country dial plan deployed for the customer.

1. Log in as Provider administrator.
2. Set the hierarchy path to the customer for which you are implementing the As Dialed feature.
3. Go to **Route Patterns**.
4. Click the route pattern.
5. On the **Pattern Definitions** tab, edit the Route Pattern field.
 - If the route pattern contains the country code after the dot, move it to immediately before the dot.
 - If the route pattern does not contain the country code, add it immediately before the dot.

Example: For Great Britain:

- Change ****001.44!** to ****00144.!**
- Change ****002.!** to ****00244.!**

6. On the **Called Party Transformations** tab, change the Prefix Digits (Outgoing Calls) field from + to +<cc> where <cc> is the appropriate country code.

Example: For Great Britain, change + to +44

7. Click **Save**.

Edit route lists for Called-Party as dialed feature

If country dial plans have been deployed, use this procedure to implement the Called-Party As Dialed feature.

Important: Edit all country-specific route lists for the customer with the following exceptions:

- Emergency
 - International
 - Operator
 - Service
-

Before you begin

To complete this procedure you need to know the country-specific trunk prefix.

1. Log in as Provider administrator.
2. Set the hierarchy path to the customer for which you want to implement the Called-Party As Dialed feature.
3. Go to **Route Lists**.
4. Click the route list to edit.

- 5. Click the + to expand the Route Group Items section.
- 6. For Called Party Discard Digits, select PreDot.
- 7. For Called Party Prefix Digits, enter the appropriate trunk prefix for the country.
- 8. Click **Save**.

7.3.8. Plus number dialing customization

Tip: *Use the Action search to navigate Automate*

Overview

You can make the following customizations to improve + number dialing:

- Suppress the outside dial tone, which is unnecessary for + number dialing.
- Support Digit by Digit Dialing

The procedures to implement the customizations depend on whether you have deployed country-specific dial plans or not.

	Country-Specific Dial Plans Not Deployed	Country-Specific Dial Plans Deployed
Suppress Outside Dial Tone	1. Edit Country Dial Plan Schema to Suppress Outside Dial Tone	1. Edit Cisco UCM translation patterns to Suppress Outside Dial Tone
	2. Deploy Country Dial Plan	
Support Digit by Digit Dialing	1. Edit Country Dial Plan Schema to Enable Digit by Digit Dialing	1. Edit Cisco UCM Translation Patterns to Enable Digit by Digit
	2. Deploy Country Dial Plan	

Edit country dial plan schema to suppress outside dial tone

To suppress an unnecessary outside dial tone for + number dialing, edit the pre-11.5(1) country dial plan schema prior to deploying the country dial plan.

1. Login as the Provider administrator.
2. Go to **Dial Plan Schema**.
3. Click the country dial plan schema you want to modify.

Important: Select the country dial plan schema located closest to the customer hierarchy node.

4. Click the **Translation Patterns** tab.
5. For each translation pattern that begins with '+' and that does not contain another '+', uncheck the Provide Outside Dial tone check box.
6. Click **Save**.

Edit country dial plan schema to enable digit by digit dialing

To enable digit by digit dialing for + number calling, edit the country dial plan schema prior to deploying the country dial plan.

Important: Enabling digit by digit dialing also introduces Post Dial Delay.

1. Login as the Provider administrator.
2. Go to **Dial Plan Schema**.
3. Click the country dial plan schema you want to modify.

Important: Select the country dial plan schema located closest to the customer hierarchy node.

4. Click the **Translation Patterns** tab.
5. For each translation pattern that begins with '+' and that does not contain another '+', uncheck the Urgent Priority check box.
6. Click **Save**.

Edit Cisco UCM translation patterns to suppress outside dial tone

If pre-11.5.1 country dial plans have been deployed, edit the Cisco UCM translation patterns to suppress an unnecessary outside dial tone for + number dialing.

1. Log in as the Provider administrator.
2. Set the hierarchy path to the customer for which you are suppressing the outside dial tone.
3. Go to **Translation Patterns**.
4. Filter the translation patterns to see only + numbers for a country dial plan.
 - a. Click the funnel-shaped filter icon on the Translation Pattern column heading.

- b. Select **Starts With** as the Filter Type.
 - c. Enter + in the Value field.
 - d. Click + to add another filter.
 - e. Select **Partition** as the Column.
 - f. Select **Contains** as the Filter Type.
 - g. Enter <ISO-CC>DP in the Value field, where <ISO-CC> is the three letter ISO country code for a country dial plan deployed for the customer. For example, for a US customer enter USADP.
 - h. Click **Apply**.
5. Click each translation pattern except for ones that contain more than one '+’.
 6. Uncheck the **Provide Outside Dial Tone** checkbox.
 7. Click **Save**.

Edit Cisco UCM translation patterns to enable digit by digit dialing

If country dial plans have been deployed, edit the Cisco UCM translation patterns to enable digit by digit dialing.

Important: Enabling digit by digit dialing also introduces Post Dial Delay.

1. Log in as the Provider administrator.
2. Set the hierarchy path to the customer for which you are enabling digit by digit dialing.
3. Go to **Translation Patterns**.
4. Filter the translation patterns to see only + numbers for a country dial plan.
 - a. Click the funnel-shaped filter icon on the Translation Pattern column heading.
 - b. Select **Starts With** as the Filter Type.
 - c. Enter + in the Value field.
 - d. Click + to add another filter.
 - e. Select **Partition** as the Column.
 - f. Select **Contains** as the Filter Type.
 - g. Enter <ISO-CC>DP in the Value field, where ISO-CC> is the three letter ISO country code for the country dial plan deployed for the customer.
For example, for a US customer enter USADP.
 - h. Click **Apply**.
5. Click each translation pattern except for ones that contain more than one '+’.
6. Uncheck the **Urgent Priority** checkbox.
7. Click **Save**.

7.3.9. Correct device-based routing CoS to enable SNR

Tip: *Use the Action search to navigate Automate*

Overview

In early versions of Automate (v11.5), country dial plans were configured with the PreDBRteSel-PT route partition in the site DBRDevice Calling Search Space (CSS). This configuration causes problems with Single Number Reach (SNR). The correction is to remove the PreDBRteSel-PT route partition from the site DBRDevice calling search space, and add it to each device-based routing Class of Service (CoS) CSS for the site.

If you have deployed country dial plans, correct the deployed CSS using Correction for SNR If Dial Plan Deployed.

If you have not deployed country dial plans, correct the country dial plans schemas using Correction for SNR If Dial Plan Not Deployed.

- Correction for SNR If Dial Plan Deployed
- Correction for SNR If Dial Plan Not Deployed

Correction for SNR if dial plan deployed

This procedure corrects site level Class of Service CSS to enable Single Number Reach (SNR).

Perform this procedure for each site where you have deployed a site dial plan.

1. Sign in as a Provider administrator.
2. Set the hierarchy path to the site.
3. Go to **Calling Search Spaces**.
4. Click the Cu<CustomerId>-<ISOCountryCode>DP-DBRDevice-CSS calling search space.
5. Remove the Cu<CustomerId>-<ISOCountryCode>DP-PreDBRteSet-PT route partition.
6. Click **Save***.
7. Go to **Class of Service**.
8. Click a device base routing (DBR) Class of Service CSS.
9. Add the Cu<CustomerId>-<ISOCountryCode>DP-PreDBRteSet-PT route partition.
 - a. Scroll down to the last route partition.
 - b. Click the Plus icon (+) to add a route partition.
 - c. Set the Index to one more than the last index value.
 - d. Select Cu<CustomerId>-<ISOCountryCode>DP-PreDBRteSet-PT for the route partition.
10. Click **Save**.
11. Repeat steps 8 through 10 for each DBR Class of Service CSS.

Correction for SNR if dial plan not deployed

This procedure updates site country dial plan schemas to correct the device based routing Class of Service CSS. This correction enables Single Number Reach (SNR) when the country dial plan is deployed to the customer site.

Perform this procedure for each affected country dial plan schema.

1. Sign in as a Provider administrator.
2. Go to **Dial Plan Schema**.
3. Click the country site schema HcsGenericSite<ISOCountryCode>DP-V<Version>-SCH. Edit the instance at the Provider hierarchy node.
4. Click the **Calling Search Spaces** tab.
5. Click the {{pwf.HcsDpUniqueSitePrefixMCR}}-<ISOCountryCode>DP-DBRDevice-CSS
6. Click **More** under the Partitions column.
7. Remove the {{pwf.HcsDpUniqueCustomerPrefixMCR}}-<ISOCountryCode>DP-PreDBRteSel-PT partition (index 2).
8. Click a device base routing Class of Service CSS.
9. Click **More** under the Partitions column.
10. Click the Plus icon (+) adjacent to the last route partition.
11. For Route Partition Name, enter {{pwf.HcsDpUniqueCustomerPrefixMCR}}-<ISOCountryCode>DP-PreDBRteSel-PT, where the <ISOCountryCode> is the three character country ISO code for this schema file (for example. USA).
12. For Index, enter a value that is one greater than the current highest route partition index.
13. Repeat steps 8 through 12 for each device based routing Class of Service CSS in the site country dial plan schema.
14. Click **Save**.

7.4. Dial plans for Caribbean countries

7.4.1. Dial plans for Caribbean countries overview

Country, ISO, and area codes for Caribbean countries

The following Caribbean countries follow North American Numbering Plan (NANP) and most of these countries have one area code, except Puerto Rico with two and The Dominican Republic with three area codes. The Caribbean countries are:

Country	ISO	Area Code
Anguilla	AIA	264
Antigua and Barbuda	ATG	268
The Bahamas	BHS	242
Barbados	BRB	246
Bermuda	BMU	441
The British Virgin Islands	BVI	284
The Cayman Islands	CYM	345
The Commonwealth of Dominica	DMA	767
The Dominican Republic	DOM	809, 829, 849
Grenada	GRD	473
Jamaica	JAM	876
Montserrat	MSR	664
Puerto Rico	PRI	787, 939
Saint Kitts and Nevis	KNA	869
Saint Lucia	LCA	758
Saint Vincent and the Grenadines	VCT	784
Saint Maarten	SXM	721
Trinidad and Tobago	TTO	868
The Turks and Caicos Islands	TCA	649
The US Virgin Islands	VIR	340

Calls to neighboring Caribbean countries will be treated similar to calls to USA or Canada. They will be treated as Call Type 03.

Since all of these countries are in the NANP dial plan, and instead of repeating the common Translation Patterns for each country, the dial plans for Caribbean Countries have been split into NANP Schema, and each Country specific Schema.

Call type options for Caribbean countries

Calls to neighboring Caribbean countries can be treated similar to calls to the USA or Canada. In this case they will be treated as Call Type 03 (Normally mobile call type, but has been reused as Calls to NANP countries including USA, Canada and other Caribbean Countries).

Since all of these countries are in the NANP dial plan, and instead of repeating the common Translation Patterns for each country, the dial plans for Caribbean Countries have been split into NANP Schema, and each Country specific Schema.

Alternatively, calls to the Caribbean countries can be treated differently than calls to USA or Canada with the use of the CariCC schema. With this schema the area codes belonging to the Caribbean countries will be call typed as Call Type 12 (International Restricted).

Use the following table as a guide when implementing dial plans for Caribbean countries.

Use of Call Type 03 or Call Type 12 for Caribbean Countries

Call Type (3)	Call Type (12)
Configure NANP schema. (The first time any Caribbean country is to be deployed, the NanpDP schema has to be specified. Subsequent Caribbean countries do not require this step.)	Configure NANP Schema. (The first time any Caribbean country schema is to be deployed, the Customer specific NanpDP schema and CariCCDP Schema is to be included along with the Country specific Schema. The subsequent Caribbean countries only need the Country specific Schema.)
Configure Site Schema	Configure CariCC schema
Configure Customer Schema	Configure Country Specific schema
Configure Calling Search spaces	Configure Feature schema
	Configure Site schema
	Configure Calling Search Spaces
	Configure Route List
	Configure Route Patterns

7.4.2. North American numbering plan schema

The NANP schema is at a customer level and consists of the common translation patterns across all the NANP countries. The following call types are covered in this schema:

- Call Type (01) - International calls outside of NANP dialed as 011+.
- Call Type (03) - Normally mobile call type, but has been reused as Calls to NANP countries including USA, Canada and other Caribbean Countries (1+NPA+NX XXXX).
- Call Type (05) - Service calls (N11).
- Call Type (07) - Premium Rate Service (e.g. 900).
- Call Type (08) - Toll Free or Free phone Service (e.g.800, 888).
- Call Type (09) - PCS (Personal Communication Service)(e.g. 500).
- Call Type (10) - Special Rate Service (SRS) calls to Directory Assistance (411, 1+NPA 555 1212).
- Call Type (11) - Operator Services (0-, 0+).

The translation patterns related to Nanp schema are assigned to the CuX-NanpDP-Defn-PT partition, where X is the customer ID.

7.4.3. Caribbean countries schema (Optional)

The Caribbean countries schema is also at a customer level and consists of all the area codes assigned to the Caribbean countries. This is an optional schema to be used only if calls to the Caribbean countries are to be treated differently than calls to USA or Canada. If this schema is not loaded, or the corresponding partition has not been assigned to the Calling Search Space, calls to other Caribbean countries will be call typed as (03). If this schema is activated, the area codes belonging to the Caribbean countries will be call typed as:

- Call Type (12) - International Restricted.

The translation patterns related to Caribbean Countries Area codes are assigned to the CuX-CariCCDP-Defn-PT partition, where X is the customerID.

7.4.4. Country-specific schema

Each Caribbean country mentioned above will have its own country specific schema:

- The Customer Schema will consist of the following call types:
 - Call Type (02) - The National call type is used if the Caribbean country has multiple area codes (DOM and PRI).
 - Call Type (05) - Service Calls if different from NANP patterns (N11) (Trinidad and Tobago).
- The Site Schema will consist of the following call types:
 - Call Type (04) - Emergency Patterns.
 - Call Type (06) - Local Call (most of these countries follow 7 digit dialing). The mobile calls are treated as local calls. If they need to be separated out, then please assign them to Call Type (02) National Calls.

7.4.5. Installing the dial plan

Tip: *Use the Action search to navigate Automate*

Specify call type 12 feature schema

The current feature schema does not support *call type 12*. To access the correct schema use the JSON file, **CallScreening-Feature-V3**.

1. Import the file: CallScreening-Feature-V3.json.
2. Within this JSON file is the schema: Customer-CallScreening-Feature-V3-SCH.









Replace the existing feature schema with Customer-CallScreening-Feature-V3-SCH schema. The screen shot is for Type 4 Schema Group. It can also be applied to other Schema Group Types.

Adding Customer-CallScreening-V3-SCH Schema

Dial Plan Schema Group [Cisco Type 4 Schema Group] Save Delete Help Back Action

General **Site Defaults** **Core Schemas** **Feature Schemas** **Country Schemas** **Custom Workflows**

+ Feature Dial Plan Schemas

	Dial Plan Schema Usage *	Dial Plan Schema Scope *	Dial Plan Schema Name *
 	Add Site ▼	Customer ▼	Customer-CallScreening-Feature-V3-SCH ▼
 	Add Site ▼	Customer ▼	CustomerToDCLIPR-Feature-V2-SCH ▼
 	Add Site ▼	Customer ▼	Customer-FONet-Feature-V3-SCH ▼
 	Add Site ▼	Customer ▼	Customer-FACnCMC-Feature-V3-SCH ▼





Specify site schema

The first time you deploy a Caribbean country, the NanpDP (North American Numbering Plan Dial Plan) schema must be specified. Deploying subsequent Caribbean countries does not require this process.

If you are using Call Type 12 the first time any Caribbean country schema is to be deployed, the Customer specific NanpDP schema and CariCCDP Schema must be included along with the Country specific Schema. The subsequent Caribbean countries only need the Country specific schema.

The example shown is for Grenada but this can be applied to any Caribbean country from the list of Caribbean countries shown.

Defining the Customer Specific NanpDP Schema and CariCCDP Schema

	Add Site ▼	Grenada ▼	Customer ▼	HcsGenericCustomerNanpDP-V1 ▼
	Add Site ▼	Grenada ▼	Customer ▼	HcsGenericCustomerCariCCDP ▼
	Add Site ▼	Grenada ▼	Customer ▼	HcsGenericCustomerGRDDP-V1 ▼
	Add Site ▼	Grenada ▼	Site ▼	HcsGenericSiteGRDDP-V1-SCH ▼

Define calling search spaces

Update the calling search spaces to include the NANP route partition as well as (if used) the CariCC route partition. The following is an example of a typical CSS.

1. Log in as the Customer administrator or the Provider administrator. For a list of the roles and tasks that can be done at each level, see Roles and Privileges.
2. Go to **Calling Search Spaces**, then insert **NANPDP Route Partitions** after the country specific Defn PT.

Calling Search Spaces Including NanDP and CariCCDP

Route Partitions		
	Partition Name *	Partition Index
⊕ ⊖	Cu1Si28-GRDDP-Local-PT	1
⊕ ⊖	Cu1-GRDDP-Defn-PT	2
⊕ ⊖	Cu1-NanpDP-Defn-PT	3
⊕ ⊖	Cu1-CarICCDP-Defn-PT	4
⊕ ⊖	Cu1-noFONet-PT	5

Route list required

A new route list is required if calls to neighboring countries are to be routed over a different trunk group. To create a new route list, refer to *Configure Route Lists*.

Create route patterns

- Following Route Patterns are to be created for Call Type 12. The following example shows RP **012 for IntlRst Call Type - no FAC no CMC. If FAC and or CMC is required, other Route Patterns can be created as required.

Route Pattern: RP **012 for IntlRst Call Type - no FAC no CMC

Pattern ^	Description	Partition	Route Filter	Associated Device
**001.1	DOM Intl Call Type - no FAC no CMC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**012.1	DOM IntlRst Call Type - no FAC no CMC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**101.1	DOM Intl Call Type - FAC no CMC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**201.1	DOM Intl Call Type - CMC no FAC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**301.1	DOM Intl Call Type - CMC FAC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL

7.5. Local breakout (LBO)

7.5.1. Local breakout (LBO) workflows

Tip: *Use the Action search to navigate Automate*

Overview

In addition to centralized breakout using the aggregation layer, customers can also connect to PSTN through a local gateway. Using a local gateway is also referred to as *Local Breakout* (LBO). For LBO, each site or location requiring LBO is equipped with a local gateway. When a local gateway is added to a location, the administrator defines the call types that can be routed through the local gateway. For example, you can select national calls to be routed through the local gateway. By default, all call types are routed by LBO.

Enable local break out custom workflows

If you have done a fresh install of Cisco Unified CDM 10.6(2) or later, your Type 1-4 Cisco Dial Plan Schema Group will already have the following Local Break Out (LBO) custom workflows specified:

- `associateLboGateway`
- `unassociateLboGateway`

However, if you have upgraded from a pre-10.6(2) version, you must update your Dial Plan Schema Group to enable these custom workflows, if you want to use Local Break Out.

1. Log in as the provider administrator.
2. Go to **Dial Plan Schema Group**.
3. Select the appropriate schema group that is in use by your customer.
4. Select the **Custom Workflows** tab.
5. Add the following Dial Plan Event to Workflow bindings:
 - `associateLboGateway > HcsDefaultAddLBOGatewayPWF`
 - `unassociateLboGateway > HcsDefaultDelLBOGatewayPWF`
6. Click **Save**.

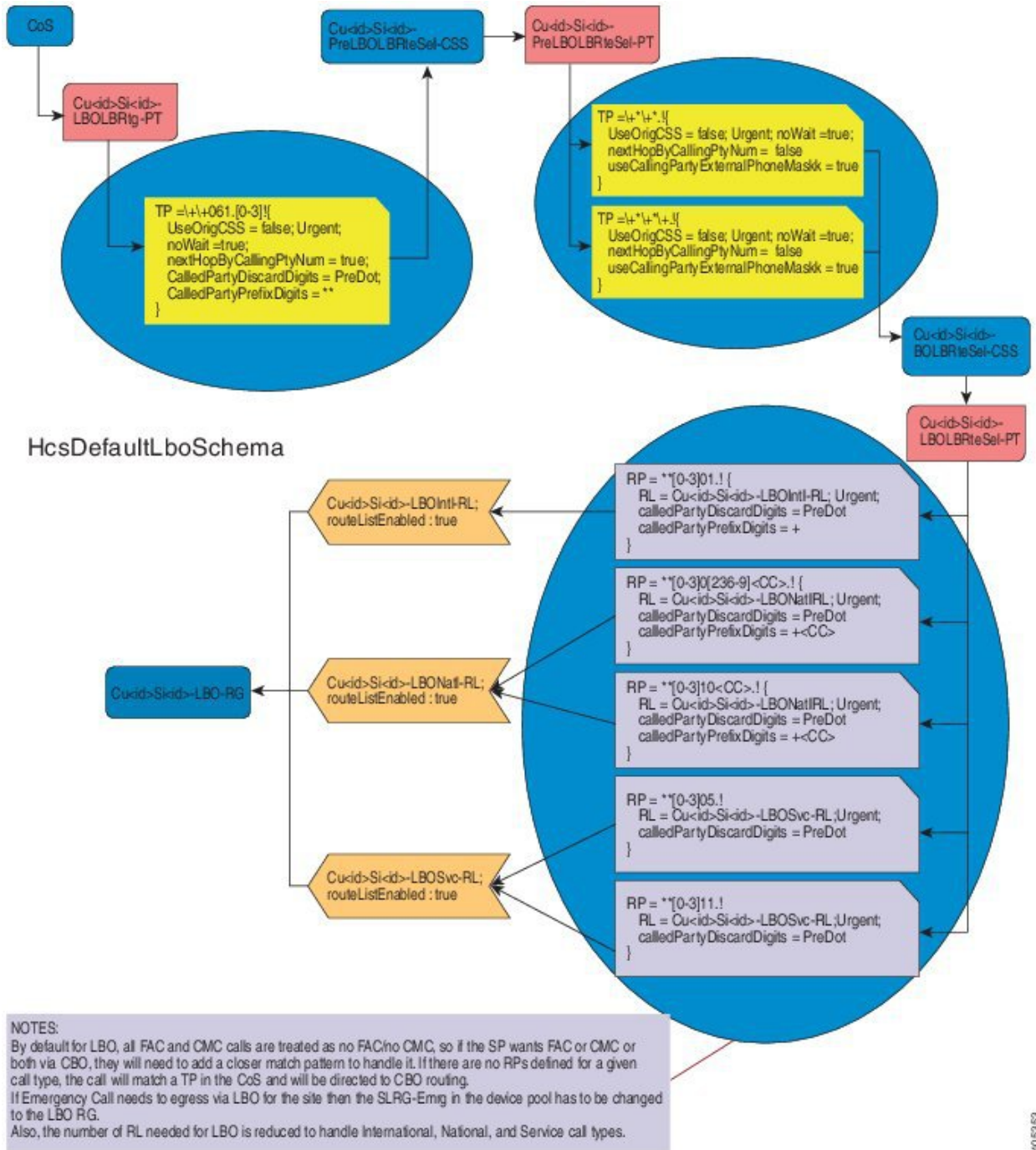
Custom workflow, `associateLboGateway`

The `associateLboGateway` custom workflow is optional. If it is not specified in the customer's Dial Plan Schema Group, when a SIP local gateway is associated with a site only the IOS Command Builders are triggered.

The `HcsDefaultAddLBOGatewayPWF` is triggered every time a SIP local gateway is associated with a site and executes the following logic:

- If the site-specific `Cu<cid>Si<sid>-LBO-RG` route group does not exist, it is created with the SIP Trunk associated with the SIP Local Gateway as a member device.
- If the site-specific `Cu<cid>Si<sid>-LBO-RG` route group exists, it is updated to include the SIP Trunk associated with the SIP Local Gateway as a member device.
- For line-based routing (LBR), the `HcsDefaultLboSchema` is deployed.

Figure 7. `HcsDefaultLboSchema`



- For device-based routing (DBR), if this is the first SIP Local Gateway associated to the site, the site default device pool `Cu<cid>Si<sid>-DevicePool` is updated, such that all the default Local Route Groups are set to the new `Cu<cid>Si<sid>-LBO-RG`.
- Once a SIP Local Gateway is associated with a site and the `HcsDefaultLboSchema` dial plan schema has been deployed, the `Cu<cid>Si<sid>-LBOLBRTg-PT` route partition can be used when constructing a site line-based routing (LBR) Class of Service (CoS) that uses local break-out.

Note: The LBR CoS must be defined such that the `LBOLBRTg-PT` (used for LBO) is higher priority than the

LBRtg-PT [used for Central Break-out (CBO)].

- By default, when more SIP Local Gateways are associated to the same site, the Cu<cid>Si<sid>-LBO-RG route group is updated to include the additional SIP Trunk associated with the additional gateway. The trunks in this route group use the Top Down distribution algorithm.

Custom workflow, *unassociateLboGateway*

The *unassociateLboGateway* custom workflow is required only if *associateLboGateway* is enabled. If it is not specified in the customer's Dial Plan Schema Group, when a SIP local gateway is disassociated from a site only the IOS Command Builders are triggered.

The *HcsDefaultDelLBOGatewayPWF* is triggered every time a SIP local gateway is disassociated from a site and executes the following logic:

- Update the site-specific Cu<cid>Si<sid>-LBO-RG route group to remove the SIP Trunk associated with the SIP Local Gateway as a member device.
- For line-based routing (LBR), if this is the last SIP Local Gateway associated with the site, the Translation Patterns are removed from the Cu<cid>Si<sid>-LBOLBRtg-PT route partition. Removing the Translation Patterns forces the class of service CSS's that use LBO to fall back to central break-out (CBO).
- For device-based routing (DBR), if this is the last SIP Local Gateway associated with the site, the site default device pool, Cu<cid>Si<sid>-DevicePool, is updated such that all the default Local Route Groups are no longer associated with Cu<cid>Si<sid>-LBO-RG.

8. Call search spaces and partitions

8.1. Calling search spaces and partitions

This chapter lists the components that are created and used by the dial plan. The Calling Search Spaces (CSSs) and associated partitions are created when the customer dial plan is added in Cisco Unified Communications Manager (UCM). The following CSSs and partitions are available to be used with SIP trunk transformations:

SIP trunk transformation CSSs

CSS Name	Description	Partitions	Description
Cu<cid>-CGPNTTransform-CSS	Per Customer Call-inGPartyNumber Transformation CSS	Cu<cid>-DN2DDI4RCCN-PT	Per customer partition contains Calling Party Transformation Pattern for a non-Emergency PSTN call. The transformation pattern is a DN or range of DNs that map to a DDI or range of DDIs. This partition is used for Calling, Redirecting and Connected number transformation.
		Cu<cid>-DN2DDI4Emer-PT	Per customer partition is used to provision Calling Party Transformation Patterns for the Emergency Call. The pattern should be in the following format - “*2*<sid>DN”, where <sid> is the internal site id (can be acquired with the macro “HcsDpSiteId” and DN is either a DN or range of DNs that map to a DDI or range of DDIs associated to the site.

CSS Name	Description	Partitions	Description
Cu<cid>-CDPNTransform-CSS	Per customer CalledPartyNumber Transformation CSS	Cu<cid>-CDPNTransfPat-PT	Per customer partition contains Called Party Transformation Pattern. Not used.
Cu<cid>-RDPNTransform-CSS	Per customer RedirectingPartyNumber Transformation CSS	Cu<cid>-DN2DDI4RCCN-PT	Per customer partition contains Calling Party Transformation Pattern for a non-Emergency PSTN call. The transformation pattern is a DN or range of DNs that map to a DDI or range of DDIs. This partition is used for Calling, Redirecting and Connected number transformation.
Cu<cid>-CNPNTTranform-CSS	Per customer Connected Number Transformation CSS	Cu<cid>-DN2DDI4RCCN-PT	Per customer partition contains Calling Party Transformation Pattern for a non-Emergency PSTN call. The transformation pattern is a DN or range of DNs that map to a DDI or range of DDIs. This partition is used for Calling, Redirecting and Connected number transformation.
Cu<cid>-IngressFromCBO-CSS	Per customer for handling Inbound Call from the trunk	Cu<cid>-E164LookUp-PT	Per customer partition contains DDIs to DNs translation patterns. Each translation pattern is a DDI or range of DDIs that map to a DN or range of DNs with the CSS set to InterSiteRouting partition (Cu<cid>-ISR-PT).
		Cu<cid>-FMCLookUp-PT	Per customer partition for mapping FMC numbers to DN. Not used.
Cu<cid>-IngressFromUnity-CSS	Per customer for handling Inbound Call from CUC	Cu<cid>-URILookUp-PT Cu<cid>-ISR-PT	Per customer partition containing a list of URIs associated to the DN. Per customer intersite routing partition contains a list of DN ranges and translation patterns with the CSS Cu<sid>-DirNum-CSS
		Cu<cid>-URILookUp-PT	Per customer partition containing a list of URIs associated to the DN.

Partitions for Class of Service

The following partitions are available when building a Class of Service (CoS) and should be ordered in the CoS CSS as shown in the following table.

Partition	Description
1. Cu<cid>Si<sid>-<ISO>DP-Local-PT	Per site partition for handling local PSTN dialing behavior, where <cid> is the unique customer id (obtain with the macro HcsDpCustomerId), <sid> is the unique customer site id (obtain with the macro HcsDpSiteId) and <ISO> is the Country ISO code (for example, United Kingdom = ISO(GBR))
2. Cu<cid>-<ISO>DP-Defn-PT	Per customer country dial plan definition. It contains a set of translation patterns associated with the dialing behavior, eliminates post dial delay, classifies it to a different call type, and prefixes the Force On-Net feature code to the Called Number as the next feature to be processed.
3. Cu<cid>-FONet-PT or Cu<cid>-noFONet-PT	Use the noFONet-PT if Force OnNet is not needed, or use the FONet-PT to enable Force OnNet.
4. One or more of the following blocking partitions: <ul style="list-style-type: none"> • Cu<cid>-BlkIntl-PT • Cu<cid>-BlkNatI-PT • Cu<cid>-BlkMobl-PT • Cu<cid>-BlkLocI-PT • Cu<cid>-BlkPRS-PT • Cu<cid>-BlkFPN-PT • Cu<cid>-BlkPCS-PT • Cu<cid>-BlkSRS-PT • Cu<cid>-BlkOpr-PT • Cu<cid>BlkAll-PT 	To block the following: <ul style="list-style-type: none"> • International call type • National call type • Mobile call type • Local call type • Premium Rate Service call type • Toll free call type • Personal Comm Service type • Special Rate call type • Operator call type • ALL PSTN call types; use only if Internal Calls is allowed
5. Cu<cid>-Allowed-PT	This partition is needed after all the blocking partitions, or if none of the blocking partitions are needed.
6. One of the following partitions is the next partition needed in the CoS CSS: <ul style="list-style-type: none"> • 24HrsCLIP-PT • 24HrsCLIR-PT • WkHrsCLIP-PT • WkHrsCLIR-PT 	This partition is needed to allow calls as described below: <ul style="list-style-type: none"> • 24HrsCLIP-PT* To allow calls 24 hours a day with calling number and name presentation set to Allowed • 24HrsCLIR-PT*To allow calls 24 hours a day with calling number and name presentation set to Restricted • WkHrsCLIP-PT*To allow calls during working hours with calling number and name presentation set to Allowed • WkHrsCLIR-PT*To allow calls during working hours with calling number and name presentation set to Restricted

Partition	Description
7. One of the following: <ul style="list-style-type: none"> Cu<cid>-FAC-PT Cu<cid>-noFAC-PT 	Use FAC-PT if Forced Authorization Code is needed, or use noFAC-PT. In addition to using the FAC-PT, the FAC feature must be manually provisioned on Cisco UCM.
8. One of the following: <ul style="list-style-type: none"> Cu<cid>-CMC-PT Cu<cid>-noCMC-PT 	Use CMC-PT if Client Matter Code is needed, or use noCMC-PT. In addition, you must manually provision the CMC feature on Cisco UCM.
9. One of the following: <ul style="list-style-type: none"> Cu<cid>-<ISO>DP-LBRtg-PT Cu<cid>-<ISO>DP-DBRtg-PT 	If Line Based Routing is needed then add the LBR routing partition (Cu<cid>-<ISO>DP-LBRtg-PT). If Device Based Routing then add the DBR routing partition (Cu<cid>-<ISO>DP-DBRtg-PT).
10. The following partitions handle internal dialing: <ul style="list-style-type: none"> Cu<cid>-PreISR-PT Cu<cid>-AllowVM-PT Cu<cid>Si<sid>-AllowInternal-PT Cu<cid>Si<sid>-Feature-PT 	These partitions handle internal dialing as described below: <ul style="list-style-type: none"> Cu<cid>-PreISR-PT per customer PreInter-SiteRouting partition Cu<cid>-AllowVM-PT per customer Allowing Voice Mail partition Cu<cid>Si<sid>-AllowInternal-PT per site Allowing Intra Site dialing partition Cu<cid>Si<sid>-Feature-PT*per site Allow Call Feature partition
11. Cu<cid>-URILookUp-PT	Partition used to handle URI dialing

Device CSSs

The following are available for configuring Device CSSs.

Calling Space	Search	Description
Cu<cid>Si<sid>-<ISO>DP-Emer-CSS		This CSS is used for devices that have lines that use Line Based Routing (LBR). It contains the Cu<cid>Si<sid>-<ISO>DP-Emer-PT which contains translation and route patterns to handle emergency calls.
Cu<cid>Si<sid>-<ISO>DP-DBRDevice-CS		This CSS is used for devices that have lines that use Device Based Routing (DBR). It contains Cu<cid>Si<sid>-<ISO>DP-Emer-PT and the DBR Route Selection partition.

Route lists created when adding a country dial plan for a customer

The following Route Lists are created when a country dial plan is added for a customer:

- Line Based Routing
 - Cu<cid>-<ISO>Intl-RL
 - Cu<cid>-<ISO>Natl-PL
 - Cu<cid>-<SIO>Mobl-PL
 - Cu<cid>-<ISO>Emer-RL
 - Cu<cid>-<ISO>Serv-RL
 - Cu<cid>-<ISO>Local-RL
 - Cu<cid>-<ISO>PRSN-RL
 - Cu<cid>-<ISO>FPHN-RL
 - Cu <cid>-<ISO>PCSN-RL
 - Cu<cid>-<ISO>SRSN-RL
 - Cu<Cid>-<ISO>Oper-RL
- Device Based Routing* Each of the Route Lists below configured with a single Name Standard Local Route Group member associated with Call Type.
 - Cu<cid>-<ISO>Intl-SLRG-RL
 - Cu<cid>-<ISO>Natl-SLRG-RL
 - Cu<cid>-<SIO>Mobl-SLRG-RL
 - Cu<cid>-<ISO>Emer-SLRG-RL
 - Cu<cid>-<ISO>Serv-SLRG-RL
 - Cu<cid>-<ISO>Local-SLRG-RL
 - Cu<cid>-<ISO>PRSN-SLRG-RL
 - Cu<cid>-<ISO>FPHN-SLRG-RL
 - Cu<cid>-<ISO>PCSN-SLRG-RL
 - Cu<cid>-<ISO>SRSN-SLRG-RL
 - Cu<Cid>-<ISO>Oper-SLRG-RL

The route group used by the above is provisioned with Automate SIP trunk and route group.

LBR route patterns can be found in Cu<cid>-<ISO>DP-LBRteSel-PT which is associated with Cu<cid>-<ISO>DP-LBRteSel-CSS.

DBR route patterns can be found in Cu<cid>-<ISO>DP-DBRteSel-PT which is associated with Cu<cid>Si<sid>-<ISO>DP-DBRDevice-CSS.

9. Telephony design and dial plan primer

9.1. Architecture primer

9.1.1. Overview

Understanding the dial plan model requires a basic understanding of the architecture and the interaction between the elements. The architecture consists of three discrete layers:

- Aggregation layer
- Infrastructure layer
- Customer-premises layer

These layers comprise the majority of the call flow interactions.

The aggregation layer handles inbound/outbound call routing between customer premises and PSTN, while all intra-customer interactions are handled at the infrastructure layers.

The numbering plan facilitates this design, allowing for a simple routing methodology, and is discussed in this section.

- Aggregation Layer
- Customer Premises Layer
- Voicemail - Cisco Unity Connection (CUC)

9.1.2. Aggregation layer

The aggregation layer is responsible for the following:

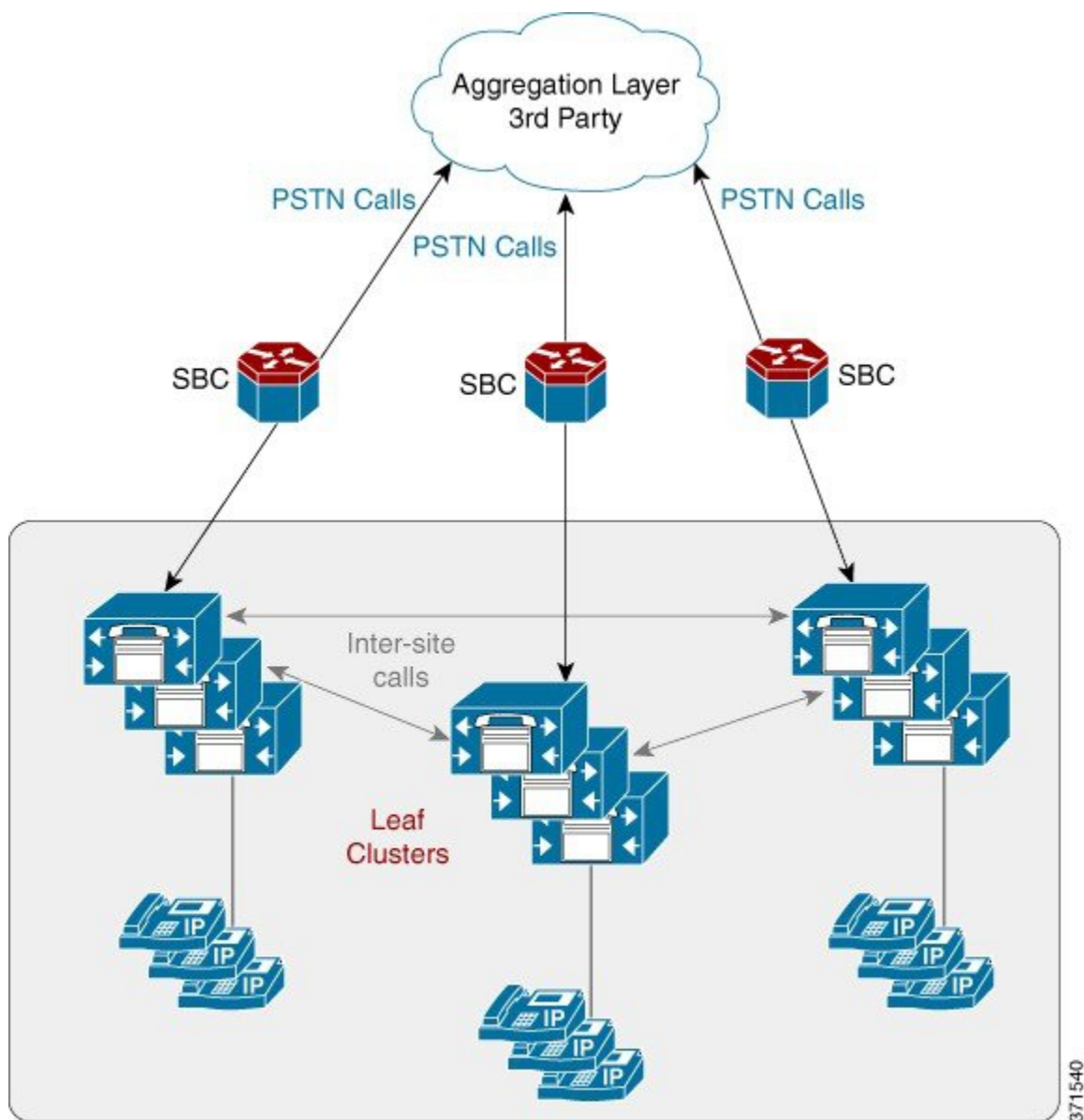
- E.164 call routing
- Routing E.164 calls between two Automate customers
- Routing calls from the PSTN to IP Lines on Cisco Unified Communications Manager (UCM) clusters
- Routing calls from IP Lines (on UCM clusters) to centralized PSTN breakout
- Routing calls to other components within the aggregation layer
- Routing calls to Cisco Webex (can be a separate route)
- Routing calls to Cisco Contact Center Enterprise (can be a separate route)

The primary use of the aggregation is to aggregate central PSTN traffic. Any call that is received at the aggregation layer must be treated as a call either from or to the PSTN. The aggregation supports PSTN breakout like SS7 and SIP.

A service provider using an early version of Automate (VOSS-4-UC v10.x/11.5(x)) can only use the customer's own aggregation device (third party).

The aggregation layer is connected to the UC applications through the third-party session border controller as shown in the following figure. The SBC is used mainly as a media aggregation point. The SBC is used for media anchoring and VRF translation functions. Additionally, it provides SIP header normalization functions for inter-operating with various service provider networks. The SBC is configured manually; it is not provisioned automatically from Automate. For signaling, there is one-to-one mapping of trunk from leaf clusters to signaling aggregation node, IMS or any other third-party softswitch. In general, there is no dial plan requirement for the SBC.

Figure 1. Logical diagram showing SBC adjacency for each customer



Note: The Forced On-Net feature in UCM can be used between users of a customer; that is, a user dialing the PSTN number of another user of the same customer.

Calls between various clusters and the aggregation traverse SIP trunks. SIP is the only protocol that must be configured for these types of trunks.

9.1.3. Customer premises layer

This layer connects customer endpoints: phones, mobile devices, and local gateways to the SP network; and provides end user interfaces to network management software. This layer may handle PSTN routing and Survivable Remote Site Telephony (SRST) if a local breakout design is used. This layer can also include C-series servers for UC applications as part of the Extender deployment model.

9.1.4. Voicemail - CUC

Cisco Unity Connection (CUC) is connected to the leaf clusters as a SIP connection (telephony integration). For each Cisco UCM IP phone line that exists on the leaf cluster that requires voicemail, there is also a voice mailbox definition on the CUC. On CUC, the voice mailbox definition is associated to the telephony integration and leaf cluster that contains the line definition. The leaf clusters have a voicemail pilot number defined that helps to route calls to the CUC. With this scenario, each leaf cluster can use the same number for the voicemail pilot number.

Note: For Shared Architecture Dial Plan (G3) dial plan, the voicemail pilot number can be shared within a customer (that is, across locations) but it has to be unique across customers that belong to the shared architecture of UCM and CUC.

9.2. Numbering plan design

9.2.1. Directory numbers classification

The Cisco HCS dial plan enables the creation of directory numbers (Cisco Unified Communications Manager Internal DNS) with these choices of characteristics:

Dial plan classification

Dial Configuration Type	Plan	Site tion (SLC)	Loca- Code	IDP (Inter Site Prefix (ISP))	IDP in DN	Extension Dial- ing Prefix (EDP)	Extension Format
1		Yes		Yes	No	Unnecessary with ISP	SLC + Ext, No ISP in SLC
2		Yes		Yes	Yes	Unnecessary with ISP	ISP+SLC+Ext (ISP is part of SLC)
3		Yes		No	No	Yes/No	SLC+Ext and no ISP, can be with or without EDP
4		No		No	No	Not Applicable	Ext (Flat Dial Plan/ no SLC)

9.2.2. Extension Numbers

An extension number is composed of one or more digits in the range 0 to 9 and must be unique within a site, although the same extension number can exist in multiple sites (that is, overlapping extension numbers). The length is determined on a site-by-site basis.

Extension number ranges chosen should not overlap with the intersite prefix or with PSTN access prefixes. To prevent overlap, do not use extension number ranges starting with a PSTN access prefix such as 9, or the chosen intersite prefix, commonly 8. Overlap between extension numbers and the emergency number at any location must be avoided. For example, if the emergency number is 112, then extension 112 or extension number ranges 112X (where X is one or more digits) are not permitted.

For a Flat Dial Plan (G2), the extensions and the internal DNs are the same. Extensions under Flat Dial Plan (G2) cannot overlap and have to be unique across all locations for a customer.

For a Type 4 Flat Dial Plan, the extensions and the internal DNs are the same. Extensions under Flat Dial Plan cannot overlap and have to be unique across all locations for a customer.

9.2.3. Site location codes

A Site Location Code (SLC) is a number composed of one or more digits in the range 0 to 9, used to prefix the extension number to create a unique directory number (DN). This enables the same extension number to exist in multiple sites (that is, overlapping extension numbers). Only one SLC is allowed at each site, and the SLC must be unique within the customer. An SLC is used to group a set of DNs to a site that has similar characteristics. The length may be determined on a site-by-site basis. Automate does not allow a site code to be created that has either of the following characteristics:

1. Has a first portion that matches an existing site code
2. Matches the first portion of an existing, longer site code

For example, if site code 123 already exists and the user attempts to create site code 12, then the provisioning system does not allow it because site code 12 matches the first portion of 123. Similarly, if the user attempts to create site code 1234, then the provisioning system does not allow it because the existing site code 123 matches the first portion of 1234.

The restrictions above are required to prevent calls from being routed to the wrong site partitions due to overlapping numbers.

Note: Within the document, *site* and *location* are used interchangeably.

Note: There are no SLCs for Flat Dial Plan (G2).

Note: There are no SLCs for Flat Dial Plan (Type 4).

9.2.4. Full national number

In Automate and the Dial Plan model, Full National Number (FNN) is a user number and does not include the area code. FNN is used in number construction with other options to build the external phone number mask on Cisco UCM.

9.2.5. E.164 number

The dial plan is structured such that the calling and called party numbers for all inbound PSTN calls entering the Cisco UCM are in an E.164 format. The conversion to E.164 takes place at the aggregation layer or local gateway. Similarly, the calling and called party numbers for all outbound PSTN calls leaving the Unified Communications Manager are also in an E.164 format. The conversion to E.164 takes place at the Cisco UCM.

The format of the E.164 number is: `+#COUNTRY##NATCODE##FNN#`, where:

- '+' is the International Escape Character
- '#COUNTRY#' is the Country Code (1 for United States, 44 for United Kingdom, and so on)

Note: Some countries do not use area codes; for example, Singapore.

#NATCODE# - Area Code #FNN# - PSTN Subscriber Number

9.2.6. Intersite prefix

The intersite dialing prefix (ISP) is optional and customer wide, and it tells the dial plan that the user is making an on-net call, and that the digits to follow must be in the format of a site location code (SLC) and an extension number. The ISP is a single digit number in the range 0 to 9 and must be unique within the customer's network. The ISP is deployment configurable to any value, but must not overlap with the PSTN dialing prefix or emergency number. The ISP is an optional configurable value within a customer's dial plan.

Note: Customer-wide means that the same ISP must be used for all of a customer's sites. If the first site that is provisioned begins with the digit 8, then all other sites should also begin with the digit 8.

Under one service provider you can have the ISP as 7 for one customer and 8 for another customer.

A standalone ISP is not supported, but rather, the ISP is implemented as the first digit of the SLC, for the following reasons:

- Corporate Directory Support*If the ISP is not included in the site code, then after directory lookup, you must manually insert the ISP before call completion.
- Callback Support*If the ISP is not included in the site code, then the calling party number is not contained in the ISP. You must manually insert the ISP before call completion.

ISP does not apply to Type 4 Dial Plans.

9.2.7. PSTN access prefix

The PSTN prefix is defined on a country basis. It is specified for each service provider for each country and each customer in the country. When the caller dials a PSTN number with a PSTN access prefix (typically a 9 in the United Kingdom and United States), this tells the dial plan that the caller is making an off-net call.

When the caller dials the PSTN breakout number, the dial plan routes the call to the correct PSTN breakout location, whether it is a central or a local gateway.

10. Limitations in Cisco UCM

10.1. Call limitations

This section explains the limitations and observations in the looping dial plan with the proposed solutions.

Call Type	Observation	Proposed Solution
Incoming calls from PSTN forwarded via: <ul style="list-style-type: none">• Call Forward All back to the PSTN• Call Forward All, No Answer, . . . To Voice-Mail• SNR• Dial Via Office	For any such call types or features, creating an outbound Call Leg based on the restricted A - Number by Cisco UCM, fails if the incoming calling party is anonymous. In this scenario, the calling party number does not have a PAI field and the From field is set to "anonymous" with no digits in the incoming CLIR PSTN call. For security purposes, HCS prefixes a dial plan pattern (for example, +*+*) to the incoming calling party number to "anonymous". If the Cisco UCM pattern does not have the capability of that matching letter (dial plan pattern), the call fails. Also, UCM cannot match the dial plan pattern (for example, +*+*) because the calling party number ("++*+*anonymous") is treated as enbloc by Cisco UCM.	Insert a dummy PAI in Cisco UCM with a Lua script. <ul style="list-style-type: none">• INBOUND: If there is no P-Asserted-Identity (PAID), set the PAID to <customer-defined-dummy-DN> and set the privacy to restrict the number.• OUTBOUND: If the PAID is <customer-defined-dummy-DN>, remove the PAID

Index

F

Feature

- Feature Number Management, [31](#)

Flowchart

- Audit Number Inventory, [61](#)

- E164 Inventory Management (*Provider*), [64](#)

- Number Cooling, [56](#)

N

- Number Management (*Feature*), [31](#)

Q

Quick Add User (*Feature*)

- Feature Number Management, [50](#)

Quick User (*Feature*)

- Feature Shared Line Across Sites, [229](#)