VOSS-4-UC
Provider HCS Dial Plan Management Support Guide

Release 19.3.3

Jul 09, 2020

Legal Information

Please take careful note of the following legal notices:

- Copyright © 2020 VisionOSS Limited.
  All rights reserved.
- VOSS, VisionOSS and VOSS-4-UC are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- The terms Cisco, Movius, MeetingPlace, Netwise and all other vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

Security Information

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

Contents

1 Overview

1.1. Telephony, Design and HCS Dial Plan Overview

VOSS-4-UC provides automation and standardization to Unified Communications Manager and other elements such as IOS devices, Cisco Unity Connection, and Cisco Unified in a repeatable way.

Bulk loaders can be employed to provision and onboard customers. Central to this goal, the routing architecture and associated element configuration meet in a configurable model that is used within VOSS-4-UC.

In this guide, the model is referred to as the HCS Dial Plan Model and HCS Dial Plan or simply Dial Plan Model and Dial Plan.

Important: Only the VOSS-4-UC Provider solution supports the HCS dialplan tools and the solution in the same way that it is supported in CUCDM.

The main purpose of the Dial Plan Model is to create a preintegrated baseline configuration of Unified Communications Manager applications. The Dial Plan Model can then be integrated into the platform and the service provider infrastructure with minimal effort. The Dial Plan Model configures not only the end customer equipment like Unified Communications Manager or on-premises routers, but also the interaction with aggregation layers using products such as Cisco Session Management Edition, or Session Border Controller for those functions. The standard configurations are provided, but the service providers must customize parts of the model for a particular environment.

For the end customers, the dial plan is designed to handle a significant portion of the corporate dialing schemes. It includes a standardized model on how to handle intrasite, intersite, and PSTN calls, generally using a site + extension methodology. It also spans advanced routing requirements of elements like central versus local breakout for PSTN calls and also handles the different numbering requirements across multiple countries.

The intersection point between the dial plan and VOSS-4-UC comes in the definition of standard telephony services that abstract Unified Communications Manager configurations into simpler choices that correspond to the feature plans a service provider wants to offer, and end customer to consume. For example, the partitions, calling search spaces, and translation patterns are predefined based on a choice of simple outbound, inbound, call forwarding, and time of day settings, which in VOSS-4-UC are exposed as service types. These services are combined into feature packages and templates that define a user or lines telephony services.

Given the central role to the architecture and the provision workflow, this document outlines the key architectural elements that define the Dial Plan Model, the mechanics of how the model is constructed, and the resulting service configurations in VOSS-4-UC. In addition, the model can be customized to fit different infrastructure requirements and customized service types.

1.2. Dial Plan Model Overview

The Dial Plan Model was formalized to facilitate a common basis for all the translation patterns, partitions, and calling search spaces, and provide consistent naming conventions. The model included G1 (Flat Dial Plan), G2 (Generic Dial Plan) and G3 (Shared Architecture Dial Plan) inter- and intra-site calling patterns. The model evolved to provide structure and consistency across deployments but was cumbersome to manage.

The Dial Plan Model in VOSS-4-UC 10.x/11.5(x) leverages templates and workflows in VOSS-4-UC 10.x/11.5(x) using json files to implement the model. The new model is more flexible and is designed to simplify dial plan management wherever possible.

The Dial Plan Model in VOSS-4-UC 10.x/11.5(x) consists of four basic, predefined call 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)

These four dial model types encompass all the functionality that was available on the previous Dial Plan Model, but in order to offer flexibility for service providers, the four types can be extended with custom schemas. Customization is managed through discrete, selectable elements in VOSS-4-UC 10.x/11.5(x).

The Dial Plan Model provides flexible features such as:

- 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 country of the customer sets the PSTN prefix for all other sites of the country for that customer.

In VOSS-4-UC 10.x/11.5(x), the administrator is asked at either the customer or site level to fill in a template which determines the Dial Plan Model that is delivered to the Cisco Unified Communications Manager and sites.

At the customer level, the Dial Plan Model is based on the following configuration elements:

- 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 Voice Mail ID?

At the site level, the Dial Plan Model is based on the following configuration elements:

- Site Name
- External breakout number
- SLC
- Extension length

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- Extension Prefix required
- Extension Prefix
- Published number
- Emergency number

High level work flows manage the following in VOSS-4-UC 10.x/11.5(x):

- Locations, Region and Device Pools per site
- Call Manager 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
- Voice Mail
- Routing
- Emergency Calling Line Identification
- Inventory Management
- Gateway Management

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2 Manage Dial Plan

2.1. Roles and Privileges

Depending on the role assigned, an administrator has the following Dial Plan privileges:

Note: 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.

Dial Plan Roles and Privileges

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)	

Continued 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)	

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

2.2. Create a Customer Dial Plan

This procedure determines the type of Cisco HCS dial plan schema (Type 1 to 4) to be used, depending on how you fill in the form.

Note: You can have only one dial plan per customer. If you try to add a second dial plan, the dial plan will fail. Once you have created the customer dial plan, Enable CSS filtering is the only setting that you can

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

modify.

2.2.1. Procedure

1. Log in as provider or customer administrator. For a list of the roles and tasks that can be done at each level, see see *Roles and Privileges*.
2. Choose **Dial Plan Management > Customer > Dial Plan**.
3. Click **Add** to add a Customer Dial Plan.
4. Perform one of the following:
   - If a Site Location Code is required for this customer, select the **Site-Location Code (SLC) based dial plan?** check box, OR
   - If an SLC is not required, go to Step 8.
5. Perform one of the following:
   - To add an extension prefix for the dial plan, select the **Use extension prefix?** check box. Enter the extension prefix in the form and go to Step 8.
   - To add an ISP for the dial plan, select the **Inter-Site Prefix required for inter-site dialing?** check box. Enter the Inter-Site Prefix (ISP). The ISP can be one digit in length.
6. If the ISP should be included in the directory number, select the **Is ISP included in directory number?** check box. If not, go to Step 8.
7. If the ISP should be included as part of the Voice Mail ID, select the **Is ISP included in Voice Mail ID?** check box. If not, go to the next step.
8. Select the **Enable CSS filtering** check box to filter the calling search spaces available when configuring a Subscriber, Phone, or Line, to site level Class of Service calling search spaces. Filtering is disabled by default, which results in all available Cisco Unified Communications Manager calling search spaces being available when configuring a Subscriber, Phone, or Line.
9. Click **Save** to add the Customer Dial Plan you defined.

   Note:

   The Customer ID is a unique, auto-generated, read-only number allocated to the customer. The Customer ID is particularly useful in shared deployments (where a cluster may be shared across multiple customers) to correlate specific elements to a customer. It appears in the Cisco Unified Communications Manager as an prefix to elements (for example Cu2Si7 identifies Customer 2, Site 7).

   Note:

   The Cisco HCS dial plan schemas are configured such that the customer-level dial plan elements are not pushed to the Cisco Unified Communications Manager until the first site for the customer is deployed. Therefore, you will not see any dial plan elements provisioned on the Cisco Unified Communications Manager until at least one site is deployed for the customer. See *Create a Site Dial Plan*.

   Note:

   When adding lines (DNs) at the site level, you must remember to define your DNs appropriately (that is, you are responsible for using ISP+SLC+EXT if you deploy a Type 2 dial plan). Otherwise your inter/intra site calls won't route. To define your directory numbers, refer to *Add Directory Number Inventory*.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.3. Create a Site Dial Plan

2.3.1. Before You Begin

A site dial plan cannot be created until a customer dial plan is created for the customer. There are attributes that are defined in the customer dial plan that are needed when creating a site dial plan.

A site dial plan does not get created automatically for a site when a site is created. Perform this procedure to associate a site dial plan with the site. After the first site for a specific customer is deployed, the customer-level dial plan elements are provisioned on Cisco Unified Communications Manager (Unified CM), followed by the site-specific dial plan elements. Each subsequent site only has site-specific dial plan elements to provision, so it takes less time to create. If there is more than one site for a customer, do not forget to apply the site dial plan to each site.

Note: Step 13 of this procedure takes a few minutes to provision the site dial plan, especially for the first site.

Each site can have one site dial plan only.

2.3.2. Procedure

1. Log in as the Customer Administrator or Provider Administrator. For a list of the roles and tasks that can be done at each level, see *Roles and Privileges*.
2. Set the hierarchy path to the site for which you want to create a site dial plan. If the hierarchy path is not set to a site, you are prompted to choose a site.
3. Choose **Dial Plan Management > Site > Dial Plan**.
4. Click **Add** to add a Site Dial Plan.
5. Modify the **External Breakout Number** if desired. The **External Breakout Number** is the PSTN prefix that is used when deploying a country dial plan. For Cisco HCS Type 1 to 4 dial plan schemas, you deploy country dial plans at the customer level. The country dial plan is not pushed to Unified CM until the first site associated with a given country is deployed. For example, if a site is associated with the United States, and it is the first site dial plan being created for the USA, the US country dial plan is deployed as part of creating the site's dial plan. Default is 9. The **External Breakout Number** is one digit in length.

   Note:

   We support only one **External Breakout Number** for each country. For example, all sites within USA have the same External break out as the first site within USA.
6. Enter the **Site Location Code** using a maximum of eight digits. The SLC must be unique across sites for a customer. Note: If the Customer Dial Plan does not use SLCs, this field does not appear.
7. Perform one of the following for sites without Inter-Site Prefixes (ISPs):

   Note: This field appears if your Customer Dial Plan does not use ISPs; for example, HCS Type 3 dial plans (SLC, no ISP, DN=SLC+EXT)

   - Select the **Use extension prefix?** check box if your customer dial plan has an extension prefix defined and you want this site to use the extension prefix, OR

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- If an Extension prefix is not defined in the customer dial plan for this site, go to the next step.

8. Enter the **Area Code**. Enter zero or more valid local area codes for the site. Specify the length of the subscriber part of the PSTN number for each area code. 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.
9. Enter the **Local Number Length**. Local Number Length is the length for the subscriber section of the entire E.164 number.
10. Select the **Area Code used for Local Dialing** check box if the area code is needed for local dialing from this site. In the US this setting determines whether you use 7-digit or 10-digit local dialing.
11. Choose the **Published number** from the drop-down of available E.164 inventory numbers, or enter a custom number.

    The site published number is the default E.164 mask when a line is associated to a phone at a particular site.
12. Choose the **Emergency Call Back Number** for the site from the drop-down of available E.164 inventory numbers, or enter a custom number.

    The 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.

    Note:

    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.

    Note: Under the **Emergency Call Back Number** drop-down, there is a **Site ID** read-only field. The **Site ID** is a unique, auto generated, read-only number for each customer site which is prefixed to elements as an identifier (for example, Cu4Si2 indicates Customer 4, Site 2).
13. Click **Save** to add the Site Dial Plan you defined. The site information is loaded on the Unified CM, and is identifiable by its Customer ID, Site ID prefix.

2.4. Update a Site Dial Plan

2.4.1. Procedure

1. Log in as the provider, reseller, or customer administrator.
2. Set the hierarchy path to the site for which you want to update the site dial plan.
3. Choose **Dial Plan Management > Site > Dial Plan**.
4. Click the Site Dial Plan you want to update.
5. In the **Dial Plan** screen, you can update the following fields:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Field	Description
Area Code	An area code associated with the site.
Local Number Length	The length of a locally dialed number for the specified area code.
Area Code Used for Local Dialing	Select this check box if 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.

Note: You can also add or delete Area Codes.

6. Click **Save**.

2.4.2. Area Code Changes

For the Cisco Type 1-4 dial plans, area code changes result in the affected local dialing translation patterns getting reapplied for the site. For new area codes, new translation patterns are deployed to the site based on the country dial plan schema associated with the site. Any translation patterns related to deleted area codes are undeployed from Cisco Unified CM based on the site's country dial plan schema. For updated area codes, related translation patterns are undeployed from Cisco Unified CM, then new translation patterns based on the updated area codes are deployed.

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. If an area code is:

- Added - The area code add IOS command is generated.
- Deleted - 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.
- Updated - The area code delete and add IOS commands are generated as necessary based on the added and deleted logic.

2.4.3. Published Number Changes

If you changed the Published Number, the following site defaults are updated if they used the previous Published Number:

- Default CUCM Phone Line E164 Mask
- Default CUCM Device Profile Line E164 Mask
- Line E164 Mask

If you changed the Published Number, then Phone Line Masks, Device Profiles, and Remote Destination Profiles that use the previous Published Number are updated. Any Phone Line Masks, Device Profiles, and Remote Destination Profiles that use a number other than the previous Published Number are not updated.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

If you changed the Published Number, previously generated E164 IOS commands for a SIP Local Gateway associated with the site are automatically regenerated.

2.4.4. Emergency Call Back Number Changes

If you have configured a Type 1 - 4 dial plan, 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.

2.4.5. What to Do Next

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

2.5. Configure Class of Service

Use this procedure to create a new Calling Search Space (CSS) or edit 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.

2.5.1. Procedure

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

   Warning:

   When adding Class of Service, ensure that you select a valid site under the customer in the hierarchy node breadcrumb at the top of the view. If you attempt to add a Class of Service at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

2. Choose **Dial Plan Management > Site > Class of Service**.

   Note:

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

3. Perform one of:
   - To add a Class of Service, click **Add**.
   - To edit an existing class of service, click on the COS to be edited, edit the required fields and then click **Save**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- To clone an existing class of service, click on the COS to be cloned, and then click **Action > Clone**.

4. Enter a unique name for the Class of Service in the **Class of Service Name** field. Try to make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_). You can also make use of macros that are available in the system to create a Class of Service name. For a list of possible macros, see “Macros and Site Defaults Macros” in the “Advanced Feature Guide”. Macros allow you to dynamically add site IDs, customer IDs, and other types of information to the CSS.

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

   Note:

   The actual CSS that is sent to the Cisco Unified Communications Manager (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.

5. Add a description for the Class of Service in the **Description** field if desired.
6. Choose route partition members to include in the Class of Service by performing the following:
   a. Click + to add route partitions.
   b. From the drop-down menu, select a route partition member.
   c. Repeat this step as required until you have selected all desired members for this Class of Service.

   Note: To remove a member from the Class of Service, click -.
7. Click **Save** to add the Class of Service that you defined. The new Class of Service appears in the table of Classes of Service and it can be edited or deleted as required.

2.6. Clone a Class of Service

Use this procedure to clone an existing Class of Service (CoS) to the same site hierarchy node with a new name.

2.6.1. Procedure

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

   Note:

   When cloning a Class of Service (CoS), ensure that you select a valid site under the customer in the hierarchy node breadcrumb at the top of the view. If you attempt to clone a Class of Service at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

2. Choose **Dial Plan Management > Site > Class of Service**.
3. Click on the Class of Service to be cloned.
4. Click **Action > Clone**.
5. Enter a unique name for the Class of Service in the **Class of Service Name** field. Make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).
6. (Optional) Add a description for the Class of Service in the **Description** field.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7. Click **Save** to save the new Class of Service.

   Note:

   You must save the cloned CoS to the same site hierarchy node as the original CoS. You cannot save the cloned Class of Service to a different site, or to a different hierarchy node.

   The new Class of Service appears in the table of Classes of Service and it can be edited or deleted as required.

2.7. Configure Short Code

2.7.1. Before You Begin

You must add a Site Dial Plan before configuring Short Code. Refer to Create a Site Dial Plan.

Use this procedure to configure Short Codes. Short codes are used for abbreviated dialing to other extensions and services.

2.7.2. Procedure

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. If you attempt to add a Short Code at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

2. Choose **Dial Plan Management > Site > Short Code**.
3. Click **Add** to add a Short Code.
4. 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
5. From the **Short Code Type** drop-down, choose one of:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

6. Enter the value for the Short Code Type in the **Value** field.
7. 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.
8. 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.

2.8. How to Configure Directory Number Routing

Use this procedure to define Directory Number Routing. 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.

2.8.1. Procedure

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

   Warning:

   When adding Directory Number Routing, 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 add Directory Number Routing at any other node in the hierarchy, you will receive an error indicating that you must be at a site.
2. Choose **Dial Plan Management > Site > Directory Number Routing**.
3. Click **Add** to add Directory Number Routing.
4. Enter a prefix in the **Directory Number Routing Prefix** field using up to 30 characters. Example: Enter 234
5. Enter a DN mask length in the **Directory Number Mask Length** field. Example: Enter 4. For this example, the Directory Number Routing would be 234XXXX, where XXXX is the mask.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

6. Click **Save** to add the Directory Number Routing that you defined. The new Directory Number Routing appears in the table and it can be edited or deleted as required.

2.9. Create a Customer

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

In VOSS-4-UC, if the customer name matches an existing customer previously configured in HCM-F, you can migrate the existing customer.

You can disable number management for the customer if required.

2.9.1. Procedure

1. Log in as provider or reseller administrator, depending on which organization manages the customer.

   Log in with the provider or reseller administrator's email address, which is case-sensitive. The provider administrator can find the reseller administrator's email address by choosing **User Management > Local Admins** and then clicking the reseller.
2. If logged in as provider, and the customer is to be added under a reseller, set the hierarchy path to the reseller.
3. Choose **Customer Management > Customers**.
4. Click **Add**.
5. Complete the following fields:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Field	Description
Customer Name	The name of the customer. This field is mandatory. Note: Any spaces in the customer name are converted to underscores in the customer local administrator name and email, if the **Create Local Admin** check box is selected. Note: A customer that has been configured in HCM-F and synced into VOSS-4-U may exist at the sys.hcs hierarchy. If the Customer Name you enter matches this customer, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this customer to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the customer, enter a different Customer Name.
Description	Customer description
Extended Name	The Extended Name can be used to provide a more descriptive name of the customer. The Extended Name is also used by external clients to correlate their own customer records with the customer records stored in HCS. This Extended Name value is synced to the Customer record in the Shared Data Repository (SDR). The Extended Name is not referenced by other components in HCS.
External Customer ID	The External Customer ID is used by the Service Inventory service. The External Customer ID is 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 which receives the Service Inventory reports. If the Service Inventory service is not being used, this field is not required. However, it can be used to correlate customer records in external systems with customer records in HCS.
Domain Name	Customer domain. This field is used to create email addresses for: • The customer default local administrator, for example: Customer1Admin@customer1.com • Site default local administrators under the customer, for example: Site1Admin@customer1.com If the customer domain is omitted, the provider domain (or reseller domain, if the customer is under a reseller in the hierarchy and the reseller domain was provided) is used instead.
Public Sector	Set the Customer as a Public Sector customer. Used for License Reporting.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Field	Description
Account ID	The Account ID is used by external clients to correlate their own customer records with the customer records stored in HCS. This Account ID value is synced to the Customer record in the Shared Data Repository.
Deal IDs	Deal IDs are used by the Hosted License Manager (HLM) service which can be activated on the Hosted Collaboration Management Fulfillment (HCM-F) server. HLM supports Point of Sales (POS) report generation. The report includes all customers on the system with aggregate license consumption at customer level. The optional **Deal ID** field associated with the customer is included in the report. Each customer can have zero or more Deal IDs. The **Deal ID** field is free text format and each deal ID is separated by a comma.
Prime Collaboration	Prime Collaboration is the application which monitors equipment used by this customer. Available Prime Collaboration applications must first be configured using the HCM-F User Interface. Then HCM-F synchronization must be executed on VOSS-4-UC. After the HCM-F data syncs into VOSS-4-UC, available Prime Collaboration applications will appear in this drop-down. Select an available Prime Collaboration application to monitor Unified Communications applications and customer equipment configured for this customer. To unassociate Prime Collaboration for this customer, choose **None**.
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	Select to disable Number Management for this customer. If selected, you cannot add Directory Numbers and E164 Numbers to inventories for this customer.

6. Click **Save**.

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.10. Directory Number Inventory

The number inventory can exist at a different level to the lines for users and devices that consume (`device/cucm/Line`) are typically at the site level with the user, service or device they are on. However, the inventory can exist at the customer level.

Use this procedure to add a single directory number (DN) or range of DNs for your customer. The DNs (extensions) you specify are validated against the Dial Plan type (Type 1 to 4). The extension length assigned to the site is enforced for site location code (SLC)-based dial plans. The maximum number of directory numbers you can add at a time is 1,000. For more information on Type 1 to Type 4 dial plans, see *Directory Numbers*.

If the allocation and availability of numbers is not site specific, for example E164 dial plan/Type 4 flat dial plan, then generally it is easier to have the inventory at the customer level. This saves moving numbers around sites to increase availability and keeps a more central inventory of available numbers. It is also key if numbers are going to be shared across sites.

If the number allocation is site specific, for example site code+ext dial plan, local breakout if E164 dial plan, then these numbers can be added or assigned to a site level.

Number inventory cannot exist at a intermediate node - only provider, customer, or site.

Number inventory is not partition or cluster aware. If the same numbers are used multiple times but in different partitions, then these all map to the same inventory number. This should be taken into account when thinking about the hierarchy level that the number inventory exists.

Also, not being cluster aware, if the same number exists on different clusters, this again will map back to the same inventory value unless numbers are assigned to the site level.

Since the inventory is not partition aware, if the same directory number is used on a cluster but in different partitions, then VOSS-4-UC workflows will update the inventory when *any* of those instances are changed - for instance, if there is a directory number 1111 in Cluster X partition and a directory number 1111 in Cluster Y partition, and the inventory entry is marked used.

If one of those instances are deleted, we check to see if there are other instances of that line based on the number only (not partition), before clearing the “used” flag. In this case, the other instance will be found and the inventory will stay marked as “used”.

Deleted numbers, e.g. as a result of a subscriber or phone delete are automatically placed into a cooling period for a predetermined amount of time as specified in the *Global Settings*. During this period the number is unavailable and cannot be used, i.e. allocated to a subscriber, phone, device, etc.

The **Cooling End Date** (yyyy-mm-dd) displays the date on which the cooling period elapses, at which time the number becomes available in the list of available numbers.

Numbers in the cooling period can also be manually removed from the cooling period, and reintroduced into the list of available numbers. See also *Number Cooling*.

Note:

- A number cooling auto expiry schedule runs daily. This schedule polls the **Cooling End 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.
- You cannot add directory numbers if **Number Management** has been disabled for the customer.
- If you are a customer with multiple sites using a Type 4 dialing plan, ensure that the directory numbers you specify are unique across sites.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- This procedure creates the DN inventory only in VOSS-4-UC. The numbers are not synced to Cisco Unified Communications Manager.
- Directory numbers can only be added or deleted. You cannot edit the directory numbers once they are added. The usage and availability property for each DN is associated with a line or taken into use by a service.
- Using bulk loader sheet or API, you can create the Directory Number (DN) Inventory only at the customer hierarchy. The Details column of Sub-transactions shows whether the DN already exists or it is creating a new DN. If any DNs exist in the range, the sub-transaction fails and parent transaction shows the status Success with Async Failures.

2.11. View Directory Number Inventory

Use this procedure to view the range of directory numbers that have been defined for a site.

Note: In VOSS-4-UC, an * can appear before a directory number in a Type 4 dial plan.

2.11.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose an available site from the hierarchy node breadcrumb at the top of the interface.
3. Choose **Dial Plan Management > Number Management > Directory Number Inventory**.

   The list of all directory numbers (DNs) configured for the site appears. You can view the list of DN numbers or delete a DN number from this page. To filter the list of directory numbers, click the up arrow beside the title of the Internal Number column. Enter the Search String you want to locate, and all directory numbers that match the search string appear.

   When a DN is first added to the inventory, the Used column is blank, and the Available column shows 'true.' The Used column changes to 'true' when the DN is put into use when a line is created and associated to a phone or subscriber. The Available column indicates that the DN is used by a device or service that does not allow a shared line (for example, a Hunt Pilot).

   The E164Number column and value on an instance form displays as in the examples below for E164 Associations (N to 1 DN), depending on the number of E164's being associated and whether a primary E164 is set or not.

   Note that the first example display is also the display for E164 Associations (N to N DN):

   - `\+27726043938`

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

   - `\+27726043938 (P)`

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

   - `\+27726043938 (P) [+8]`

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- `\+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.

Directory numbers that begin with a * (asterisk), denote DNs that are used with hunt groups, assistant lines, Contact Center lines, and so on. This type of directory number cannot be reached from an outside line. Typically, a DN 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 DN to inventory on VOSS-4-UC does not add a directory number on Cisco Unified Communications Manager until it is associated to a line on VOSS-4-UC.

The Directory Number Inventory entries appear in other end-user provisioning tasks in VOSS-4-UC as described in the table that follows. For more information on provisioning each of these tasks, refer to the VOSS-4-UC Core Feature Guide.

Task	VOSS-4-UC + Location	Notes
Lines	**Subscriber Management > Lines**	When lines are added through phones and subscriber, line details can be modified. The DN for the line cannot be modified; if you attempt to change the DN assigned to the line, the operation fails.
Phones	**Subscriber Management > Phones > Lines tab > Dirn > Pattern**	The Dirn > Pattern contains a list of available directory numbers. DNs that are used are marked as “true” in the Directory Number Inventory. Only available DNs are listed.
Subscribers	**Subscriber Management > Subscribers > Phones > Lines > Dirn**	The Dirn > Pattern contains a list of available directory numbers. DNs that are used are marked as “true” in the Directory Number Inventory. Only available DNs are listed.
	Subscriber Management > Subscribers > Voicemail	The “Voicemail Line” list contains DNs provisioned to lines.
Quick Add Subscribers	**Subscriber Management > Quick Add Subscriber > Lines > Directory Number**	The Directory Number list contains available directory numbers. DNs that are used are marked as “true” in the Directory Number Inventory. Only available DNs are listed.
PLAR (Hotdial)	**Subscriber Management > PLAR (Hotdial)**	DNs provisioned to lines are displayed in the Hotdial Destination Pattern list
Hunt Groups	**Subscriber Management > Hunt Groups > Members> Directory Number**	DNs provisioned to lines are displayed in the Pattern list
Call Pickup Groups	**Subscriber Management > Call Pickup Groups > Call Pickup Group > Line**	DNs provisioned to member lines are displayed in the Pattern list

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.12. Add Directory Number Inventory

Note: You must deploy a customer and site dial plan before performing this procedure.

1. Log in as provider, reseller, or customer administrator.
2. Choose an available customer from the hierarchy node breadcrumb at the top of the interface.
3. Choose **Dial Plan Management > Number Management > Add Directory Number Inventory**.
4. From the **Site** drop-down menu, choose the site for which you are adding directory numbers. Leave this field empty to add customer level directory numbers.

   Note:

   Customer level directory numbers can only be created for dial plans that do not use site location codes (flat dial plans). Attempting to create customer level directory numbers for site location code-based dial plans result in an error instructing you to specify a site when adding new DN inventory.
5. Using the **Extension Length**, **Site Location Code**, and **ISP** read-only fields as a guide for the site, enter the first number for the DN range in the **Starting Extension** field.

   Note:

   For a Type 4 dial plan (no SLCs), the **Starting** and **Ending Extension** fields must contain no more than 16 digits each, including the + sign before the DN number, if used. For Types 1 to 3 dial plans, the **Starting** and **Ending Extension** fields must be less than or equal to the site Extension Length. If the **Starting** or **Ending Extension** field length is less than the site Extension Length, the DN number is padded with zeroes until its length equals that of the site Extension Length.

   For a Type 4 dial plan (no SLCs), the **Starting** and **Ending Extension** fields may contain a * prefix (asterisk) before the 15-digit directory number. The * prefix denotes DNs that are used with hunt groups, assistant lines, Contact Center lines, and so on. This type of directory number cannot be reached from an outside line and cannot be associated with E.164 numbers. Typically, a DN 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.

   Example: If the **Extension Length** field shows four digits for a Type 3 Dial Plan, ensure that you enter a number containing four digits or less in the **Starting Extension** field. For example, DN 1234. If you enter DN 123, the extension number is created as DN 0123.
6. (Optional). Using the **Extension Length**, **Site Location Code**, and **ISP** read-only fields as a guide for the site, enter the last number for the DN range in the **Ending Extension** field. If you are adding a single DN, the ending number is the same as the starting number.

   Note:

   The maximum number of directory numbers you can add is 1,000 at a time. If you need more than 1,000 directory numbers, repeat this procedure as required to add ranges.
7. Enter a Tag name for the entered range to allow for tag filtering of the inventory list available from **Dial Plan management > Number Management > Directory Number Inventory**.
8. Use the following fields to input additional information (free text) for: **Description**, **Extra1** to **Extra3**.

   The **E164Number** field is disabled for manual input (but can be bulk loaded). It is automatically populated when E164 numbers are associated with Directory Numbers from **Dial Plan Management > Number Management > E164 Associations (N to N DN)** or **Dial Plan Management > Number Management > E164 Associations (N to 1 DN)**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

The E164Number value on an instance form displays as in the examples below for E164 Associations (N to 1 DN), depending on the number of E164's being associated and whether a primary E164 is set or not.

Note that the first example display is also the display 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]`

9. Click **Save** to save the single DN or DN range.

Note: You can verify that the directory number or numbers were added correctly by navigating to **Dial Plan Management > Number Management > Directory Number Inventory**.

Columns for the Tag, E164Number and other additional information fields are also shown.

2.13. Number Cooling

2.13.1. Pre-requisites

The Number Cooling feature must be enabled and configured in *Global Settings* before it will work.

2.13.2. Overview

If this feature is *enabled*, when a directory number used by a device or service, e.g. phone, device profile, hunt group pilot etc. becomes unused and available by either unassigning it from the device or service or by deleting the device or service, then the number is automatically moved into a cooling period and marked as unavailable for a pre-configured number of days.

During this cooling period, the number cannot be reused until either the cooling period has elapsed, or until a provider administrator has manually removed the number from the cooling period. Only once the number has been removed from the cooling period will the directory number be reintroduced into the pool of available numbers for allocation to a subscriber, phone, device etc.

The **Number Cooling** form allows a provider administrator to manually add directory numbers to a cooling period (thereby *removing them from* the list of available numbers), or to manually remove directory numbers from a cooling period (thereby *adding them back* to the list of available numbers).

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.13.3. Apply cooling

1. Navigate to the required hierarchy level (Provider or Customer) from which you want to add numbers to a cooling period.
2. On the **Number Cooling** form, choose **Apply cooling** from the **Select Action** drop-down.
3. Enter an optional cooling duration in days (max = 999) to apply to the selected numbers. This setting overrides the value set in their global settings. If this field is left blank, then the cooling duration set in the global settings for each number will apply.
4. Set **Filters** to determine which numbers will be included in the **Available** box in the **Select Numbers** area, these include:
   - **Include available numbers**
   - **Include cooling numbers**
   - **Contains**. Used to further refine the numbers displayed in the **Available** box.
   - **Show numbers at/below hierarchy**. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
5. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box. Note that the **Available** box will not display numbers that are used, i.e. it will only display numbers that are unused and available.
6. Click **Save**. The selected number/s are placed into a cooling period and will no longer be available for use until the cooling period has elapsed or until they have been manually removed from cooling.

2.13.4. Remove from cooling

1. Navigate to the required hierarchy level (Provider or Customer) from which you want to remove numbers from a cooling period, i.e. add them back into the list of available numbers.
2. On the **Number Cooling** form, choose **Remove from cooling** from the **Select Action** drop-down.
3. Set **Filters** to determine which numbers will be included in the **Available** box in the **Select Numbers** area, these include:
   - **Include cooling numbers**
   - **Expires from cooling within (days)**.
   - **Contains**. Used to further refine the numbers displayed in the *Available* box.
   - **Show numbers at/below hierarchy**. Allows you to select a lower hierarchy level than the one selected on the hierarchy breadcrumb.
4. Select one or more numbers in the **Available** box and click **Select** to move them to the **Selected** box.
5. Click **Save**. The selected number/s are removed from the cooling period and are available for allocation to a subscriber or phone, etc.

See also:

- *Global Settings*
- *Directory Number Inventory*
- *Run the Directory Number Inventory Audit Tool*

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.14. Run the Directory Number Inventory Audit Tool

When you run the Directory Number Inventory (DNI) Audit Tool, the tool checks and updates your directory number inventory since the last data sync. A sync of `device/cucm/Line` from the Unified CM will result in various line types being brought in - including lines assigned to devices, CTI devices, and so on - essentially anything that would be seen under Directory Numbers in Unified CM.

This will create a number inventory entry for all the `device/cucm/Lines` that are in the system and at the site level. Any lines not at the site level will not be processed in the audit tool.

Note: This can result in inventory entries being created for lines that are not just user device related, for example CTI ports, CTI route points, and so on. The Audit will not remove number inventory entries if a corresponding `device/cucm/Line` does not exist, for example if it is removed outside of VOSS-4-UC.

The Number Inventory audit then includes logic to then determine if a number is used or not and to set the number inventory value accordingly. That logic handles the following cases:

- If a line is assigned to at least one of: phone, device profile, or remote destination profile, then it will be marked used = true and available will be left as true.
- If a number is used as a Hunt Pilot - it will mark the number used = true and available = false.
- Any other usage of the line is not handled, for example CTI route point. So while these numbers are added to the inventory, they will not be marked used or unavailable through the audit process.

When you run the tool, it creates new DNs for lines that don't have them.

You specify where you want the tool to run and create a new DN inventory:

- **Customer Create**
  - Always creates new DN Inventory at the customer hierarchy level.
  - This option is only available for non-SLC dial plans, for instance Type 4 or non-SLC shell dial plan.
  - The DN inventory will be created at Customer hierarchy if the line exists at the customer level or at a site. The reason is that even if the administrator moves the line to a site later, the DN inventory at the customer level still applies. If the DN inventory already exists, it will be updated.
- **Site Create**
  - Always creates new DN Inventory at the site hierarchy level.
  - This option applies to any type of dial plan.
  - The DN inventory is created at the first site the line is encountered. If more than one line with the same pattern but different partitions exist, the DN inventory will be created for the first line encountered with that pattern.
  - If the line exists at customer level, a warning message is logged and the DN inventory is not created. If the DN inventory already exists, it will be updated.
- **Smart Create**
  - Create new DN Inventory at the site hierarchy level.
  - If the line exists at a site and is not used by a phone in another site, this option creates a new DN inventory at the hierarchy where the line exists.
  - If the line exists at a site, is referenced by one or more phones in other sites, and the dial plan type is non-SLC, thats is type 4, this option creates a new DN inventory at the Customer level.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

  - If the line exists at a site, is referenced by one or more phones in other sites, and the dial plan type is SLC, that is type 1-3, a new DN inventory is created at the site where the line exists.
  - If the line exists at customer level, a warning message is logged and the DN inventory is not created. If the DN inventory already exists, it will be updated.

For sites using Site Location Code-based dial plans, DN inventories can be created only at the Site hierarchy. The option to create DN inventories at the Customer hierarchy is unavailable in this case.

The DN Inventory Audit Tool will mark data/InternalNumberInventory instances as Shared across sites if a line is associated with multiple devices.

From **Directory Number Inventory**, you can see a list of DNs and move, delete, and export them as desired.

Log Messages provides information and warning messages generated by the Directory Number Inventory Audit Tool.

Note: You cannot run the Directory Number Inventory Audit Tool if number management has been disabled for the customer.

2.14.1. Common Errors and Caveats

- Duplicate device profiles (same profile name) in different clusters.

  Ensure device profiles are not duplicated across the sites.
- Duplicate phones (same MAC) in different clusters.

  Ensure phones are not duplicated across the clusters
- Same directory number in one or more clusters.

  Ensure directory numbers (even in different partitions) are not duplicated across clusters.
- Numbers that are in a Cooling state will not be audited.

2.14.2. Procedure

1. Log in to VOSS-4-UC as provider or reseller administrator.
2. Open the **Directory Number Inventory Audit Tool** form.
3. If prompted, choose the correct hierarchy and click **OK**.

   Note: The tool can only be run from Customer hierarchies. If you run the tool from a hierarchy that is not of type Customer, the tool will automatically provide you with a valid Customer hierarchy choice.

   ---

4. From the **Directory Number Inventory Creation Policy** drop-down, choose an option.

   Note: Customers with Site Location Code-based dial plans will not see the **Customer Create** option.

   ---

5. Click **Save**.

The DN inventory is updated at the hierarchy you specified and below.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.15. E.164 Inventory Management

2.15.1. E164 Inventory Management

E.164 Inventory Management provides Direct Dial-In (DDI)/Direct Inward Dialing (DID) mapping to Directory Numbers (DN) using translation patterns in the VOSS-4-UC. The DDI-to-DN mapping allows you to route incoming PSTN calls to the appropriate internal directory number.

E.164 Inventory Management includes the ability to:

- Add, view, and delete E.164 number inventory
- Associate a range of E.164 numbers to a range of DNs
- View associated range of E.164 numbers to a range of Directory numbers
- Disassociate a range of E.164 numbers from a range of DNs
- Associate a range or set of E.164 numbers to a single DN
- Disassociate a range or set of E.164 numbers from a single DN
- View single Directory number associations

The E.164 inventory is available in the drop-down menus for Site Published Number and Emergency Number when creating a Site Dial Plan.

2.15.2. Add E.164 Inventory

Use this procedure to define an inventory of E.164 numbers available to users.

Important:

Each addition to the E.164 Inventory must contain a unique set of numbers. That is, you cannot assign the same number more than once (globally).

Note: In VOSS-4-UC, you can define E.164 Inventory at the customer level.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to point to the customer for whom you are adding the E.164 inventory.
3. Choose **Dial Plan Management > Number Management > Add E164 Inventory**.
4. Provide the following information:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Fields	Description
Site	For a site-specific E.164 inventory, select the customer site. For a customer-wide E.164 inventory, leave this field unset.
Country	Select the country associated with the E.164 inventory. If a site was specified, this field is automatically populated with the country associated with the site. This field is mandatory.
Country Code	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	Enter the starting number of the range of E.164 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. This field is mandatory.
Ending Number	Enter the ending number of the range of E.164 numbers. The format is the same as the **Starting Number**. This field is optional. If not provided, the single E.164 Number specified in the Starting Number is added. If provided, the range of E.164 Numbers is added: **Starting Number**, **Ending Number**, inclusive. A maximum of 1000 numbers can be added at a time.
Number Type	Number type - geo, non geo, etc. Informational only. The field may be hidden.

5. Click **Save**.

2.15.3. Associate a Range of E.164 Numbers to a Range of Directory Numbers

Use this procedure to associate a range of E.164 numbers with a range of directory numbers (DN) at a customer or site. These associations create Direct Dial Inward (DDI) associations so that incoming PSTN numbers are routed to directory numbers.

If you create the association at a site, you can mix customer-level DNs and E.164 numbers with site-level DNs and E.164 numbers.

Note:

- In VOSS-4-UC, the event related to SIP Local Gateway is generated as a result.
- Only DNs or E.164 numbers that are not currently associated are available for association.

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to point to the customer or site where you want to associate E.164 numbers with directory numbers.
3. Choose **Dial Plan Management > Number Management > E164 Associations (N to N DN)**.
4. Click **Add**.
5. Provide the following information:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Field	Description
Range	Select one of these ranges: Note: The range values you select map to the mask value when the association translation pattern is created. For example, when 10 is selected, all E.164 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 nonzero number. Likewise, when 100 is selected, the E.164 number and DN end in two zeros. This pattern results in a mask of XX. • 1 - To list all E.164 numbers and DNs • 10 - To list all E.164 numbers and DNs that end in one zero (0) • 100 - To list all E.164 numbers and DNs that end in two zeros (00) • 1000 - To list all E.164 numbers and DNs that end in three zeros (000) This field is mandatory and affects what appears in the fields that follow.
E164 Number	Choose the starting number of the range of E.164 numbers from the drop-down menu. For a customer-level association, only customer-level E.164 numbers are available. For a site-level configuration, both customer-level and site-level E.164 numbers are available. This field is mandatory.
DN Number	Choose the starting extension number from the drop-down menu. This field is mandatory. Note: You cannot associate extension numbers that begin with the prefix '*' (asterisk) or '#" (hash).

6. Click **Save**.

- When listing the Directory Number Inventory and displaying a directory number, the E.164 Number format is as listed in *View Directory Number Inventory*.
- For a site-level association, a translation pattern that is used to route inbound PSTN calls to their associated DNs is created on the Unified CM. This pattern is the mapping between the E.164 range and DN range.
- For a customer-level association, a translation pattern is created on each Unified CM cluster that has a dial plan provisioned.
- For a site-level association, 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.
- For a customer-level association, if the E.164 number has the same country as any SIP Local Gateway configured for the customer, 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.

2.15.4. Associate a Set of E.164 Numbers to One Directory Number

Use this procedure to associate a set of E.164 numbers with one Directory Number (DN) at a customer or site. For example, you could associate a set of E.164 numbers for the sales department with an attendant's DN.

If you create the association at a site, you can mix customer-level DNs and E.164 numbers with site-level DNs and E.164 numbers.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

You can optionally specify a primary E.164 number to associate with the DN. This step can be useful when you perform a DN-to-E.164 translation (for example, when provisioning translation rules for LBO gateways) and the DN is associated to more than one E.164 presentation.

Note:

- You cannot associate numbers if Number Management has been disabled for the customer.
- Only DNs or E.164 numbers that are not currently associated are available for association.

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the customer or site where you are associating a set of E.164 numbers with one DN.
3. Choose **Dial Plan Management > Number Management > E164 Associations (N to 1 DN)**.
4. Click **Add**.
5. From the **DN Number** drop-down, choose an extension number. This field is mandatory.
6. In the E164 Ranges table, click + as required, to add multiple sets of E.164 numbers. The E.164 numbers do not need to be contiguous. Provide the following information:

Field	Description
E164 Range	Choose one of these ranges: Note: The range values you choose map to the mask value when the association translation pattern is created. For example, when 10 is chosen, all E.164 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 nonzero number. Likewise, when 100 is chosen, the E.164 number and DN end in two zeros. This pattern results in a mask of XX. • 1 - To list all E.164 numbers • 10 - To list all E.164 numbers that end in one zero (0) • 100 - To list all E.164 numbers that end in two zeros (00) • 1000 - To list all E.164 numbers that end in three zeros (000) This field is mandatory and affects what appears in the E.164 Number field.
E164 Number	Choose the starting number of E.164 numbers. For a customer-level association, customer-level E.164 numbers are available. For a site-level configuration, both customer-level and site-level E.164 numbers are available. This field is mandatory.

7. In the optional **Primary E164** field, enter the primary E.164 number to associate with the DN. Make sure the E.164 number you enter starts with + and falls within the range you specified in the **E164 Range** drop-down.
8. Click **Save**.
    - When listing the Directory Number Inventory and displaying a directory number, the E.164 number format is as listed in *View Directory Number Inventory*.
    - For a site-level association, one or more translation patterns that are used to route inbound PSTN calls to their proper DN are created on the Unified CM. These patterns are the mappings between

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

the set of E.164 numbers and the single directory number. When you associate a set of E.164 numbers to a single DN, multiple translation patterns are created; that is, each DN-to-E.164 range association results in a translation pattern being created on Cisco Unified Communications Manager.

- For a customer-level association, the translation patterns are created on each Unified CM cluster that has a dial plan provisioned.
- For a site-level association, if the site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwAddMultiE164AssociationEVT is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.
- For a customer-level association, if the E.164 number has the same country as any SIP Local Gateway configured for the customer, 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.

2.16. Manual Configuration for Intersite Cross-Cluster Support

2.16.1. Manual Configuration for Intersite Cross-Cluster Support

In order to support intersite calls for customers that have sites that span multiple clusters, the following manual procedure is required.

1. Create a full-mesh network between clusters for customers. Create trunk, route group, and route list with VOSS-4-UC 10.x/11.5(x) for a given cluster to every other cluster owned by the customer. For a shared Cisco Unified Communications Manager, a SIP security profile is needed for each trunk. For procedures, see Configure SIP Trunks and Configure Route Groups Configure Route Lists.
2. For each site added to a cluster, a route pattern must be added 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 Cisco Unified Communications Manager 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.

2.17. Manual Configuration for Local Breakout Support

2.17.1. Manual Configuration for Local Breakout Support

Important: Use this procedure only if you are using Cisco Unified CDM 10.6(1). Unified CDM 10.6(2) or later supports local breakout (LBO).

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

To manually configure a local gateway for a site to support LBO, perform the following manual steps.

1. Ensure that the VOSS-4-UC 10.x/11.5(x) hierarchy is set to the site where the local gateway is to be added.
2. Use VOSS-4-UC 10.x/11.5(x) 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, 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 Cisco Unified Communications Manager, 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 Cisco Unified Communications Manager is in +E.164 format. Therefore, all incoming and outgoing calls between the gateway and Cisco Unified Communications Manager 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.

2.18. Voice Mail

2.18.1. Create Voice Mail Service

Before You Begin

To associate Voice Mail Service with a Cisco Unified Communications Manager (Unified CM), you must know the SIP trunking endpoint information between the Voice Mail Server and the Unified CM.

A Cisco Unity Connection server must be configured before performing this procedure. For more information, see “Set Up Cisco Unity Connection” in the VOSS-4-UC Core Feature Guide.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Procedure

1. Log in as provider or reseller administrator.
2. Make sure that the hierarchy path is set to the correct provider or reseller node.
3. Choose **Services > Voice Mail > Voice Mail Service**.
4. Click **Add** to add a Voice Mail Service.
5. Enter a **Voice Mail Service Name** if desired. Do not add spaces in the name.
6. From the **Cisco Unity Connection Cluster** drop-down, choose the name of the server for the voice mail service.

   Note: The Cisco Unity Connection server must be previously defined under the Provider level at **Device Management > CUCs**. This is also the location whether the Voice Mail server in a multitenant environment is categorized as Dedicated or Partitioned. This determines what elements are available to the Voice Mail Server, whether another tenant should be created on the Voice Mail Server, and so on.
7. To integrate the Voice Mail Service with Unified CM, select the **Integrate with Cisco Unified CM** check box. Default = unchecked.
8. If Cisco Unified CM manages the Voice Mail Service, choose the Cisco Unified Communications Manager to be paired with the Cisco Unity Connection Server from the **Cisco Unified CM Cluster** drop-down menu.

   Note: The Unified CM must be previously defined under the Provider level at **Device Management > CUCMs**.
9. Complete the SIP trunk provisioning information (between the SIP trunk and the Cisco Unity Connection server) in the following fields:
   a. Enter the hostname or IP address of the Voice Mail Server in the **Cisco Unity Connection Server Address** field.
   b. Enter the Voice Mail Server port number (1 to 65535) in the **Cisco Unity Connection Server Port** field.

      Note: Do not specify port 5061, which is reserved for secure SIP.
   c. Enter the hostname or IP address for the Voice Mail Server to reach the Unified CM in the **Cisco Unified CM Server Address** field.
   d. Enter the Cisco Unified Communications port number in the **Cisco Unified CM Server Port** field.

      Note: Do not specify port 5061, which is reserved for secure SIP.

      Note: Only one Unified CM and one Cisco Unity Connection can be specified here. To support redundancy and failover in a multinode configuration, the trunk information must be manually updated on the UC apps.
10. In the **Voice Messaging Ports** field, enter the number of voice messaging ports to be created for the voice mail service and associated with the appropriate Port Group on Cisco Unity Connection when the voice mail service is associated to a customer.

    Valid values are 1 - 250. Default = 3. This field is mandatory.

    Note: The number of voice messaging ports that you add cannot 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 Cisco Unity Connection license files. If the license files do not enable the total number of ports, you will not be able to add the new ports.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

11. Click **Save** to add the Voice Mail Service you defined.

    When a shared Voice Mail Service is created and the **Integrate with Cisco Unified CM** check box is selected, the following occurs:

    - In Unified CM: Cluster-level SIP Trunk and Route Group is provisioned for the shared voice mail service.
    - In Cisco Unity Connect: Cluster-level Port Group appears on the PhoneSystem for the shared voice mail service.

What to Do Next

Perform Associate Voice Mail Services to Customer.

2.18.2. Associate Voice Mail Services to Customer

Before You Begin

- To associate Voice Mail Service with a customer, the Voice Mail Service must be created before starting this procedure. See *Create Voice Mail Service*.
- If the **Integrate with Cisco Unified CM** check box was selected when the Voice Mail services was created, a customer dial plan and a site dial plan must be created before a Voice Mail Service can be associated with a customer; otherwise the association will fail.

Procedure

1. Log in as provider or reseller administrator.
2. Set the hierarchy path to the customer to which you want to associate the Voice Mail Service.
3. Choose **Services > Voice Mail > Associate Voice Mail Service to Customer**.
4. Click **Add** to associate Voice Mail Service to a 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** to associate the Voice Mail Service with the customer. The association appears in the list. When the Voice Mail Service is associated with a customer and the **Integrate with Cisco Unified CM** check box 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Note: The deployment mode for the Voice Mail service is determined by the mode selected when the Cisco Unity Connection is first added to VOSS-4-UC using **Device Management > CUC**.

2.18.3. Disassociate Voice Mail Services from Customers

Procedure

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. Choose **Services > Voice Mail > 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.

2.18.4. Define a Voice Mail Pilot Number

Before You Begin

To create one or more Voice Mail Pilot Numbers for Voice Mail Services that have previously been associated with the customer, the following procedures must be completed before performing this procedure:

- Voice Mail Service must be created. See Create Voice Mail Service.
- Voice Mail Service must be associated with the customer. See Associate Voice Mail Services to Customer.

Note: In VOSS-4-UC, the Voice Mail Pilot Number is selectable from a list of available DN inventory.

Procedure

1. Log in as provider or customer administrator.
2. Make sure the hierarchy path is set to the customer or site that you are defining a Voice Mail Pilot Number for.
3. Choose **Services > Voice Mail > Pilot Numbers**.
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: More than one Pilot Number can be created for a single Voice Mail Service.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7. Click **Save** to create the Pilot Number. The Pilot Number appears in the list. When a Pilot Number is created for a Voice Mail Service and the **Integrated with CUCM** check box 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

2.18.5. Creating DDIs for Voice Mail Pilot Numbers

Before You Begin

To create a DDI for a voice mail pilot number, perform the following steps on VOSS-4-UC. The voice mail pilot number must be created before performing this procedure. See Define a Voicemail Pilot Number.

1. Log in to VOSS-4-UC as a Provider, Reseller, or Customer administrator.
2. Use the breadcrumbs to navigate to the customer hierarchy node that contains the voice mail pilotnumber.
3. Select **Device Management > CUCM > Route Patterns**.
4. Select **Add**.
5. Create a new route pattern instance with the following information:
   a. On the **Pattern Definition** tab, complete the following item:.
      i. **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.
      ii. **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 **Device Management > CUCM > Route Patterns** 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.18.6. Associate Pilot Number to a Site

Before You Begin

- To associate a Voice Mail Pilot number with a site, the Pilot Number must be created before starting this procedure. See Define a Voice Mail Pilot Number.

Note: In VOSS-4-UC, 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.

Procedure

1. Log in as a Customer or Provider administrator.
2. Set the hierarchy path to the desired Site.
3. Choose **Services > Voice Mail > Associate Pilot Number to Site**.
4. Click **Add** to associate a Voice Mail Pilot Number with a site.
5. From the **Voice Mail Service** drop-down, choose the mandatory name of the Voice Mail Service.
6. From the **Voice Mail Service Pilot Number** drop-down, choose the mandatory Pilot Number for the selected Voice Mail Service.
7. From the **E164 Number** drop-down, optionally choose a E164 number from your site's inventory to associate with the Pilot Number, or type the E164 number you want to use.
8. Click **Save** to associate the Voice Mail Service Pilot Number with the site.
    - The association appears in the list. When a Pilot Number is associated to a site, the **Site Management > Defaults > CUC Defaults** are updated so that the subscriber management templates can take advantage of this new Voice Mail 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.

2.18.7. Disassociate Pilot Number from a Site

Note: In VOSS-4-UC, the event related to SIP Local Gateway is generated as a result.

Procedure

1. Log in as the Customer Administrator. For a list of the roles and tasks that can be done at each level, see *Roles and Privileges*.
2. Choose **Services > Voice Mail > Associate Pilot Number to Site**.
3. From the list of associations, choose the Pilot Number association to be disassociated, by selecting the check box in the leftmost column.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

2.19. Adding Aggregation Trunk and Route Group and Associating to Existing Route List and SLRG

2.19.1. Adding Aggregation Trunk and Route Group and Associating to Existing Route List and SLRG

In VOSS-4-UC 10.x/11.5(x), 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:

Note: In step 11, navigate to Device Management > CUCM > Local Route Groups if you are using Cisco Unified CDM 10.6(1).

---

1. In VOSS-4-UC 10.x/11.5(x), create a region for the trunk as follows:
    a. Sign in as a provider or reseller and navigate to **Device Management > CUCM > Regions Information > Region**.
    b. Click **Add**.
    c. Provide a name in the format Cu<cid>-Trunk-<TrunkName>-Region.
2. In Cisco Unified Communications Manager, 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 VOSS-4-UC 10.x/11.5(x) and perform the following:
    a. Navigate to **Device Management > CUCM > SIP Trunks**.
    b. Click **Add**.
4. In the **Device Information** tab, perform the following:
    a. Choose the Unified CM from the drop-down list.
    b. Provide a device name; for example, Cu<cid>-Trunk-<TrunkName>.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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>-CNPNTranform-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>-CDPNTransform-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>-CGPNTransform-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. Navigate to **Device Management > 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- 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. Navigate to **Device Management > CUCM > 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. Navigate to **Device Management > CUCM > 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.20. Configure SIP Profiles

2.20.1. How to Configure SIP Profiles

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to the node where the Cisco Unified Communications Manager is configured.
3. Perform one of the following:
   - If you signed in as a provider or reseller administrator, choose **Device Management > CUCM > SIP Profiles**.
   - If you signed in as a customer administrator, choose **Device Management > Advanced > SIP Profiles**.
4. Perform one of the following:
   - To add a new SIP profile, click **Add**, then go to Step 5.
   - To 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** popup window appears, select the NDL for the SIP profile from the drop-down menu. The window appears when you are on a nonsite hierarchy node. If you are at a site hierarchy node, the NDL associated with the site is automatically used.

   Note:

   The **Network Device List** drop-down menu only appears when a SIP profile is added; it does not appear when you edit a SIP profile.
6. Enter a unique name for the new SIP profile in the **Name** field, or modify the existing **Name** if desired.
7. On the **SIP Profile Information** tab, complete at minimum, the mandatory *SIP Profile Information Fields*.
8. On the **SDP Information** tab, complete at minimum, the mandatory *SDP Information Fields*.
9. On the **Parameters used in Phone** tab, complete the required *Parameters used in Phone Fields*.
10. On the **Normalization Script** tab, complete the required *Normalization Script Fields*.
11. On the **Incoming Requests FROM URI Strings** tab, complete the required *Incoming Requests FROM URI Strings Fields*.
12. On the **Trunk Specific Configuration** tab, complete at minimum, the mandatory *Trunk Specific Configuration Fields*.
13. On the **Trunk SIP OPTIONS Ping** tab, complete the required *Trunk SIP OPTIONS Ping Fields*.
14. On the **Trunk SDP Information** tab, complete the required *Trunk SDP Information Fields*.
15. Click **Save** to save a new SIP profile or to update an existing SIP profile.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

SIP Profile Information Fields

Option	Description
Name (Mandatory)	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description (Optional)	This field identifies the purpose of the SIP profile; for example, SIP for 8865. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Default MTP Telephony Event Payload Type (Optional)	This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. Usually, the default value specifies the appropriate payload type. Be sure that you have a good understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. Default-101 Range-96 to 127 This parameter’s value affects calls with the following conditions: • An outgoing SIP call from Cisco Unified Communications Manager • For the calling SIP trunk, the **Media Termination Point Required** check box is checked on the SIP Trunk Configuration window
Early Offer for G.Clear Calls (Optional)	This feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options: • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Disable Early Media on 180 (Optional)	By default, Unified CM signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in these responses, instead of playing ringback locally, Unified CM connects media. The calling phone then plays whatever the called device is sending (such as ringback or busy signal). If you receive no ringback, the device you are connecting to may include SDP in the 180 response, but not send media before 200OK response. In this case, select this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response. Note: Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.
Outgoing T.38 INVITE include audio mline (Optional)	The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, configure a SIP trunk with this SIP profile. Note: The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.
Use Fully Qualified Domain Name in SIP Requests (Optional)	This feature enables Unified CM to relay a caller's alphanumeric hostname by passing it to the called device or outbound trunk as SIP header information. Enter one of the following: **f** - To disable this option. The IP address for Unified CM is passed to the line device or outbound trunk instead of the user's hostname. **t** - To enable this option. Unified CM relays an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call originates from a line device on the Unified CM cluster, and is routed on a SIP trunk, then the configured Organizational Top-Level Domain (for example, Cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call originates from a trunk on Unified CM and is being routed on a SIP trunk, then: • If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging preserves the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. • If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. Default: f - Disabled
Assured Services SIP conformance (Optional)	Select this check box for third-party AS-SIP endpoints and AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

SDP Information Fields

Option	Description
SDP Transparency Profile (Optional)	Displays the SDP Transparency Profile Setting (read-only)
Accept Audio Codec Preferences in Received Offer (Optional)	Choose one of the following options: • **On** - Enables Unified CM to honor the preference of audio codecs in the received offer and preserve it while processing. • **Off** - Enables Unified CM to ignore the preference of audio codecs in a received offer and apply the locally configured Audio Codec Preference List. The default selects the service parameter configuration. • **Default** - Selects the service parameter configuration. Default: Default
Require SDP Inactive Exchange for Mid-Call Media Change (Optional)	This feature determines how Unified CM handles midcall updates to codecs or connection information such as IP address or port numbers. If you select this check box, during midcall codec or connection updates Unified CM sends an INVITE a-inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. Note For early offer enabled SIP trunks, the Send send-receive SDP in midcall INVITE parameter overrides this parameter. If this check box is clear, Unified CM passes the midcall SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. Default: Clear
Allow RR/RS bandwidth modifier (RFC 3556) (Mandatory)	Specifies the RR (RTDP bandwidth allocated to other participants in an RTP session) and RS (RTCP bandwidth allocated to active data senders) in RFC 3556. Options are: • Transport Independent Application Specific bandwidth modifier (TIAS) and AS • TIAS only • AS only • CT only Default: TIAS and AS

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Parameters used in Phone Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Caller ID Blocking (Optional)	This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or email address from phones that have caller identification enabled. Valid values are: • **Off** - Disabled permanently and cannot be turned on and off locally by the user interface • **On** - Enabled permanently and cannot be turned on and off locally by the user interface
Do Not Disturb Control (Optional)	This field sets the Do Not Disturb (DND) feature. Valid values are: • **User** - The dndControl parameter for the phone specifies 0. • **Admin** - The dndControl parameter for the phone specifies 2.
Telnet Level for 7940 and 7960 (Optional)	Cisco Unified IP Phones 7940 and 7960 do not support SSH for sign-in access or HTTP that is used to collect logs. However, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values: • **Disabled** - No access • **Limited** - Some access but cannot run privileged commands • **Enabled** - Full access
Resource Priority Namespace (Optional)	This field enables the administrator to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line using its SIP Profile.
Timer Keep Alive Expires (seconds) (Optional)	Unified CM requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages sent to the backup Unified CM to ensure its availability for failover. Default: 120 seconds
Timer Subscribe Expires (seconds) (Optional)	This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the" Expires" header field. Valid values: Any positive number Default: 120 seconds
Timer Subscribe Delta (seconds) (Optional)	Use this parameter with the `Timer Subscribe Expires` setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by `Timer Subscribe Expires`. Range: 3 to 15 seconds Default: 5 seconds
Maximum Redirections (Optional)	Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call. Default: 70 redirections
Off hook To First Digit Timer (msec) (Optional)	This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. Range: 0 to 15,000 microseconds Default: 15,000 microseconds
Call Forward URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call forward feature.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Normalization Script Fields

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.

Incoming Requests FROM URI Strings Fields

Option	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX - Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 55000 - Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Trunk Specific Configuration Fields

Option	Description
Reroute Incoming Request to new Trunk based on	Unified CM only accepts calls from a SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Unified CM accepts the call, Unified CM uses the configuration for this setting to determine whether to reroute the call to another trunk. From the drop-down list, choose the method that Unified CM uses to identify the SIP trunk where the call gets rerouted: • **Never** - If the SIP trunk matches the IP address of the originating device, choose this option. Unified CM, which identifies the trunk by the incoming packet's source IP address and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • **Contact Info Header** - If the SIP trunk uses a SIP proxy, choose this option. Unified CM parses the IP address or domain name and the signaling port number in the incoming request's header. Unified CM then reroutes the call to the SIP trunk using that IP address and port. If no SIP trunk is identified, the call occurs on the trunk where the call arrived. • **Call-Info Header with purpose-x-cisco-origIP** - If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Unified CM performs the following: – parses the Call-Info header – looks for the parameter `purpose-x-cisco-origIP` – uses the IP address or domain name and signaling port number in the header to reroute the call to the SIP trunk using the IP address and port If the parameter is not in the header, or no SIP trunk is identified, the call occurs on the SIP trunk where the call arrived. Default: Never Note: This setting does not work for SIP trunks connected to: • A Unified CM IM and Presence Service proxy server. • Originating gateways in different Unified CM groups

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
RSVP Over SIP	This field configures RSVP over SIP trunks. From the drop-down list, choose the method that Unified CM uses to configure RSVP over SIP trunks: • **Local RSVP** - In a local configuration, RSVP occurs within each cluster, between the endpoint and the local SIP trunk, but not on the WAN link between the clusters. • **E2E** - In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the endpoints, including within the local cluster and over the WAN.
Resource Priority Namespace List	Select a configured Resource Priority Namespace list from the drop-down menu. The Namespace List is configured in Unified CM in the Resource Priority Namespace List menu. You can access the menu in Unified CM from System MLPP > Namespace.
Fall back to local RSVP	Select this check box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this check box is clear, end-to-end RSVP calls that cannot establish an end-to-end connection fail.
SIP Rel1XX Options	This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint. Valid values are: • **Disabled** - Disables SIP Rel1XX. • **Send PRACK if 1XX contains SDP** - Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • **Send PRACK for all 1XX messages** - Acknowledges all1XX messages with PRACK. If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.
Video Call Traffic Class	Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list, select one of: • **Immersive** - High-definition immersive video. • **Desktop** - Standard desktop video. • **Mixed** - A mix of immersive and desktop video. Unified CM Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth and Immersive Bandwidth. The pool used depends on the type of call determined by the Video Call Traffic Class. Refer to the “Call Admission Control” chapter of the Cisco Unified Communications Manager System Guide for more information.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Calling Line Identification Presentation (Mandatory)	Select one of: • **Strict From URI presentation Only** - To select the network-provided identity • **Strict Identity Headers presentation Only** - To select the user-provided identity • **Default** - To select the system default calling line identification Default: Default
Session Refresh Method (Mandatory)	Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions. This allows the Unified CM and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified CM received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified CM initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified CM can send both Update and Invite requests. Specify whether to use **Invite** or **Update** as the Session Refresh Method. Default: Invite Note: Sending a midcall Invite request requires specifying an offer SDP in the request. This means that the far end must send an answer SDP in the Invite response. Update: Unified CM requests a SIP Update if the SIP session's far end supports the Update method in the Supported or Require headers. When sending the Update request, the Unified CM includes an SDP. This simplifies the session refresh since no SDP offer or answer exchange is required. Note: If the far end of the SIP session does not support the Update method, the Unified CM continues using the Invite method for session refresh.
Early Offer Support for voice and video calls (Mandatory)	This field configures Early Offer support for voice and video calls. When enabled, Early Offer support includes a session description in the initial INVITE for outbound calls. Early Offer configuration settings on SIP profile apply only to SIP trunk calls. These configuration settings do not affect SIP line side calls. If this profile is shared between a trunk and a line, only a SIP trunk that uses the profile is affected by these settings. The Media Transfer Point (MTP) Required check box on the Trunk Configuration window, if enabled, overrides the early offer configuration on the associated SIP profile. Unified CM sends the MTP IP address and port with a single codec in the SDP in the initial INVITE. From the drop-down list box, select one of the following three options: • **Disabled (Default value)** - Disables Early Offer; no SDP will be included in the initial INVITE for outbound calls. • **Best Effort (no MTP Inserted)** – Provide Early Offer for the outbound call only when caller side's media port, IP and codec information is available. – Provide Delayed Offer for the outbound call when caller side's media port, IP and codec information is not available. No MTP is inserted to provide Early Offer in this case. • **Mandatory (insert MTP if needed)** - Provide Early Offer for all outbound calls and insert MTP when caller side's media port, IP and codec information is not available. Default: Disabled (Default value)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Selecting the **Enable ANAT** and **MTP Required** check boxes sets Unified CM to insert a dual-stack MTP and send an offer with two m-lines, for IPv4 and IPv6. If a dual- stack MTP cannot be allocated, Unified CM sends an INVITE without SDP. When you select the **Enable ANAT** check box and the **Media Termination Point Required** check box is clear, Unified CM sends an INVITE without SDP. When the **Enable ANAT** and **MTP Required** check boxes are cleared (or when an MTP cannot be allocated), Unified CM sends an INVITE without SDP. When you clear the **Enable ANAT** check box but you select the **MPT Required** check box, consider the information, which assumes that an MTP can be allocated: • Unified CM sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Unified CM sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Unified CM determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.
Deliver Conference Bridge Identifier	When checked, the SIP trunk passes the b-number identifying the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require this field. Selecting this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Selecting this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.
Allow Passthrough of Configured Line Device Caller Information	Select this check box to allow passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Select this check box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Select this check box to reject anonymous outgoing calls.
Send ILS Learned Destination Route String	When this check box is selected, for calls routed to a learned directory URI, learned number, or learned pattern, Unified CM: • adds the `x-cisco-dest-route-string` header to outgoing SIP INVITE and SUBSCRIBE messages • inserts the destination route string into the header When this check box is clear, Unified CM does not add the x-cisco-dest-route-string header to any SIP messages. The x-cisco-dest-route-string header allows Unified CM to route calls across a Session Border Controller.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Trunk SIP OPTIONS Ping Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Trunk SDP Information Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.20.2. SIP Profile Field Descriptions

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)	This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. Usually, the default value specifies the appropriate payload type. Be sure that you have a good understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. Default-101 Range-96 to 127 This parameter’s value affects calls with the following conditions: • An outgoing SIP call from Cisco Unified Communications Manager • For the calling SIP trunk, the **Media Termination Point Required** check box is checked on the SIP Trunk Configuration window
Early Offer for G.Clear Calls (Optional)	This feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options: • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Redirect by Application (Optional)	If you select this check box and configure this SIP Profile on the SIP trunk, the Unified CM administrator can: • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the calls get routed correctly. • Prevent a DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at stack level causes the call to be routed, not blocked. This behavior occurs if you leave the **Redirect by Application** check box clear.
Disable Early Media on 180 (Optional)	By default, Unified CM signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in these responses, instead of playing ringback locally, Unified CM connects media. The calling phone then plays whatever the called device is sending (such as ringback or busy signal). If you receive no ringback, the device you are connecting to may include SDP in the 180 response, but not send media before 200OK response. In this case, select this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response. Note: Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.
Outgoing T.38 INVITE include audio mline (Optional)	The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, configure a SIP trunk with this SIP profile. Note: The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Use Fully Qualified Domain Name in SIP Requests (Optional)	This feature enables Unified CM to relay a caller's alphanumeric hostname by passing it to the called device or outbound trunk as SIP header information. Enter one of the following: **f** - To disable this option. The IP address for Unified CM is passed to the line device or outbound trunk instead of the user's hostname. **t** - To enable this option. Unified CM relays an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call originates from a line device on the Unified CM cluster, and is routed on a SIP trunk, then the configured Organizational Top-Level Domain (for example, Cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call originates from a trunk on Unified CM and is being routed on a SIP trunk, then: • If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging preserves the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. • If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. Default: f - Disabled
Assured Services SIP conformance (Optional)	Select this check box for third-party AS-SIP endpoints and AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Table: SDP Information Tab

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
SDP Transparency Profile (Optional)	Displays the SDP Transparency Profile Setting (read-only)
Accept Audio Codec Preferences in Received Offer (Optional)	Choose one of the following options: • **On** - Enables Unified CM to honor the preference of audio codecs in the received offer and preserve it while processing. • **Off** - Enables Unified CM to ignore the preference of audio codecs in a received offer and apply the locally configured Audio Codec Preference List. The default selects the service parameter configuration. • **Default** - Selects the service parameter configuration. Default: Default
Require SDP Inactive Exchange for Mid-Call Media Change (Optional)	This feature determines how Unified CM handles midcall updates to codecs or connection information such as IP address or port numbers. If you select this check box, during midcall codec or connection updates Unified CM sends an INVITE a-inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. Note For early offer enabled SIP trunks, the Send send-receive SDP in midcall INVITE parameter overrides this parameter. If this check box is clear, Unified CM passes the midcall SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. Default: Clear
Allow RR/RS bandwidth modifier (RFC 3556) (Mandatory)	Specifies the RR (RTDP bandwidth allocated to other participants in an RTP session) and RS (RTCP bandwidth allocated to active data senders) in RFC 3556. Options are: • Transport Independent Application Specific bandwidth modifier (TIAS) and AS • TIAS only • AS only • CT only Default: TIAS and AS

Table: Parameters used in Phone Tab

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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
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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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: • **None** - No value is inserted • **Phone** - The value user-phone is inserted in the To, From, and Contact Header for REGISTER • **IP** - The value user-ip is inserted in the To, From, and Contact Header for REGISTER Default: None
DTMF DB Level (Optional)	This field specifies the in-band DTMF digit tone level. Valid values are: • 6 dB below nominal • 3 dB below nominal • Nominal • 3 dB above nominal • 6 dB above nominal Default: Nominal
Call Hold Ring Back (Optional)	This parameter causes the phone to ring in cases where you have another party on hold when you hang up a call. Valid values are: • **Off** - Off permanently and cannot be turned on and off locally by the user interface • **On** - On permanently and cannot be turned on and off locally by the user interface
Anonymous Call Block (Optional)	The field configures anonymous call block. Valid values are: • **Off** - Disabled permanently and cannot be turned on and off locally by the user interface • **On** - Enabled permanently and cannot be turned on and off locally by the user interface
Caller ID Blocking (Optional)	This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or email address from phones that have caller identification enabled. Valid values are: • **Off** - Disabled permanently and cannot be turned on and off locally by the user interface • **On** - Enabled permanently and cannot be turned on and off locally by the user interface
Do Not Disturb Control (Optional)	This field sets the Do Not Disturb (DND) feature. Valid values are: • **User** - The dndControl parameter for the phone specifies 0. • **Admin** - The dndControl parameter for the phone specifies 2.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Telnet Level for 7940 and 7960 (Optional)	Cisco Unified IP Phones 7940 and 7960 do not support SSH for sign-in access or HTTP that is used to collect logs. However, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values: • **Disabled** - No access • **Limited** - Some access but cannot run privileged commands • **Enabled** - Full access
Resource Priority Namespace (Optional)	This field enables the administrator to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line using its SIP Profile.
Timer Keep Alive Expires (seconds) (Optional)	Unified CM requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages sent to the backup Unified CM to ensure its availability for failover. Default: 120 seconds
Timer Subscribe Expires (seconds) (Optional)	This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the" Expires" header field. Valid values: Any positive number Default: 120 seconds
Timer Subscribe Delta (seconds) (Optional)	Use this parameter with the `Timer Subscribe Expires` setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by `Timer Subscribe Expires`. Range: 3 to 15 seconds Default: 5 seconds
Maximum Redirections (Optional)	Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call. Default: 70 redirections
Off hook To First Digit Timer (msec) (Optional)	This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. Range: 0 to 15,000 microseconds Default: 15,000 microseconds
Call Forward URI (Optional)	This URI provides a unique address that the phone that is running SIP sends to Unified CM to invoke the call forward feature.
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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX - Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 55000 - Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.

Table: Trunk Specific Configuration Tab

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Reroute Incoming Request to new Trunk based on	Unified CM only accepts calls from a SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Unified CM accepts the call, Unified CM uses the configuration for this setting to determine whether to reroute the call to another trunk. From the drop-down list, choose the method that Unified CM uses to identify the SIP trunk where the call gets rerouted: • **Never** - If the SIP trunk matches the IP address of the originating device, choose this option. Unified CM, which identifies the trunk by the incoming packet's source IP address and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • **Contact Info Header** - If the SIP trunk uses a SIP proxy, choose this option. Unified CM parses the IP address or domain name and the signaling port number in the incoming request's header. Unified CM then reroutes the call to the SIP trunk using that IP address and port. If no SIP trunk is identified, the call occurs on the trunk where the call arrived. • **Call-Info Header with purpose-x-cisco-origIP** - If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Unified CM performs the following: – parses the Call-Info header – looks for the parameter `purpose-x-cisco-origIP` – uses the IP address or domain name and signaling port number in the header to reroute the call to the SIP trunk using the IP address and port If the parameter is not in the header, or no SIP trunk is identified, the call occurs on the SIP trunk where the call arrived. Default: Never Note: This setting does not work for SIP trunks connected to: • A Unified CM IM and Presence Service proxy server. • Originating gateways in different Unified CM groups

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
RSVP Over SIP	This field configures RSVP over SIP trunks. From the drop-down list, choose the method that Unified CM uses to configure RSVP over SIP trunks: • **Local RSVP** - In a local configuration, RSVP occurs within each cluster, between the endpoint and the local SIP trunk, but not on the WAN link between the clusters. • **E2E** - In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the endpoints, including within the local cluster and over the WAN.
Resource Priority Namespace List	Select a configured Resource Priority Namespace list from the drop-down menu. The Namespace List is configured in Unified CM in the Resource Priority Namespace List menu. You can access the menu in Unified CM from System MLPP > Namespace.
Fall back to local RSVP	Select this check box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this check box is clear, end-to-end RSVP calls that cannot establish an end-to-end connection fail.
SIP Rel1XX Options	This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint. Valid values are: • **Disabled** - Disables SIP Rel1XX. • **Send PRACK if 1XX contains SDP** - Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • **Send PRACK for all 1XX messages** - Acknowledges all1XX messages with PRACK. If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.
Video Call Traffic Class	Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list, select one of: • **Immersive** - High-definition immersive video. • **Desktop** - Standard desktop video. • **Mixed** - A mix of immersive and desktop video. Unified CM Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth and Immersive Bandwidth. The pool used depends on the type of call determined by the Video Call Traffic Class. Refer to the “Call Admission Control” chapter of the Cisco Unified Communications Manager System Guide for more information.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Calling Line Identification Presentation (Mandatory)	Select one of: • **Strict From URI presentation Only** - To select the network-provided identity • **Strict Identity Headers presentation Only** - To select the user-provided identity • **Default** - To select the system default calling line identification Default: Default
Session Refresh Method (Mandatory)	Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions. This allows the Unified CM and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified CM received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified CM initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified CM can send both Update and Invite requests. Specify whether to use **Invite** or **Update** as the Session Refresh Method. Default: Invite Note: Sending a midcall Invite request requires specifying an offer SDP in the request. This means that the far end must send an answer SDP in the Invite response. Update: Unified CM requests a SIP Update if the SIP session's far end supports the Update method in the Supported or Require headers. When sending the Update request, the Unified CM includes an SDP. This simplifies the session refresh since no SDP offer or answer exchange is required. Note: If the far end of the SIP session does not support the Update method, the Unified CM continues using the Invite method for session refresh.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Selecting the **Enable ANAT** and **MTP Required** check boxes sets Unified CM to insert a dual-stack MTP and send an offer with two m-lines, for IPv4 and IPv6. If a dual- stack MTP cannot be allocated, Unified CM sends an INVITE without SDP. When you select the **Enable ANAT** check box and the **Media Termination Point Required** check box is clear, Unified CM sends an INVITE without SDP. When the **Enable ANAT** and **MTP Required** check boxes are cleared (or when an MTP cannot be allocated), Unified CM sends an INVITE without SDP. When you clear the **Enable ANAT** check box but you select the **MPT Required** check box, consider the information, which assumes that an MTP can be allocated: • Unified CM sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Unified CM sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Unified CM determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.
Deliver Conference Bridge Identifier	When checked, the SIP trunk passes the b-number identifying the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require this field. Selecting this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Selecting this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.
Allow Passthrough of Configured Line Device Caller Information	Select this check box to allow passthrough of configured line device caller information from the SIP trunk.

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	When this check box is selected, for calls routed to a learned directory URI, learned number, or learned pattern, Unified CM: • adds the `x-cisco-dest-route-string` header to outgoing SIP INVITE and SUBSCRIBE messages • inserts the destination route string into the header When this check box is clear, Unified CM does not add the x-cisco-dest-route-string header to any SIP messages. The x-cisco-dest-route-string header allows Unified CM to route calls across a Session Border Controller.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Table: Trunk SIP OPTIONS Ping Tab

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

Table: Trunk SDP Information Tab

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

2.21. Configure SIP Trunk Security Profiles

2.21.1. How to Configure SIP Trunk Security Profiles

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to the node where the Cisco Unified Communications Manager is configured.
3. Perform one of:
   - If you signed in as the provider or reseller administrator, choose **Device Management > CUCM > SIP Trunk Security Profiles**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- If you signed in as the customer administrator, choose **Device Management > Advanced > SIP Trunk Security Profiles**.

4. Perform one of:
   - To add a new SIP trunk security profile, click **Add**, then go to Step 5.
   - To 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** popup window appears, select the NDL for the SIP trunk security profile 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 appears when a SIP trunk security profile is added. It does not appear when you edit a SIP trunk security profile.
6. Enter a unique name for the new SIP trunk security profile in the **Name** field, or modify the existing Name if desired. This field is mandatory.
7. Complete, at minimum, the other mandatory *SIP Trunk Security Profiles Fields*
8. Click **Save** to save a new SIP trunk security profile or to update an existing SIP trunk security profile.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

SIP Trunk Security Profiles Fields

Option	Description
Name (Mandatory)	Enter a name for the security profile. When you save the new profile, the name displays in the **SIP Trunk Security Profile** drop-down list in the Trunk Configuration window. The maximum length for the name is 64 characters.
Description (Optional)	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Security Mode (Optional)	From the drop-down list, choose one of the following options: • **Non Secure** - No security features except image authentication apply. A TCP or UDP connection opens to Cisco Unified Communications Manager. • **Authenticated** - Unified CM provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • **Encrypted** - Unified CM provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling.
Incoming Transport Type (Optional)	Choose one of: • TCP+UDP • UDP • TLS • TCP If you do not specify an incoming transport type, **TCP+UDP** is assigned. When **Device Security Mode** is **Non Secure**, **TCP+UDP** specifies the transport type. When **Device Security Mode** is **Authenticated** or **Encrypted**, **TLS** specifies the transport type. Note: The Transport Layer Security (TLS) protocol secures the connection between Unified CM and the trunk.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Outgoing Transport Type (Optional)	From the drop-down list, choose the outgoing transport mode. Choose one of: • TCP+UDP • UDP • TLS • TCP When **Device Security Mode** is **Non Secure**, choose **TCP** or **UDP**. When **Device Security Mode** is **Authenticated** or **Encrypted**, **TLS** specifies the transport type. Note: **TLS** ensures signaling integrity, device authentication, and signaling encryption for SIP trunks. Tip: Use **UDP** as the outgoing transport type when connecting SIP trunks between Unified CM systems and IOS gateways that do not support TCP connection reuse. See “Understanding Session Initiation Protocol (SIP)” in the “Cisco Unified Communications Manager System Guide” for more information.
Enable Digest Authentication (Optional)	Select this check box to enable digest authentication. If you select this check box, Unified CM challenges all SIP requests from the trunk. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of **Authenticated** or **Encrypted** to use these features. Tip: Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.
Nonce Validity Time (mins) (Optional)	Enter the number of minutes (in seconds) that the nonce value is valid. When the time expires, Unified CM generates a new value. Note: A nonce value (a random number that supports digest authentication) is used to calculate the MD5 hash of the digest authentication password. Default = 600 minutes. If you do not specify a Nonce Validity Time, the default of 600 minutes is assigned.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Accept replaces header (Optional)	If you want Unified CM to accept new SIP dialogs, which have replaced existing SIP dialogs, select this check box. If you selected **Enable Application Level Authorization**, go to the **Application User Configuration** window and select **Accept Header Replacement** for any application users authorized for this method.
Transmit security status (Optional)	If you want Unified CM to send the security icon status of a call from the associated SIP trunk to the SIP peer, select this check box. Default = Cleared.
Allow charging header (Optional)	If you want to allow RFC 3455 SIP charging headers in transactions (for example, where billing information is passed in the headers for prepaid accounts), select this check box. If the check box is clear, RFC 3455 SIP charging headers are not allowed in sessions that use the SIP profile. Default = **Cleared**.
SIP V.150 Outbound SDP Offer Filtering (Mandatory)	Choose one of the following filter options from the drop-down list: • **Use Default Filter** - The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System Service Parameters Clusterwide Parameters (Device-SIP) in Unified CM Administration. • **No Filtering** - The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • **Remove MER V.150** - The SIP trunk removes V.150 MER SDP lines in outbound offers. Choose this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified CM. • **Remove Pre-MER V.150** - The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Choose this option to reduce ambiguity when your cluster is in a network of MER-compliant devices that cannot process offers with pre-MER lines. Default = **Use Default Filter** .

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.21.2. SIP Trunk Security Profile Field Descriptions

Option	Description
Name (Mandatory)	Enter a name for the security profile. When you save the new profile, the name displays in the **SIP Trunk Security Profile** drop-down list in the Trunk Configuration window. The maximum length for the name is 64 characters.
Description (Optional)	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Security Mode (Optional)	From the drop-down list, choose one of the following options: • **Non Secure** - No security features except image authentication apply. A TCP or UDP connection opens to Cisco Unified Communications Manager. • **Authenticated** - Unified CM provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • **Encrypted** - Unified CM provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling.
Incoming Transport Type (Optional)	Choose one of: • TCP+UDP • UDP • TLS • TCP If you do not specify an incoming transport type, **TCP+UDP** is assigned. When **Device Security Mode** is **Non Secure**, **TCP+UDP** specifies the transport type. When **Device Security Mode** is **Authenticated** or **Encrypted**, **TLS** specifies the transport type. Note: The Transport Layer Security (TLS) protocol secures the connection between Unified CM and the trunk.
Outgoing Transport Type (Optional)	From the drop-down list, choose the outgoing transport mode. Choose one of: • TCP+UDP • UDP • TLS • TCP When **Device Security Mode** is **Non Secure**, choose **TCP** or **UDP**. When **Device Security Mode** is **Authenticated** or **Encrypted**, **TLS** specifies the transport type. Note: **TLS** ensures signaling integrity, device authentication, and signaling encryption for SIP trunks. Tip: Use **UDP** as the outgoing transport type when connecting SIP trunks between Unified CM systems and IOS gateways that do not support TCP connection reuse. See “Understanding Session Initiation Protocol (SIP)” in the “Cisco Unified Communications Manager System Guide” for more information.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Enable Digest Authentication (Optional)	Select this check box to enable digest authentication. If you select this check box, Unified CM challenges all SIP requests from the trunk. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of **Authenticated** or **Encrypted** to use these features. Tip: Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.
Nonce Validity Time (mins) (Optional)	Enter the number of minutes (in seconds) that the nonce value is valid. When the time expires, Unified CM generates a new value. Note: A nonce value (a random number that supports digest authentication) is used to calculate the MD5 hash of the digest authentication password. Default = 600 minutes. If you do not specify a Nonce Validity Time, the default of 600 minutes is assigned.
X.509 Subject Name (Optional)	This field applies if you configured TLS for the incoming and outgoing transport type. For device authentication, enter the subject name of the X.509 certificate for the SIP trunk device. If you have a Unified CM cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts. This situation results in multiple X.509 subject names for the trunk. If multiple X.509 subject names exist, enter one of the following characters to separate the names: space, comma, semicolon, or a colon. You can enter up to 4096 characters in this field. Tip: The subject name corresponds to the source connection TLS certificate. Ensure that subject names are unique for each subject name and port. You cannot assign the same subject name and incoming port combination to different SIP trunks. Example: SIP TLS trunk1 on port 5061 has X.509 Subject Names my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has X.509 Subject Names my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have X.509 Subject Name my_ccm4 but cannot have X.509 Subject Name my_cm1.
Incoming Port (Optional)	Choose the incoming port. Enter a value that is a unique port number from 0 to 65535. The value that you enter applies to all SIP trunks that use the profile. The default port value for incoming TCP and UDP SIP messages is 5060. The default SIP secured port for incoming TLS messages is 5061. If the incoming port is not specified, the default port of 5060 is used. Tip: All SIP trunks that use TLS can share the same incoming port; all SIP trunks that use TCP + UDP can share the same incoming port. You cannot mix SIP TLS transport trunks with SIP non-TLS transport trunk types on the same port.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Accept replaces header (Optional)	If you want Unified CM to accept new SIP dialogs, which have replaced existing SIP dialogs, select this check box. If you selected **Enable Application Level Authorization**, go to the **Application User Configuration** window and select **Accept Header Replacement** for any application users authorized for this method.
Transmit security status (Optional)	If you want Unified CM to send the security icon status of a call from the associated SIP trunk to the SIP peer, select this check box. Default = Cleared.
Allow charging header (Optional)	If you want to allow RFC 3455 SIP charging headers in transactions (for example, where billing information is passed in the headers for prepaid accounts), select this check box. If the check box is clear, RFC 3455 SIP charging headers are not allowed in sessions that use the SIP profile. Default = **Cleared**.
SIP V.150 Outbound SDP Offer Filtering (Mandatory)	Choose one of the following filter options from the drop-down list: • **Use Default Filter** - The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System Service Parameters Clusterwide Parameters (Device-SIP) in Unified CM Administration. • **No Filtering** - The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • **Remove MER V.150** - The SIP trunk removes V.150 MER SDP lines in outbound offers. Choose this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified CM. • **Remove Pre-MER V.150** - The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Choose this option to reduce ambiguity when your cluster is in a network of MER-compliant devices that cannot process offers with pre-MER lines. Default = **Use Default Filter** .

2.22. Configure SIP Trunks

2.22.1. How to Configure SIP Trunks

1. Log in as provider, reseller, or customer administrator.
2. Make sure the hierarchy path is set to the node where the Cisco Unified Communications Manager is configured.
3. Perform one of:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > SIP Trunks**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > SIP Trunks**.
4. Perform one of:
   - To add a new SIP trunk, click **Add**, then go to Step 5.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- To edit an existing SIP trunk, choose the SIP trunk to be updated by clicking it in the list of SIP trunks and go to step 6.

5. From the **CUCM** drop-down menu, select the hostname, domain name, or IP address of the Unified CM to which you want to add the SIP trunk.

   Note:

   The **CUCM** drop-down menu only appears when a SIP trunk is added; it does not appear when you edit a SIP trunk.

   Important

   The **CUCM** drop-down menu shows, in addition to the Unified CM located at the node, ALL the Unified CM nodes in the hierarchies above the node you are adding the SIP trunk. To provision a Unified CM server, refer to the "Installation Tasks" section of Installing Cisco Unified Communications Manager.

6. Enter a unique name for the new SIP trunk in the **Device Name** field, or modify the existing **Device Name** if desired.
7. On the **Device Information** tab, complete at minimum, the mandatory *Device Information Fields*.
8. On the **Call Routing General** tab, complete at minimum, the mandatory *Call Routing General Fields*.
9. On the **Call Routing Inbound** tab, complete the required *Call Routing Inbound Fields*.
10. On the **Call Routing Outbound** tab, complete the required *Call Routing Outbound Fields*.
11. On the **SP Info** tab, complete the required *SP Info Fields*.
12. On the **GeoLocation** tab, complete at minimum, the mandatory *GeoLocation Fields*.
13. Click **Save** to save a new SIP trunk or to update an existing SIP trunk.

    The SIP trunk appears in the SIP trunk list. You can view the SIP trunk and its characteristics by logging in to the Unified CM where the SIP trunk was added, selecting Device Trunk, and performing the "Find" operation. When you click on the name of the SIP trunk in the list, the trunk characteristics are displayed.

    Note:

    The SIP trunk is automatically reset on the Unified CM as soon as it is added. To reset the SIP trunk at any other time, refer to "Reset SIP Trunk".

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Device Information Fields

Option	Description
Device Name *	Enter a unique identifier for the trunk using up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only. Default value: None
Trunk Service Type	Choose one of: • **None** - Choose this option if the trunk is not used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine • **Call Control Discovery** - Choose this option to enable the trunk to support call control discovery. • **Extension Mobility Cross Cluster** - Choose this option to enable the trunk to support the Extension Mobility Cross Cluster (EMCC) feature. Choosing this option causes the following settings to remain blank or clear and become unavailable for configuration, thus retaining their default values: Media Termination Point Required, Unattended Port, Destination Address, Destination Address IPv6, and Destination Address is an SRV. • **Cisco Intercompany Media Engine** - Ensure that the Cisco IME server is installed and available before you configure this field. • **IP Multimedia Subsystem Service Control (ISC)** - Choose this option to enable the trunk to support IP multimedia subsystem service control. Default value: None (Default)
Description (Optional)	Enter a descriptive name for the trunk using up to 114 characters in any language, but not including double-quotes (“), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>). Default value: empty
Device Pool *	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers (Unified CMs) that the trunk uses to distribute the call load dynamically. Note: Calls that are initiated from a phone that is registered to a Unified CM that does not belong to the device pool of the trunk use different Unified CMs of this device pool for different outgoing calls. Selection of Unified CM nodes occurs in a random order. A call that is initiated from a phone that is registered to a Unified CM that does belong to the device pool of the trunk uses the same Unified CM node for outgoing calls if the Unified CM is up and running. Default value: Default
Common Device Configuration	Choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Default value: None
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Unified CM clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Default value: Use System Default

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. Default value: None
Location *	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. Choose the appropriate location for this trunk: • Hub_None - Specifies that the locations feature does not keep track of the bandwidth that this trunk consumes. • Phantom - Specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. • Shadow - Specifies a location for intercluster enhanced location CAC. Valid for SIP intercluster trunks (ICT) only. Default value: Hub_None
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls is attempted. Default value: None
Tunneled Protocol	Choose the QSIG option if you want to use SIP trunks or SIP gateways to transport (tunnel) QSI messages from Unified CM to other PINXs. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Path Replacement, and Message Waiting Indication (MWI). Note: Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway. Default value: None
QSIG Variant	To display the options in the **QSIG Variant** drop-down list, choose QSIG from the **Tunneled Protocol** drop-down menu. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down menu, select one of: • No Changes - Default. Keep this parameter set to the default value unless a VOSS support engineer instructs otherwise. • Not Selected • ECMA - Select for ECMA PBX systems that use Protocol Profile 0x91 • ISO - Select for PBX systems that use Protocol Profile 0x9F Default value: No Changes

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down menu, choose QSIG from the **Tunneled Protocol** drop-down menu. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down menu, select one of • No Changes - Keep this parameter set to the default value unless a VOSS support engineer instructs otherwise. • Not Selected • Use Global Value ECMA - If you selected the ECMA option from the QSIG Variant drop-down menu, select this option. • Use Global Value ISO - If you selected the ISO option from the QSIG Variant drop-down menu, select this option. • Use Local Value Default value: No Changes
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. From the drop-down menu, select one of: • None - This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode - Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. Default value: None
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. Default value: 0 (zero), Range is from 0 to 300 minutes

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Media Termination Point Required	You can configure Unified CM SIP trunks to always use an Media Termination Point (MTP). Select this box to provide media channel information in the outgoing INVITE request. When this check box is selected, all media channels must terminate and reoriginate on the MTP device. If you clear the check box, the Unified CM can decide whether calls are to go through the MTP device or be connected directly between the endpoints. Note: If the check box remains clear, Unified CM attempts to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible. For example, existing phones that run SCCP support only out-of-band DTMF, and existing phones that run SIP support RFC2833. Because the DTMF methods are not identical, the Unified CM dynamically allocates an MTP. If, however, a new phone that runs SCCP, which supports RFC2833 and out-of band, calls an existing phone that runs SIP, Unified CM does not allocate an MTP because both phones support RFC2833. So, by having the same type of DTMF method supported on each phone, there is no need for MTP. Default value: False (Cleared)
Retry Video Call as Audio	This check box pertains to outgoing SIP trunk calls and does not impact incoming calls. By default, the system selects this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you clear this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call using Automatic Alternate Routing (AAR) and route list or hunt list. Default value: True (Selected)
Path Replacement Support	This check box is relevant when you select QSIG from the **Tunneled Protocol** drop-down menu. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement. Default value: False (Clear)
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you select this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool. If the user locale setting matches the terminating phone user locale, the phone displays the characters. Note: The phone may display malformed characters if the two ends of the trunk are configured with user locales that do not belong to the same language group. Default value: False (Cleared)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Transmit UTF-8 Names for QSIG APDU	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you select this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format. If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8 bit format) and encodes in ISO8859-1 format. Default value: False (Cleared)
Unattended Port	Select this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. Default value: False (Cleared)
SRTP Allowed	Select this check box if you want Unified CM to allow secure and nonsecure media calls over the trunk. Selecting this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not select this check box, Unified CM prevents SRTP negotiation with the trunk and uses RTP negotiation instead. Caution: If you select this check box, we strongly recommend that you use an encrypted TLS profile, so that keys and other security related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP still works but the keys get exposed in signaling and traces. In that case, you must ensure the security of the network between Unified CM and the destination side of the trunk. Default value: False (Cleared)
Consider Traffic on This Trunk Secure	This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. From the drop-down menu, select one of: • When using both sRTP and TLS • When using sRTP Only - Displays when you select the **SRTP Allowed** check box. Default value: When using both sRTP and TLS

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Route Class Signaling Enabled	From the drop-down menu, enable or disable route class signaling for the port. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the Hotline feature. From the drop-down menu, select one of: • Default - The device uses the setting from the Route Class Signaling service parameter • Off - Enables route class signaling. This setting overrides the Route Class Signaling service parameter • On - Disables route class signaling. This setting overrides the Route Class Signaling service parameter. Default value: Default
Use Trusted Relay Point	From the drop-down menu, enable or disable whether Unified CM inserts a trusted relay point (TRP) device with this media endpoint. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. If both TRP and RSVPAgent are needed for the endpoint, Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Unified CM first tries to find a transcoder that is also designated as a TRP. Select one of: • Default - The device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates • Off - Disables the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On - Enables the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. Default value: Default
PSTN Access	If you use the Cisco Intercompany Media Engine feature, select this check box to indicate that calls made through this trunk might reach the PSTN. Select this check box even if all calls through this trunk device do not reach the PSTN. For example, select this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When selected, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. Default value: True (Selected)
Run On All Active Unified CM Nodes	Select this check box to enable the trunk to run on every node. Default value: False (Cleared)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Call Routing General Fields

Option	Description
Remote-Party-ID	Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Unified CM to the remote destination. If you select this box, the SIP trunk always sends the RPID header. If you do not select this check box, the SIP trunk does not send the RPID header. Note: Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled. Outgoing SIP Trunk Calls The configured values of the Calling Line ID Presentation and Calling Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. If either option is set to Default, the corresponding information (Calling Line ID Presentation and/or Calling Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Unified CM. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Incoming SIP Trunk Calls The configured values of the Connected Line ID Presentation and Connected Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. Be aware that the Connected Line ID Presentation and Connected Name Presentation options are relevant for 180/200 messages that the SIP trunk sends in response to INVITE messages that Unified CM receives. If either option is set to Default, the corresponding information (Connected Line ID Presentation and/or Connected Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Unified CM. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Asserted-Identity	Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you select this check box, the SIP trunk always sends the Asserted-Type header; whether or not the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. Outgoing SIP Trunk Calls - P Headers The decision of which Asserted Identity (either P-Asserted Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Unified CM Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Unified CM Call Control dictates the type of Asserted-Identity. Outgoing SIP Trunk Calls - SIP Privacy Header The SIP Privacy header gets used only when you select the **Asserted-Identity** check box and when the SIP trunk sends either a Privacy-Asserted Identity (PAI) or Privacy Preferred Identity (PPI) header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages). The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Unified CM Call Control. If the SIP Privacy option is set to Default, the Calling Line ID Presentation and Calling Name Presentation that the SIP trunk receives from Unified CM Call Control determines the SIP Privacy header. Incoming SIP Trunk Calls - P Headers The decision of which Asserted Identity (either P-Asserted Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Unified CM Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Unified CM Call Control dictates the type of Asserted-Identity. Incoming SIP Trunk Calls - SIP Privacy Header The SIP Privacy header gets used only when you select the **Asserted Identity** check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages.) The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Unified CM Call Control. If the SIP Privacy option is set to Default, the Connected Line ID Presentation and Connected Name Presentation that the SIP trunk receives from Unified CM Call Control determine the SIP Privacy header. Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Asserted-Type	From the drop-down menu, select one of the following values to specify the type of Asserted Identity header that SIP trunk messages should include: • Default - Screening information that the SIP trunk receives from Unified CM Call Control determines the type of header that the SIP trunk sends. • PAI - The Privacy-Asserted Identity header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Unified CM. • PPI - The Privacy Preferred Identity header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Unified CM. Note: These headers get sent only if the **Asserted- Identity** check box is selected. Default value: Default
SIP Privacy	From the drop-down menu, select one of the following values to specify the type of SIP privacy header for SIP trunk messages to include: • Default - This option represents the default value; Name/Number Presentation values that the SIP trunk receives from the Unified CM Call Control compose the SIP Privacy header. For example, if Name/Number presentation specifies Restricted, the SIP trunk sends the SIP Privacy header; however, if Name/Number presentation specifies Allowed, the SIP trunk does not send the Privacy header. • None - The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Unified CM. • ID - The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Unified CM. • ID Critical - The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label critical implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Unified CM. Note: These headers get sent only if the **Asserted Identity** check box is selected. Default value: Default

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Call Routing Inbound Fields

Option	Description
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32, or choose 99 to indicate all digits. Note: Unified CM counts significant digits from the right (last digit) of the number that is called. Default value: 99
Connected Line ID Presentation	Unified CM uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send connected line information. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. • Restricted - Choose Restricted if you do not want Unified CM to send connected line information. Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default
Connected Name Presentation	Unified CM uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send connected name information. • Restricted - Choose Restricted if you do not want Unified CM to send connected name information. Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default
Calling Search Space	From the drop-down menu, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down menu by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Find and List Calling Search Spaces window. Find and choose a calling search space name. Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. Default value: None

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. Default value: None
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Unified CM adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +. Default value: None
Redirecting Diversion Header - Delivery Inbound	Select this check box to accept the Redirecting Number in the incoming INVITE message to the Unified CM. Clear the check box to exclude the Redirecting Number in the incoming INVITE message to the Unified CM. You use Redirecting Number for voice messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should select the check box. Default value: False (Cleared)
Incoming Calling Party - Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape field, you cannot configure the Strip Digits field. In this case, Unified CM takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. Default value: None
Incoming Calling Party - Strip Digits	Enter the number of digits, up to the number 24, that you want Unified CM to strip from the calling party number of Unknown type before it applies the prefixes. Default value: None
Incoming Calling Party - Calling Search Space	This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing. Default value: None

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Incoming Calling Party - Use Device Pool CSS	Select this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. Default value: True (Selected)
Incoming Called Party - Prefix	Unified CM applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. Tip: If the word Default displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Unified CM takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word Default displays in the Prefix field in the Device Pool Configuration window, Unified CM does not apply any prefix or strip digit functionality. Default value: None
Incoming Called Party - Strip Digits	Enter the number of digits that you want Unified CM to strip from the called party number of Unknown type before it applies the prefixes. Tip: To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. Default value: None
Incoming Called Party - Calling Search Space	This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device. Default value: None
Incoming Called Party - Use Device Pool CSS	Select this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. Default value: True (Selected)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Connected Party Transformation CSS	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Unified CM includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update and reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. Note: If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing. Default value: None
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window. Default value: True (Selected)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Call Routing Outbound Fields

Option	Description
Called Party Transformation CSS	This setting allows you to send the transformed called party number in an INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. Note: If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing. Default value: None
Use Device Pool Called Party Transformation CSS	To use the Called Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Called Party Transformation CSS that you configured for this device in the Trunk Configuration window. Default value: True (Selected)
Calling Party Transformation CSS	This setting allows you to send the transformed calling party number in an INVITE message for outgoing calls made over a SIP Trunk. Also when redirection occurs for outbound calls, this CSS is used to transform the connected number that is sent from Unified CM side in outgoing reINVITE / UPDATE messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Tip: If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing. Default value: None
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window. Default value: True (Selected)
Calling Party Selection	Choose the directory number that is sent on an outbound call. Select one of the following options to specify which directory number is sent: • Originator - Send the directory number of the calling device • First Redirect Number - Send the directory number of the redirecting device. • Last Redirect Number - Send the directory number of the last device to redirect the call. • First Redirect Number (External) - Send the external directory number of the redirecting device • Last Redirect Number (External) - Send the external directory number of the last device to redirect the call. Default value: Originator

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Calling Line ID Presentation	Unified CM uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send calling number information. • Restricted - Choose Restricted if you do not want Unified CM to send the calling number information. Default value: Default
Calling Name Presentation	Unified CM used calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send calling name information. • Restricted - Choose Restricted if you do not want Unified CM to send the calling name information. Note: This service is not available when QSIG tunneling is enabled. Default value: Default
Calling and Connected Party Info Format *	This option allows you to configure whether Unified CM inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages. From the drop-down menu, select one of: • Deliver DN only in connected party - In outgoing SIP messages, Unified CM inserts the calling party - s directory number in the SIP contact header information. • Deliver URI only in connected party, if available - In outgoing SIP messages, Unified CM inserts the sending party - s directory URI in the SIP contact header. If a directory URI is not available, Unified CM inserts the directory number instead. • Deliver URI and DN in connected party, if available - In outgoing SIP messages, Unified CM inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Unified CM includes the directory number only. Note: You should set this field to Deliver URI only in connected party or Deliver URI and DN in connected party only if you are setting up URI dialing between Unified CM systems of Release 9.0 or greater, or between a Cisco Unified Communications Manager system of Release 9. 0 or greater and a third party solution that supports URI dialing. Otherwise, you must set this field to Deliver DN only in connected party. Default value: Deliver DN only in connected party

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Redirecting Diversion Header Delivery - Outbound	Select this check box to include the Redirecting Number in the outgoing INVITE message from the Unified CM to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Clear the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. Use Redirecting Number for voice-messaging integration only. If your configured voice messaging system supports Redirecting Number, select the check box. Default value: False (Cleared)
Use Device Pool Redirecting Party Transformation CSS	Select this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to this device. If you do not select this check box, the device uses the Redirecting Party Transformation CSS that you configured for this device (see field below).
Redirecting Party Transformation CSS	Allows you to localize the redirecting party number on the device. Make sure that the Redirecting Party Transformation CSS that you enter contains the redirecting party transformation pattern that you want to assign to this device.
Caller Information Caller ID DN	Enter the pattern, from 0 to 24 digits that you want to use to format the Called ID on outbound calls from the trunk. For example, in North America: • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +. Default value: None
Caller Information - Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device. Default value: None
Caller Information - Maintain Original Caller ID DN and Caller Name in Identity Headers	This check box is used to specify whether you will use the caller ID and caller name in the URI outgoing request. If you select this check box, the caller ID and caller name is used in the URI outgoing request. If you do not select this check box, the caller ID and caller name is not used in the URI outgoing request. Default value: False (Cleared)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

SP Info Fields

Option	Description
Destination Address is an SRV	This field specifies that the configured Destination Address is an SRV record. Default value: False (Cleared)
Destination - Destination Address IPv4	The Destination Address IPv4 represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is selected. Tip: For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field. Note: SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. Note: For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and select the Destination Address is an SRV Destination Port check box. If the remote end is a Unified CM cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Unified CMs within the cluster. Default value: None
Destination - Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is selected. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Unified CM cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Unified CMs within the cluster. Tip: For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field. Default value: None. If IPv4 field above is completed, this field can be left blank.
Destination - Destination port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0. Note: You can now have the same port number that is specified for multiple trunks. You do not need to enter a value if the destination address is a DNS SRV port. The default 5060 indicates the SIP port. Default value: 5060

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Sort Order *	Indicate the order in which the prioritize multiple destinations. A lower sort order indicates higher priority. This field requires an integer value. Default value: Empty
Destination Address is an SRV	This field specifies that the configured Destination Address is an SRV record. Default value: False (Cleared)
Destination - Destination Address IPv4	The Destination Address IPv4 represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is selected. Tip: For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field. Note: SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. Note: For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and select the Destination Address is an SRV Destination Port check box. If the remote end is a Unified CM cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Unified CMs within the cluster. Default value: None
Destination - Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is selected. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Unified CM cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Unified CMs within the cluster. Tip: For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field. Default value: None. If IPv4 field above is completed, this field can be left blank.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Destination - Destination port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0. Note: You can now have the same port number that is specified for multiple trunks. You do not need to enter a value if the destination address is a DNS SRV port. The default 5060 indicates the SIP port. Default value: 5060
Sort Order *	Indicate the order in which the prioritize multiple destinations. A lower sort order indicates higher priority. This field requires an integer value. Default value: Empty
MTP Preferred Originating Codec	Indicate the preferred outgoing codec by selecting one of: • 711ulaw • 711alaw • G729/G729a • G729b/G729ab Note: To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. This field is used only when the **Media Termination Point Required** check box is selected on the **Device Information** tab. Default value: 711ulaw
BLF Presence Group *	Configure this field with the Presence feature. From the drop-down menu, select a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor. • Standard Presence group is configured with installation. Presence groups that are configured in Unified CM Administration also appear in the drop-down menu. • Presence authorization works with presence groups to allow or block presence requests between groups. Tip: You can apply a presence group to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk. Default value: Standard Presence Group

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
SIP Trunk Security Profile *	Select the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks that are configured in Unified CM Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. Default value: Non Secure SIP Trunk Profile
Rerouting Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. Default value: None
Out-Of-Dialog Refer Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The out-of-dialog calling search space gets used when a Unified CM refers a call (B) that is coming into SIP user (A) to a third party (C) when no involvement of SIP user (A) exists. In this case, the system uses the out-of dialog calling search space of SIP user (A). Default value: None
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified CM routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk. From the drop-down menu, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Unified CM Administration display in the SUBSCRIBE Calling Search Space drop-down menu. If you do not select a different calling search space for the SIP trunk from the drop-down menu, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, configure a calling search space as you do all calling search spaces. Default value: None
SIP Profile *	From the drop-down list box, select the SIP profile that is to be used for this SIP trunk. Default value: Standard SIP Profile

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
DTMF Signaling Method	Select one of: • No Preference - Unified CM picks the DTMF method to negotiate DTMF, so the call does not require an MTP. If Cisco Unified Communications Manager has no choice but to allocate an MTP (if the **Media Termination Point Required** check box is selected on the **Device Information** tab), SIP trunk negotiates DTMF to RFC2833. • RFC 2833 - Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Unified CM makes every effort to negotiate RFC2833, regardless of MTP usage. Out of band (OOB) provides the fallback method if the peer endpoint supports it. • OOB and RFC 2833 - Choose this configuration if both out of band and RFC2833 should be used for DTMF. Note: If the peer endpoint supports both out of band and RFC2833, Unified CM negotiates both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events are sent for the same DTMF keypress (one out of band and the other, RFC2833). Default value: No Preference
Normalization Script	From the drop-down menu, choose the script that you want to apply to this trunk. To import another script, on Unified CM go to the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script), and import a new script file. Default value: None
Normalization Script - Enable Trace	Select this check box to enable tracing within the script or clear the check box to disable tracing. When selected, the trace.output API provided to the Lua scripter produces SDI trace. Note: We recommend that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions. Default value: False (Cleared)
Script Parameters	Enter parameter names and values in the format Param1Name=Param1Value; Param2Name=Param2Value where Param1Name is the name of the first script parameter and Param1Value is the value of the first script parameter. Multiple parameters can be specified by putting semicolon after each name and value pair . Valid values include all characters except equal signs (=), semi-colons (;); and non-printable characters, such as tabs. You can enter a parameter name with no value.
Recording Information	Enter one of • 0 - None (default) • 1 - This trunk connects to a recording-enabled gateway • 2 - This trunk connects to other clusters with recording-enabled gateways

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

GeoLocation Fields

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)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.22.2. SIP Trunks Field Descriptions

Device Information Tab

Option	Description
Device Name (Mandatory)	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 (Optional)	Choose one of: • **None** - Choose this option if the trunk is not used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine • **Call Control Discovery** - Choose this option to enable the trunk to support call control discovery. • **Extension Mobility Cross Cluster** - Choose this option to enable the trunk to support the Extension Mobility Cross Cluster (EMCC) feature. Choosing this option causes the following settings to remain blank or clear and become unavailable for configuration, thus retaining their default values: Media Termination Point Required, Unattended Port, Destination Address, Destination Address IPv6, and Destination Address is an SRV. • **Cisco Intercompany Media Engine** - Ensure that the Cisco IME server is installed and available before you configure this field. • **IP Multimedia Subsystem Service Control (ISC)** - Choose this option to enable the trunk to support IP multimedia subsystem service control. Default value: None (Default)
Description (Optional)	Enter a descriptive name for the trunk using up to 114 characters in any language, but not including double-quotes (“), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>). Default value: empty
Device Pool (Mandatory)	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 (Optional)	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 (Optional)	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Unified CM clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Default value: Use System Default

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Media Resource Group List (Optional)	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. Default value: None
Location (Mandatory)	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. Choose the appropriate location for this trunk: • Hub_None - Specifies that the locations feature does not keep track of the bandwidth that this trunk consumes. • Phantom - Specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. • Shadow - Specifies a location for intercluster enhanced location CAC. Valid for SIP intercluster trunks (ICT) only. Default value: Hub_None
AAR Group (Optional)	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls is attempted. Default value: None
Tunneled Protocol	Choose the QSIG option if you want to use SIP trunks or SIP gateways to transport (tunnel) QSI messages from Unified CM to other PINXs. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Path Replacement, and Message Waiting Indication (MWI). Note: Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway. Default value: None
QSIG Variant	To display the options in the **QSIG Variant** drop-down list, choose QSIG from the **Tunneled Protocol** drop-down menu. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down menu, select one of: • No Changes - Default. Keep this parameter set to the default value unless a VOSS support engineer instructs otherwise. • Not Selected • ECMA - Select for ECMA PBX systems that use Protocol Profile 0x91 • ISO - Select for PBX systems that use Protocol Profile 0x9F Default value: No Changes

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down menu, choose QSIG from the **Tunneled Protocol** drop-down menu. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down menu, select one of • No Changes - Keep this parameter set to the default value unless a VOSS support engineer instructs otherwise. • Not Selected • Use Global Value ECMA - If you selected the ECMA option from the QSIG Variant drop-down menu, select this option. • Use Global Value ISO - If you selected the ISO option from the QSIG Variant drop-down menu, select this option. • Use Local Value Default value: No Changes
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. From the drop-down menu, select one of: • None - This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode - Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. Default value: None
Packet Capture Duration (Optional)	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. Default value: 0 (zero), Range is from 0 to 300 minutes
Media Termination Point Required (Optional)	You can configure Unified CM SIP trunks to always use an Media Termination Point (MTP). Select this box to provide media channel information in the outgoing INVITE request. When this check box is selected, all media channels must terminate and reoriginate on the MTP device. If you clear the check box, the Unified CM can decide whether calls are to go through the MTP device or be connected directly between the endpoints. Note: If the check box remains clear, Unified CM attempts to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible. For example, existing phones that run SCCP support only out-of-band DTMF, and existing phones that run SIP support RFC2833. Because the DTMF methods are not identical, the Unified CM dynamically allocates an MTP. If, however, a new phone that runs SCCP, which supports RFC2833 and out-of band, calls an existing phone that runs SIP, Unified CM does not allocate an MTP because both phones support RFC2833. So, by having the same type of DTMF method supported on each phone, there is no need for MTP. Default value: False (Cleared)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Retry Video Call as Audio (Optional)	This check box pertains to outgoing SIP trunk calls and does not impact incoming calls. By default, the system selects this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you clear this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call using Automatic Alternate Routing (AAR) and route list or hunt list. Default value: True (Selected)
Path Replacement Support (Optional)	This check box is relevant when you select QSIG from the **Tunneled Protocol** drop-down menu. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement. Default value: False (Clear)
Transmit UTF-8 for Calling Party Name (Optional)	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you select this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool. If the user locale setting matches the terminating phone user locale, the phone displays the characters. Note: The phone may display malformed characters if the two ends of the trunk are configured with user locales that do not belong to the same language group. Default value: False (Cleared)
Transmit UTF-8 Names for QSIG APDU (Optional)	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 (Optional)	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)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
SRTP Allowed (Optional)	Select this check box if you want Unified CM to allow secure and nonsecure media calls over the trunk. Selecting this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not select this check box, Unified CM prevents SRTP negotiation with the trunk and uses RTP negotiation instead. Caution: If you select this check box, we strongly recommend that you use an encrypted TLS profile, so that keys and other security related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP still works but the keys get exposed in signaling and traces. In that case, you must ensure the security of the network between Unified CM and the destination side of the trunk. Default value: False (Cleared)
Consider Traffic on This Trunk Secure	This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. From the drop-down menu, select one of: • When using both sRTP and TLS • When using sRTP Only - Displays when you select the **SRTP Allowed** check box. Default value: When using both sRTP and TLS
Route Class Signaling Enabled	From the drop-down menu, enable or disable route class signaling for the port. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the Hotline feature. From the drop-down menu, select one of: • Default - The device uses the setting from the Route Class Signaling service parameter • Off - Enables route class signaling. This setting overrides the Route Class Signaling service parameter • On - Disables route class signaling. This setting overrides the Route Class Signaling service parameter. Default value: Default
Use Trusted Relay Point	From the drop-down menu, enable or disable whether Unified CM inserts a trusted relay point (TRP) device with this media endpoint. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. If both TRP and RSVPAgent are needed for the endpoint, Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Unified CM first tries to find a transcoder that is also designated as a TRP. Select one of: • Default - The device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates • Off - Disables the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On - Enables the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. Default value: Default

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
PSTN Access (Optional)	If you use the Cisco Intercompany Media Engine feature, select this check box to indicate that calls made through this trunk might reach the PSTN. Select this check box even if all calls through this trunk device do not reach the PSTN. For example, select this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When selected, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. Default value: True (Selected)
Run On All Active Unified CM Nodes (Optional)	Select this check box to enable the trunk to run on every node. Default value: False (Cleared)

Call Routing General Tab

Option	Description
Remote-Party-ID (Optional)	Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Unified CM to the remote destination. If you select this box, the SIP trunk always sends the RPID header. If you do not select this check box, the SIP trunk does not send the RPID header. Note: Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled. Outgoing SIP Trunk Calls The configured values of the Calling Line ID Presentation and Calling Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. If either option is set to Default, the corresponding information (Calling Line ID Presentation and/or Calling Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Unified CM. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Incoming SIP Trunk Calls The configured values of the Connected Line ID Presentation and Connected Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. Be aware that the Connected Line ID Presentation and Connected Name Presentation options are relevant for 180/200 messages that the SIP trunk sends in response to INVITE messages that Unified CM receives. If either option is set to Default, the corresponding information (Connected Line ID Presentation and/or Connected Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Unified CM. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Asserted-Identity (Optional)	Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you select this check box, the SIP trunk always sends the Asserted-Type header; whether or not the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. Outgoing SIP Trunk Calls - P Headers The decision of which Asserted Identity (either P-Asserted Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Unified CM Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Unified CM Call Control dictates the type of Asserted-Identity. Outgoing SIP Trunk Calls - SIP Privacy Header The SIP Privacy header gets used only when you select the **Asserted-Identity** check box and when the SIP trunk sends either a Privacy-Asserted Identity (PAI) or Privacy Preferred Identity (PPI) header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages). The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Unified CM Call Control. If the SIP Privacy option is set to Default, the Calling Line ID Presentation and Calling Name Presentation that the SIP trunk receives from Unified CM Call Control determines the SIP Privacy header. Incoming SIP Trunk Calls - P Headers The decision of which Asserted Identity (either P-Asserted Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Unified CM Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Unified CM Call Control dictates the type of Asserted-Identity. Incoming SIP Trunk Calls - SIP Privacy Header The SIP Privacy header gets used only when you select the **Asserted Identity** check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages.) The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Unified CM Call Control. If the SIP Privacy option is set to Default, the Connected Line ID Presentation and Connected Name Presentation that the SIP trunk receives from Unified CM Call Control determine the SIP Privacy header. Note: The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information. Default value: True (Selected)
Asserted-Type	From the drop-down menu, select one of the following values to specify the type of Asserted Identity header that SIP trunk messages should include: • Default - Screening information that the SIP trunk receives from Unified CM Call Control determines the type of header that the SIP trunk sends. • PAI - The Privacy-Asserted Identity header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Unified CM. • PPI - The Privacy Preferred Identity header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Unified CM. Note: These headers get sent only if the **Asserted- Identity** check box is selected. Default value: Default

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
SIP Privacy	From the drop-down menu, select one of the following values to specify the type of SIP privacy header for SIP trunk messages to include: • Default - This option represents the default value; Name/Number Presentation values that the SIP trunk receives from the Unified CM Call Control compose the SIP Privacy header. For example, if Name/Number presentation specifies Restricted, the SIP trunk sends the SIP Privacy header; however, if Name/Number presentation specifies Allowed, the SIP trunk does not send the Privacy header. • None - The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Unified CM. • ID - The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Unified CM. • ID Critical - The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label critical implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Unified CM. Note: These headers get sent only if the **Asserted Identity** check box is selected. Default value: Default

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Call Routing Inbound Tab

Option	Description
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32, or choose 99 to indicate all digits. Note: Unified CM counts significant digits from the right (last digit) of the number that is called. Default value: 99
Connected Line ID Presentation	Unified CM uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send connected line information. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. • Restricted - Choose Restricted if you do not want Unified CM to send connected line information. Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default
Connected Name Presentation	Unified CM uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send connected name information. • Restricted - Choose Restricted if you do not want Unified CM to send connected name information. Note: Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default
Calling Search Space (Optional)	From the drop-down menu, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down menu by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Find and List Calling Search Spaces window. Find and choose a calling search space name. Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. Default value: None

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
AAR Calling Search Space (Optional)	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 (Optional)	Enter the prefix digits that are appended to the called party number on incoming calls. Unified CM adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +. Default value: None
Redirecting Diversion Header - Delivery Inbound (Optional)	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 (Optional)	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 (Optional)	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 (Optional)	This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing. Default value: None

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Incoming Calling Party - Use Device Pool CSS (Optional)	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 (Optional)	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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Incoming Called Party - Strip Digits (Optional)	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 (Optional)	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 (Optional)	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)
Connected Party Transformation CSS (Optional)	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Unified CM includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update and reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. Note: If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing. Default value: None
Use Device Pool Connected Party Transformation CSS (Optional)	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window. Default value: True (Selected)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Call Routing Outbound Tab

Option	Description
Called Party Transformation CSS (Optional)	This setting allows you to send the transformed called party number in an INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. Note: If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing. Default value: None
Use Device Pool Called Party Transformation CSS (Optional)	To use the Called Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Called Party Transformation CSS that you configured for this device in the Trunk Configuration window. Default value: True (Selected)
Calling Party Transformation CSS (Optional)	This setting allows you to send the transformed calling party number in an INVITE message for outgoing calls made over a SIP Trunk. Also when redirection occurs for outbound calls, this CSS is used to transform the connected number that is sent from Unified CM side in outgoing reINVITE / UPDATE messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Tip: If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing. Default value: None
Use Device Pool Calling Party Transformation CSS (Optional)	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window. Default value: True (Selected)
Calling Party Selection	Choose the directory number that is sent on an outbound call. Select one of the following options to specify which directory number is sent: • Originator - Send the directory number of the calling device • First Redirect Number - Send the directory number of the redirecting device. • Last Redirect Number - Send the directory number of the last device to redirect the call. • First Redirect Number (External) - Send the external directory number of the redirecting device • Last Redirect Number (External) - Send the external directory number of the last device to redirect the call. Default value: Originator

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Calling Line ID Presentation	Unified CM uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send calling number information. • Restricted - Choose Restricted if you do not want Unified CM to send the calling number information. Default value: Default
Calling Name Presentation	Unified CM used calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Select one of • Default - Allowed. Choose Default if you want Unified CM to send calling name information. • Restricted - Choose Restricted if you do not want Unified CM to send the calling name information. Note: This service is not available when QSIG tunneling is enabled. Default value: Default
Calling and Connected Party Info Format (Mandatory)	This option allows you to configure whether Unified CM inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages. From the drop-down menu, select one of: • Deliver DN only in connected party - In outgoing SIP messages, Unified CM inserts the calling party - s directory number in the SIP contact header information. • Deliver URI only in connected party, if available - In outgoing SIP messages, Unified CM inserts the sending party - s directory URI in the SIP contact header. If a directory URI is not available, Unified CM inserts the directory number instead. • Deliver URI and DN in connected party, if available - In outgoing SIP messages, Unified CM inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Unified CM includes the directory number only. Note: You should set this field to Deliver URI only in connected party or Deliver URI and DN in connected party only if you are setting up URI dialing between Unified CM systems of Release 9.0 or greater, or between a Cisco Unified Communications Manager system of Release 9. 0 or greater and a third party solution that supports URI dialing. Otherwise, you must set this field to Deliver DN only in connected party. Default value: Deliver DN only in connected party

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Redirecting Diversion Header Delivery - Outbound (Optional)	Select this check box to include the Redirecting Number in the outgoing INVITE message from the Unified CM to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Clear the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. Use Redirecting Number for voice-messaging integration only. If your configured voice messaging system supports Redirecting Number, select the check box. Default value: False (Cleared)
Use Device Pool Redirecting Party Transformation CSS (Optional)	Select this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to this device. If you do not select this check box, the device uses the Redirecting Party Transformation CSS that you configured for this device (see field below).
Redirecting Party Transformation CSS (Optional)	Allows you to localize the redirecting party number on the device. Make sure that the Redirecting Party Transformation CSS that you enter contains the redirecting party transformation pattern that you want to assign to this device.
Caller Information Caller ID DN (Optional)	Enter the pattern, from 0 to 24 digits that you want to use to format the Called ID on outbound calls from the trunk. For example, in North America: • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +. Default value: None
Caller Information - Caller Name (Optional)	Enter a caller name to override the caller name that is received from the originating SIP Device. Default value: None
Caller Information - Maintain Original Caller ID DN and Caller Name in Identity Headers (Optional)	This check box is used to specify whether you will use the caller ID and caller name in the URI outgoing request. If you select this check box, the caller ID and caller name is used in the URI outgoing request. If you do not select this check box, the caller ID and caller name is not used in the URI outgoing request. Default value: False (Cleared)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

SP Info Tab

Option	Description
Destination Address is an SRV (Optional)	This field specifies that the configured Destination Address is an SRV record. Default value: False (Cleared)
Destination - Destination Address IPv4	The Destination Address IPv4 represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is selected. Tip: For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field. Note: SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. Note: For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and select the Destination Address is an SRV Destination Port check box. If the remote end is a Unified CM cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Unified CMs within the cluster. Default value: None
Destination - Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is selected. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Unified CM cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Unified CMs within the cluster. Tip: For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field. Default value: None. If IPv4 field above is completed, this field can be left blank.
Destination - Destination port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0. Note: You can now have the same port number that is specified for multiple trunks. You do not need to enter a value if the destination address is a DNS SRV port. The default 5060 indicates the SIP port. Default value: 5060
Sort Order (Mandatory)	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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
MTP Preferred Originating Codec	Indicate the preferred outgoing codec by selecting one of: • 711ulaw • 711alaw • G729/G729a • G729b/G729ab Note: To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. This field is used only when the **Media Termination Point Required** check box is selected on the **Device Information** tab. Default value: 711ulaw
BLF Presence Group (Mandatory)	Configure this field with the Presence feature. From the drop-down menu, select a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor. • Standard Presence group is configured with installation. Presence groups that are configured in Unified CM Administration also appear in the drop-down menu. • Presence authorization works with presence groups to allow or block presence requests between groups. Tip: You can apply a presence group to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk. Default value: Standard Presence Group
SIP Trunk Security Profile (Mandatory)	Select the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks that are configured in Unified CM Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. Default value: Non Secure SIP Trunk Profile
Rerouting Calling Search Space (Optional)	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. Default value: None
Out-Of-Dialog Refer Calling Search Space (Optional)	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The out-of-dialog calling search space gets used when a Unified CM refers a call (B) that is coming into SIP user (A) to a third party (C) when no involvement of SIP user (A) exists. In this case, the system uses the out-of dialog calling search space of SIP user (A). Default value: None

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
SUBSCRIBE Calling Search Space (Optional)	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified CM routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk. From the drop-down menu, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Unified CM Administration display in the SUBSCRIBE Calling Search Space drop-down menu. If you do not select a different calling search space for the SIP trunk from the drop-down menu, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, configure a calling search space as you do all calling search spaces. Default value: None
SIP Profile (Mandatory)	From the drop-down list box, select the SIP profile that is to be used for this SIP trunk. Default value: Standard SIP Profile
DTMF Signaling Method	Select one of: • No Preference - Unified CM picks the DTMF method to negotiate DTMF, so the call does not require an MTP. If Cisco Unified Communications Manager has no choice but to allocate an MTP (if the **Media Termination Point Required** check box is selected on the **Device Information** tab), SIP trunk negotiates DTMF to RFC2833. • RFC 2833 - Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Unified CM makes every effort to negotiate RFC2833, regardless of MTP usage. Out of band (OOB) provides the fallback method if the peer endpoint supports it. • OOB and RFC 2833 - Choose this configuration if both out of band and RFC2833 should be used for DTMF. Note: If the peer endpoint supports both out of band and RFC2833, Unified CM negotiates both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events are sent for the same DTMF keypress (one out of band and the other, RFC2833). Default value: No Preference
Normalization Script (Optional)	From the drop-down menu, choose the script that you want to apply to this trunk. To import another script, on Unified CM go to the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script), and import a new script file. Default value: None
Normalization Script - Enable Trace (Optional)	Select this check box to enable tracing within the script or clear the check box to disable tracing. When selected, the trace.output API provided to the Lua scripter produces SDI trace. Note: We recommend that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions. Default value: False (Cleared)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Script Parameters (Optional)	Enter parameter names and values in the format Param1Name=Param1Value; Param2Name=Param2Value where Param1Name is the name of the first script parameter and Param1Value is the value of the first script parameter. Multiple parameters can be specified by putting semicolon after each name and value pair . Valid values include all characters except equal signs (=), semi-colons (;); and non-printable characters, such as tabs. You can enter a parameter name with no value.
Recording Information (Optional)	Enter one of • 0 - None (default) • 1 - This trunk connects to a recording-enabled gateway • 2 - This trunk connects to other clusters with recording-enabled gateways

GeoLocation Tab

Option	Description
Geolocation (Optional)	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 (Optional)	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 (Optional)	Select this check box to send geolocation information for this device. Default value: False (Cleared)

2.22.3. Reset SIP Trunks

Use this procedure to shut down a SIP trunk and bring it back into service. This procedure does not physically reset the hardware; it only reinitializes the configuration that is loaded by the Cisco Unified Communications Manager cluster. To restart a SIP trunk without shutting it down, use Restart SIP Trunks.

Procedure

1. Log in as provider, reseller or customer administrator.
2. Perform one of:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > SIP Trunks**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > SIP Trunks**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

2.22.4. Restart SIP Trunks

Use this procedure to restart a SIP trunk without shutting it down first. To shut down a SIP trunk prior to the reset, see *Reset SIP Trunks*.

Note: If the SIP trunk is not registered with Cisco Unified Communications Manager, you cannot restart it.

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

Procedure

1. Log in as provider, reseller or customer administrator.
2. Perform one of:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > SIP Trunks**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > SIP Trunks**.
3. From the list of trunks, click the SIP trunk to be restarted, then click **Action > Restart**.

2.23. Configure SIP Route Patterns

2.23.1. How to Configure SIP Route Patterns

Before You Begin

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

Cisco Unified Communications Manager 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.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to a customer or site level.
3. If prompted, choose the NDL that contains the Cisco Unified CM on which you are configuring the SIP Route Pattern.
4. Perform one of the following:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- If you logged in as provider or reseller administrator, choose **Device Management > CUCM > SIP Route Patterns**.
- If you logged in as customer administrator, choose **Device Management > Advanced > SIP Route Patterns**.

5. Click **Add**.
6. On the **Pattern Definition** tab, complete the *Pattern Definition Fields*.
7. Click the **Calling Party Transformations** tab, complete the *Calling Party Transformations Fields*.
8. Click the **Connected Party Transformations** tab, complete the *Connected Party Transformations Fields*.
9. Click **Save** when complete.

Pattern Definition Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Calling Party Transformations Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Connected Party Transformations Fields

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

2.24. Configure Route Groups

2.24.1. How to Configure Route Groups

Before You Begin

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

A route group allows you to designate 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.

Use this procedure to add or modify route groups.

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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Procedure

1. Log in as provider, reseller or customer administrator.
2. Perform one of:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Route Groups**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > Route Groups**.
3. Perform one of:
   - To add a new route group, click **Add**.
   - To edit an existing route group, click the group to be updated, edit the fields as required, then click **Save** to save the edited route group.
4. From the **CUCM** drop-down menu, choose or modify the Cisco Unified Communications Manager that corresponds to the route group.
5. Enter a unique name for the new route group in the **Route Group Name** field, or modify the existing Route Group Name if desired. The 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.

   Tip:

   Use concise and descriptive names for the route group. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route group. For example, - CiscoDallasAA1 - identifies a Cisco Access Analog route group for the Cisco office in Dallas.
6. From the drop-down menu, select or modify the Distribution Algorithm options for the route group. Default value is Circular.

Option	Description
Top Down	Select this option if you want Cisco Unified Communications Manager 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. Note: You need to select Top Down to prioritize the order of devices in Step 10.
Circular	Chose this option if you want Cisco Unified 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 Cisco Unified Communications Manager most recently extended a call. If the nth member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group.

7. Click + to open the **Members** box. Perform one or more of the following steps:
   - To add a device to the route group, perform Step 8.
   - To modify the priority of a device, go to Step 10.
   - To remove a device from the route group, go to Step 11.
8. To add a device to the route group:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

   Note:

   When a SIP trunk or gateway is added, all ports on the device are selected.

b. For Device Selection Order, indicate the order in which to prioritize multiple devices. A lower selection order indicates higher priority. This field requires an integer value. The default is no setting. The device selection order, if specified, overrides the position of the device in the list.

9. To add another device to the route group, click + at the top of the **Members** box, then repeat Steps 8 and 9 for each additional device.
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. To remove a device from the route group, select the device in the Members box and click the - on the right side of the **Members** box.

    Note:

    You must leave at least one device in the route group.
12. To save a new or updated route group, click **Save**. The route group appears in the **Route Group** list.

2.24.2. Delete Route Groups

Procedure

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. Perform one of:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Route Groups**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > Route Groups**.
3. From the list of trunks, choose the route group to be deleted, by clicking on its check box in the leftmost column. The Route Group profile appears.
4. Click **Delete** to delete the Route Group.
5. From the popup window, click **Yes** to confirm the deletion.

2.25. Configure Route Lists

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.25.1. How to Configure Route Lists

Before You Begin

Configure route groups before performing this procedure.

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

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

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

Use the following procedure to add route lists or to add, remove or change the order of route groups in a route list.

Procedure

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. Perform one of the following:

   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Route Lists**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > Route Lists**.

3. Perform one of:

   - To add a new route list, click **Add**, then go to Step 4.
   - To edit an existing route list, choose the list to be updated by clicking on its box in the leftmost column, then click **Edit** to update the selected route list. Go to Step 5.

4. Complete at minimum, the mandatory *Route Lists Details Fields*.
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 Items Fields*.
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**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Route Lists Details Fields

Field	Description
CUCM *	Select a Unified CM for the route list. This field is mandatory.
Name *	Enter a unique name for the new route list. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, period(s), hyphens (-), and underscore characters (_). This field is mandatory. Tip: Use concise and descriptive names for the route list. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route list. For example, 'CiscoDallasMetro' identifies a route list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.
Description	A description of the route list.
Call Manager Group Name *	Select a Unified CM Group. Default is the default field. You can choose from **Default**, **None**, or select a group. This field is mandatory. Note: The route list registers with the first Unified CM in the group (which is the Primary Unified CM).
Route List Enabled	Select to enable the route list. This is the default. Clear to disable the route list. When disabling a route list, calls in progress do not get affected, but the route list does not accept additional calls.
Run on Every Node	Select to enable the active route list to run on every node.
Route Group Items	See "Route Group Items fields".

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Route Group Items Fields

Field	Description
Route Group *	Choose the route group. This field is mandatory.
Selection Order	Indicate the order in which to prioritize multiple routes. A lower selection order indicates higher priority. This field requires an integer value. The default is no setting.
Use Calling Party's External Phone Number Mask *	Choose **On** from the drop-down list if you want the full external phone number to be used for calling line identification (CLID) on outgoing calls. Choose **Off** or **Default** if you do not want to use the full external phone number for CLID on outgoing calls. You may also configure an External Phone Number Mask on all phone devices. This field is mandatory.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the **Digit Discards** field is blank, the **Prefix Digits** field is blank, the **Calling Party Transformation Mask** field is blank, and **Use Calling Party's External Phone Number Mask** is set to **Off** or **Default**, no calling party transformation takes place.
Calling Party Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Party Number Type	Choose the format for the number type in calling party directory numbers. Unified CM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non national type numbering plan. Choose one of the following options: • **Cisco CallManager** - Use when the Unified CM sets the directory number type. • **Unknown** - Use when the dialing plan is unknown. • **National** - Use when you are dialing within the dialing plan for your country. • **International** - Use when you are dialing outside the dialing plan for your country. • **Subscriber** - Use when you are dialling a subscriber by using a shortened subscriber number.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Field	Description
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Unified CM sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • **Cisco CallManager** - Use when the Unified CM sets the Numbering Plan in the directory number. • **ISDN** - Use when you are dialing outside the dialing plan for your country. • **National Standard** - Use when you are dialing within the dialing plan for your country. • **Private** - Use when you are dialing within a private network. • **Unknown** - Use when the dialing plan is unknown.
Called Party Discard Digits	Choose the discard digit instructions that you want to be associated with this called party transformation pattern.
Called Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Called Party Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#),the international escape character +, and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device.
Called Party Number Type	Choose the format for the number type in called party directory numbers. Unified CM sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • **Cisco CallManager** - Use when the Unified CM sets the directory number type. • **Unknown** - Use when the dialing plan is unknown. • **National** - Use when you are dialing within the dialing plan for your country. • **International** - Use when you are dialing outside the dialing plan for your country. • **Subscriber** - Use when you are dialling a subscriber by using a shortened subscriber number.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Field	Description
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Unified CM sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • **Cisco CallManager** - Use when the Unified CM sets the Numbering Plan in the directory number. • **ISDN** - Use when you are dialing outside the dialing plan for your country. • **National Standard** - Use when you are dialing within the dialing plan for your country. • **Private** - Use when you are dialing within a private network. • **Unknown** - Use when the dialing plan is unknown.

2.26. Configure Date Time Groups

2.26.1. How to Configure Date Time Groups

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

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

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

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to a customer or site level.
3. If prompted, select the NDL that contains the Cisco Unified CM on which you are configuring the Date Time Group.
4. Perform one of the following:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Date Time Groups**.
   - If you logged in as a customer administrator, choose **Device Management > Advanced > Date Time Groups**.
5. Click **Add**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

6. Provide the following information:

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

7. Click **Save**.

2.27. Configure Locations

2.27.1. How to Configure Locations

Introduction

Use locations 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 from Sites. Locations are used by Cisco Unified CM to manage call admission control. Sites are used by VOSS-4-UC to logically group resources.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to a customer or site level.
3. If prompted, select the NDL that contains the Cisco Unified CM on which you are configuring the Location.
4. Perform one of the following:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Locations**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > Locations**.
5. Click **Add**.
6. On the **Location Information** tab, enter the **Name** of the Location. This field is mandatory.
7. Click the **Intra-Location** tab, and complete at minimum, the mandatory *Intra-Location Fields*.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

8. Click the **Between Locations** tab, and complete at minimum, the mandatory *Between Locations Fields*.
9. Click the **RSVP Settings** tab, and complete at minimum, the mandatory *RSVP Settings Fields*.
10. Click **Save**.

Intra-Location Fields

Field	Description
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Valid values are 0 to 2147483647, where 0 means unlimited bandwidth. This field is mandatory. Note: To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on this link.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Valid values are 1 Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. Setting the value to 1 means you cannot make video calls within this location. This field is mandatory.
Immersive Video Bandwidth	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Valid values are 1 through 2147483647, where 0 means unlimited bandwidth and 1 means no bandwidth. Setting the value to 1 means you cannot make immersive video calls within this location. This field is mandatory.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Between Locations Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

RSVP Settings Fields

Field	Description
Location	To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane. This field is mandatory.
RSVP Setting	To choose an RSVP policy setting between the current location and the location that is chosen in the Location pane at left, choose an RSVP setting from the drop-down list. This field is mandatory. Choose from the following available settings: • **Use System Default** - The RSVP policy for the location pair matches the clusterwide RSVP policy. See topics related to clusterwide default RSVP policy in the Cisco Unified Communications Manager System Guide for details: – **No Reservation** - No RSVP reservations can get made between any two locations. – **Optional (Video Desired)** - A call can proceed as a best-effort audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified Communications Manager if reservation succeeds. – **Mandatory** - Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream too. – **Mandatory (Video Desired)** - A video call can proceed as an audio-only call if a reservation for the video stream cannot be reserved.

2.28. Configure Device Pools

2.28.1. How to Configure Device Pools

Introduction

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, CTI route points, and so on.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Perform one of these options:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Device Pools**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > CUCM > Device Pools**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3. Perform one of these options:
   - To add a new device pool, click **Add**, then go to step 5.
   - To edit an existing device pool, click the line item in the table. Go to step 5.
4. In the popup, choose from the drop-down the network device list (NDL) to which you are adding the device pool, and click **OK**.

   Note:

   The NDL popup only appears when you add a new device pool instance. If you are updating an existing instance, go to Step 5.

   If you are adding the instance to a Site hierarchy node, the NDL popup does not appear. You go right to the Add Device Pool form using the NDL associated to the site.
5. From the **Device Pool Settings** tab, complete at minimum, the mandatory *Device Pool Settings Fields*.
6. From the **Local Route Group Settings** tab, complete at minimum, the mandatory *Local Route Group Settings Fields*.
7. From the **Roaming Sensitive Settings** tab, complete at minimum, the mandatory *Roaming Sensitive Settings Fields*.
8. From the **Device Mobility Related Information** tab, complete the required *Device Mobility Related Information Fields*.
9. From the **Geolocation Configuration** tab, complete the required *Geolocation Configuration Fields*.
10. From the **Incoming Calling Party Settings** tab, complete the required *Incoming Calling Party Settings Fields*.
11. From the **Incoming Called Party Settings** tab, complete the required *Incoming Called Party Settings Fields*.
12. From the **Caller ID for Calls from This Phone** tab, complete the required *Caller ID For Calls From This Phone Fields*.
13. From the **Connected Party Settings** tab, complete the required *Connected Party Settings Fields*.
14. From the **Redirecting Party Settings** tab, complete the required *Redirecting Party Settings Fields*.
15. Click **Save**.

    The route partition appears in the device pool list.

    To modify any of these characteristics, make your changes and click **Save**.

    To delete a device pool, select the check box to the left of the **Name** column in the group list, and click **Delete**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.28.2. Device Pool Settings Fields

Option	Description
Device Pool Name *	Enter the name of the new device pool that you are creating. You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces. Default value: None
Cisco Unified CM Group *	Choose the Cisco Unified Communications Manager group to assign to devices in this device pool. A Unified CM group specifies a prioritized list of up to three Unified CMs. The first Unified CM in the list serves as the primary one for that group. The other members of the group serve as backup Unified CMs for redundancy.
Calling Search Space for Auto-registration	Choose the calling search space to assign to devices in this device pool that auto-register with Unified CM. The calling search space specifies partitions that devices can search when attempting to complete a call.
Adjunct CSS	From the drop-down list, choose an existing Calling Search Space (CSS) to use for the devices in this device profile as an adjunct CSS for the Extension Mobility Cross Cluster (EMCC) feature. To configure a new CSS or modify an existing CSS, choose **Call Routing > Class of Control > Calling Search Space** in Unified CM Administration. When configuring the EMCC feature, the administrator must configure a device pool for each remote cluster. If the remote cluster is located in a different country, the adjunct CSS must embrace the partition with which the emergency patterns of that country associate. This configuration facilitates country-specific emergency call routing. Default value: None
Reverted Call Focus Priority	Choose a clusterwide priority setting for reverted calls that the hold reversion feature invokes. This setting specifies which call type, incoming calls or reverted calls, have priority for user actions, such as going off hook. • **Default**-If you choose this option, incoming calls have priority. • **Highest**-If you choose this option, reverted calls have priority. The **Not Selected** setting specifies the reverted call focus priority setting for the default device pool at installation. At installation, incoming calls have priority. You cannot choose this setting in Unified CM. Note: This setting applies specifically to hold reverted calls; it does not apply to parked reverted calls.
Intercompany Media Services Enrolled Group	Choose an **Intercompany Media Services Enrolled Group** from the drop-down list.

2.28.3. Local Route Group Settings Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.28.4. Roaming Sensitive Settings Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
SRST Reference *	From the drop-down list, choose a survivable remote site telephony (SRST) reference to assign to devices in this device pool. Choose from these options: • **Disable** - When you choose this option, devices in this device pool do not have SRST reference gateways that are available to them. • **Use Default Gateway** - When you choose this option, devices in this device pool use the default gateway for SRST. • **Existing SRST references** - When you choose an SRST reference from the drop-down list, devices in this device pool use this SRST reference gateway. Default value: None
Connection Monitor Duration	This setting defines the time that the Cisco Unified IP Phone monitors its connection to Unified CM before it unregisters from SRST and reregisters to Unified CM. To use the configuration for the enterprise parameter, you can enter “1” or leave the field blank. The default value for the enterprise parameter equals 120 seconds. Tip: When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter.
Single Button Barge	This setting determines whether the devices or phone users in this device pool have single-button access for barge and cBarge. From the drop-down list, choose from these options: • **Off** - When you choose this option, the devices in this device pool have the Single Button Barge/cBarge feature disabled. • **Barge** - When you choose this option, the devices in this device pool have the Single Button Barge feature enabled. • **CBarge** - When you choose this option, the devices in this device pool have the Single Button cBarge feature enabled. • **Default** - When you choose this option, the devices in this device pool use the service parameter setting for the Single Button Barge/cBarge feature. Default value: Default
Join Access Lines	This setting determines whether the Join Access Lines feature is enabled for the devices or phone users in this device pool. From the drop-down list, choose from these options: • **Off** - When you choose this option, the devices in this device pool have the Join Access Lines feature disabled. • **On** - When you choose this option, the devices in this device pool have the Join Access Lines feature enabled. • **Default** - When you choose this option, the devices in this device pool use the service parameter setting for the Join Access Lines feature. Default value: Default
Physical Location	Select the physical location for this device pool. The system uses physical location with the device mobility feature to identify the parameters that relate to a specific geographical location. Default value: None

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

2.28.5. Device Mobility Related Information Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.28.6. Geolocation Configuration Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.28.7. Incoming Calling Party Settings Fields

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.28.8. Incoming Called Party Settings Fields

Option	Description
National Prefix	Unified CM applies the prefix that you enter in this field to calling party numbers that use **National** for the Called Party Numbering Type. You can enter up to sixteen (16) characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Gateway** or **Trunk Configuration** window, you cannot configure the **Strip Digits** field in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the **Device Pool Configuration** window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix** field. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
National Strip Digits	Enter the number of digits, that you want Unified CM to strip from the called party number of “Unknown” type before it applies the prefixes.
National Calling Search Space	This setting allows you to transform the called party number of “Unknown” called party number type on the device. If you choose **None**, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
International Prefix	Unified CM applies the prefix that you enter in this field to called party numbers that use **National** for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Prefix** field in the Gateway or Trunk Configuration window, you cannot configure the **Strip Digits** field in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix** field. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
International Strip Digits	Enter the number of digits that you want Unified CM to strip from the called party number of International type before it applies the prefixes.
International Calling Search Space	This setting allows you to transform the called party number of International called party number type on the device. If you choose **None**, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Unknown Prefix	Unified CM applies the prefix that you enter in this field to called numbers that use **Unknown** for the Called Party Numbering Type. You can enter up to sixteen characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Prefix** in the Gateway or Trunk window, you cannot configure the **Strip Digits** in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix field**. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
Unknown Strip Digits	Enter the number of digits, that you want Unified CM to strip from the called party number of “Unknown” type before it applies the prefixes.
Unknown Calling Search Space	This setting allows you to transform the called party number of “Unknown” called party number type on the device. If you choose **None** no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Subscriber Prefix	Unified CM applies the prefix that you enter in this field to called numbers that use **Subscriber** for the Called Party Numbering Type. You can enter up to sixteen characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word “Default” instead of entering a prefix. Tip: If the word “Default” displays in the **Prefix** field in the Gateway or Trunk Configuration window, you cannot configure the **Strip Digits** field in the Gateway or Trunk Configuration window. In this case, Unified CM takes the configuration for the **Prefix** and **Strip Digits** fields from the device pool that is applied to the device. If the word “Default” displays in the **Prefix** field in the Device Pool Configuration window, Unified CM applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. Tip: To configure the **Strip Digits** field, leave the **Prefix** field blank or enter a valid configuration in the **Prefix** field. To configure the **Strip Digits** fields, do not enter the word “Default” in the **Prefix** field.
Subscriber Strip Digits	Enter the number of digits, that you want Unified CM to strip from the called party number of Subscriber type before it applies the prefixes.
Subscriber Calling Search Space	This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose **None**, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.28.9. Caller ID For Calls From This Phone Fields

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

2.28.10. Connected Party Settings Fields

Option	Description
Connected Party Transformation CSS	This setting is applicable for inbound calls only. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Unified CM includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages for SIP calls and in the Connected Number Information Element of CONNECT and NOTIFY messages for H.323 and MGCP calls. Make sure that the Connected Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. Note: If you configure the Connected Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.

2.28.11. Redirecting Party Settings Fields

Option	Description
Redirecting Party Transformation CSS	This setting allows you to transform the redirecting party number on the device to E164 format. Unified CM includes the transformed number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) sent out of Unified CM. Make sure that the Redirecting Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. that the Connected Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. Note: If you configure the Redirecting Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.29. Associate Local Route Groups to a Device Pool

2.29.1. How to Associate Local Route Groups to a Device Pool

Use this procedure to associate 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. You cannot use this procedure to add or delete device pools.

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). The Local Route Group feature enables 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.

Procedure

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. Perform one of the following:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Device Pools**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > Device Pools**.
3. Click the device pool to be associated.
4. From the **Cisco Unified CM Group** drop-down menu, select a specific Cisco Unified Communications Manager group or leave the Cisco Unified CM Group as Default.
5. Click the **Local Route Group Settings** tab.
6. In the grid, from the **Local Route Group** drop-down menu, select the local route group.
7. In the grid, from the **Route Group** drop-down menu, select the route group or gateway.
8. To save the new local route association, click **Save**.

2.30. Provision Emergency Calls

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.30.1. How to Provision Emergency Calls

There is no additional provisioning that is necessary for emergency calls. In VOSS-4-UC, 911 is provisioned 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”.

Procedure

1. When you Create 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”.

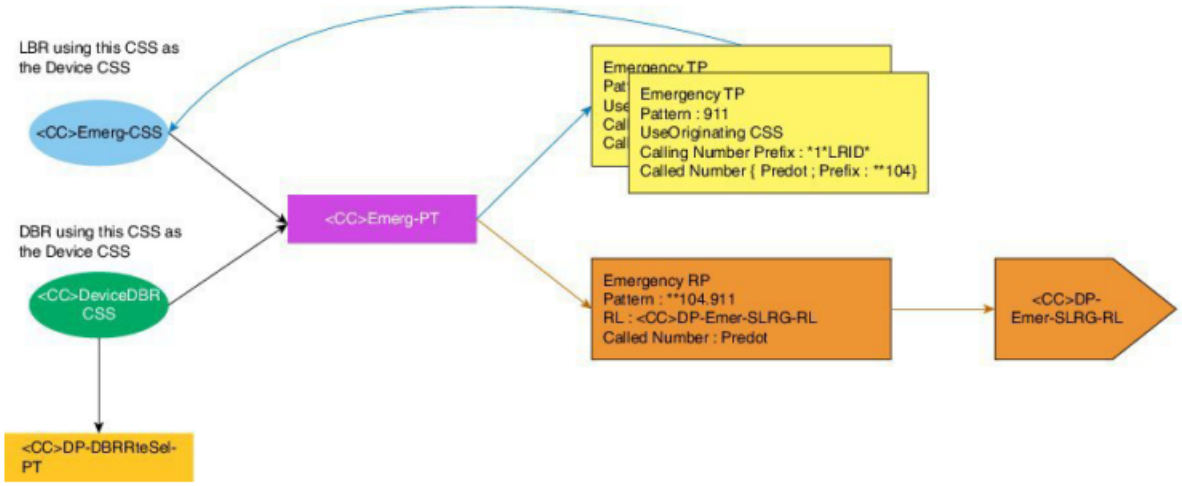
2.30.2. Emergency Handling

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.

Emergency Calling



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.31. Configure Cisco Unified Communications Manager Groups

2.31.1. Configure Cisco Unified Communications Manager Groups

In VOSS-4-UC 10.x/11.5(x), use Cisco Unified CM Groups to configure Cisco Unified Communications Manager groups.

A Cisco Unified Communications Manager group specifies a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as secondary and tertiary (backup) Cisco Unified Communications Managers.

Each device pool has one Cisco Unified Communications Manager group that is assigned to it. When a device registers, it attempts to connect to the primary (first) Cisco Unified Communications Manager in the group that is assigned to its device pool. If the primary Cisco Unified Communications Manager is not available, the device tries to connect to the next Cisco Unified Communications Manager that is listed in the group, and so on.

Cisco Unified Communications Manager groups provide important features for your system:

- Redundancy - This feature enables you to designate a primary and backup Cisco Unified Communications Managers for each group.
- Call processing load balancing - This feature enables you to distribute the control of devices across multiple Cisco Unified Communications Managers.

For most systems, you need to have multiple groups, and you need to assign a single Cisco Unified Communications Manager to multiple groups to achieve better load distribution and redundancy.

Cisco Unified Communications Manager group configuration considerations

Before configuring a Cisco Unified Communications Manager group, you must configure the Cisco Unified Communications Managers that you want to assign as members of that group.

After you have configured the Cisco Unified Communications Manager group, you can use it to configure device pools. Devices obtain their Cisco Unified Communications Manager group list setting from the device pool to which they are assigned.

1. Sign in as the provider, reseller, or customer administrator.

   Note: For Shared Architecture deployment, you must sign in only as a provider or reseller admin so that only provider or reseller admins can add Unified CM.

2. If you are adding a new instance, ensure the hierarchy path is set to the target node for the new instance.
3. Perform one of the following:
   - If you signed in as the provider or reseller administrator, select **Device Management > CUCM > Unified CM Groups**.
   - If you signed in as the customer administrator, select **Device Management > Advanced > Unified CM Groups**.
4. Perform one of the following:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- To add a new Cisco Unified Communications Manager group, click **Add**, then go to step 5.

  To edit an existing Cisco Unified Communications Manager group, click on the line item in the list of existing instances. Go to step 5.

5. Modify the following fields as required.

Option	Description
Name (Mandatory)	Enter the name of the new group.
Auto-registration Cisco Unified Communications Manager Group	Check the Auto-registration Cisco Unified Communications Manager Group check box if you want this Cisco Unified Communications Manager group to be the default Cisco Unified Communications Manager group when auto-registration is enabled. Leave this check box unchecked if you do not want devices to auto-register with this Cisco Unified Communications Manager group. Tip Each Cisco Unified Communications Manager cluster can have only one default auto-registration group. If you choose a different Cisco Unified Communications Manager group as the default auto-registration group, that is, you check the Auto-registration Cisco Unified Unified Communications Manager Group check box for a different Cisco Unified Communications Manager group, the previously chosen auto-registration group no longer serves as the default for the cluster; the Auto-registration Cisco Unified Communications Manager check box displays for the previously chosen group (the original default), and the check box gets disabled for the group that now serves as the default.
Unified CM Group Items (Mandatory)	Click **Add (+)** to select a Cisco Unified Communications Manager to add to the group. Repeat as necessary to add multiple Cisco Unified Communications Managers to the group. Click the **Remove (-)** button to remove a Cisco Unified Communications Manager from the group. Click the up and down arrow buttons to change the order of the Cisco Unified Communications Managers in the group.
Priority (Mandatory)	Enter the priority number for this Cisco Unified Communications Manager in the group. The smaller the integer, the higher the priority.
Selected Cisco Unified Communications Managers	This field displays the Cisco Unified Communications Managers that are in the Cisco Unified Communications Manager group.

6. Click **Save**.

   The group appears in the Call Manager Groups list. When you click on the name of the Cisco Unified Communications Manager group in the list, the group's characteristics are displayed.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

To modify any of these characteristics, make your changes and click **Save**.

To delete a group, check the box to the left of the Name column in the group list, and click **Delete**.

Note: Verify if the Unified CM is deployed in Shared Mode. Sign in to the Unified CDM, and navigate to **Device Management > CUCM > Servers**. On the Publisher tab, verify the Multi-Tenant field is set to Shared.

2.32. Configure Route Partitions

2.32.1. Configure Route Partitions

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.

Partitions configuration tips

Note: Timesaver

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.

If you are updating a partition, use the Apply Config button as described in the 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. Perform one of the following:
   - If you signed in as the provider or reseller administrator, select **Device Management > CUCM > Route Partitions**.
   - If you signed in as the customer administrator, select **Device Management > Advanced > Route Partitions**.
3. Make sure that the hierarchy path is set to the correct level.
4. Perform one of the following:
   - 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 characteristics, click the item in the list, make your changes, and click **Save**.

To delete a route partition, check the box to the left of the Name column in the group list, and click **Delete**.

2.33. Configure Calling Search Spaces

2.33.1. Configure Calling Search Spaces

A calling search space 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.

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Perform one of the following:
   - If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > Calling Search Spaces**.
   - If you logged in as the Customer Administrator, select **Device Management > Advanced > Calling Search Spaces**.
3. Make sure that the hierarchy path is set to the correct level.
4. Perform one of the following:
   - 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 characteristics, click the item in the list, make your changes, and click **Save**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

To delete a calling search space, check the box to the left of the Name column in the group list, and click **Delete**.

2.34. Configure Calling Party Transformation Patterns

2.34.1. Configure Calling Party Transformation Patterns

The parameters in the Calling Party Transformation Patterns window 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.

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Perform one of the following:
   - If you logged in as the Provider or Reseller Administrator, select# **Device Management > CUCM > Calling Party Transformation Patterns**.
   - If you logged in as the Customer Administrator, select **Device Management > Advanced > Calling Party Transformation Patterns**.
3. Make sure that the hierarchy path is set to the correct level.
4. Perform one of the following:
   - To add a new calling party transformation pattern, click **Add**, then go to step 5.
   - To edit an existing calling party transformation pattern, click on the line item in the table. Go to step 6.
5. In the popup, select from the drop-down the network device list (NDL) to which you are adding the calling party transformation pattern, and click **OK**.

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

   If you are adding the calling party transformation pattern to a Site hierarchy node, the NDL popup will not appear. You will go right to the Calling Party Transformation Pattern add tabs using the NDL associated to the site.
6. From the **Pattern Definition** tab, modify the following fields as required.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Calling Party Number Type	Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non national type numbering plan. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a subscriber by using a shortened subscriber number.
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

To modify any of these characteristics, click the item in the list, make your changes, and click **Save**.

To delete a calling party transformation pattern, check the box to the left of the Name column in the group list, and click **Delete**.

2.35. Configure Called Party Transformation Patterns

2.35.1. Configure Called Party Transformation Patterns

The parameters in the Called Party Transformation Patterns window 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.

1. Log in as the Provider, Reseller, or Customer Administrator.
2. Perform one of the following:
   - If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > Called Party Transformation Patterns**.
   - If you logged in as the Customer Administrator, select **Device Management > Advanced > Called Party Transformation Patterns**.
3. Make sure that the hierarchy path is set to the correct level.
4. Perform one of the following:
   - To add a new called party transformation pattern, click **Add**, then go to step 5.
   - To edit an existing called party transformation pattern, click on the line item in the table. Go to step 6.
5. In the popup, select from the drop-down the network device list (NDL) to which you are adding the called party transformation pattern, and click **OK**.

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

   If you are adding the called party transformation pattern to a Site hierarchy node, the NDL popup will not appear. You will go right to the Called Party Transformation Pattern add tabs using the NDL associated to the site.
6. From the Pattern Definition tab, modify the following fields as required.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Digit Discards	Choose the discard digit instructions that you want to be associated with this called party transformation pattern.
Called Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Prefix Digits	Enter prefix digits in the field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#),the international escape character +, and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a subscriber by using a shortened subscriber number.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco CallManager - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN - Use when you are dialing outside the dialing plan for your country. • National Standard - Use when you are dialing within the dialing plan for your country. • Private - Use when you are dialing within a private network. • Unknown - Use when the dialing plan is unknown.

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

To modify any of these characteristics, click the item in the list, make your changes, and click **Save**.

To delete a called party transformation pattern, check the box to the left of the Name column in the group list, and click **Delete**.

2.36. Configure CTI Route Points

2.36.1. How to Configure CTI Route Points

Introduction

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

Procedure

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.

   If the hierarchy path is not set to a site, you are prompted to choose a site.
3. Perform one of the following:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- If you logged in as provider or reseller administrator, choose **Device Management > CUCM > CTI Route Points**.
- If you logged in as customer administrator, choose **Device Management > Advanced > CTI Route Points**.

4. Click **Add**.
5. Complete at minimum, the mandatory *CTI Route Points Fields*.
6. Click + next to **Line**, to associate a line with the CTI Route Point. Complete, at minimum, the mandatory *CTI Route Points Line Fields*.
7. Click **Save**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.36.2. CTI Route Points Fields

Option	Description
Device Name *	Enter a unique identifier for this device, from 1 to 15 characters, including alphanumeric, dot, dash, or underscores. This field is mandatory.
Description	Enter a descriptive name for the CTI route point. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool *	Choose the name of a Device Pool. The device pool specifies the collection of properties for this device, including Cisco Unified Communications Manager Group, Date Time Group, Region, and Calling Search Space for autoregistration. This field is mandatory.
Common Device Configuration	Choose the common device configuration to which you want this CTI route point assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure common device configurations in the Common Device Configuration window.
Calling Search Space	From the drop-down list, choose a calling search space. The calling search space specifies the collection of partitions that are searched to determine how a collected (originating) number is routed.
Location *	From the drop-down list, choose the appropriate location for this CTI route point. This field is mandatory. Locations implement call admission control (CAC) in a centralized call-processing system. CAC regulates audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls between locations. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of Hub_None means that the locations feature does not track the bandwidth that this CTI route point consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.
User Locale	From the drop-down list, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font. Note: If no user locale is specified, Cisco Unified CM uses the user locale that is associated with the device pool
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List is a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources. The application chooses according to the priority order defined in a Media Resource Group List. If you choose <none>, Cisco Unified CM uses the Media Resource Group that is defined in the device pool.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Option	Description
Network Hold MOH Audio Source	Choose the audio source that plays when the network starts a hold action. If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool. If the device pool does not specify an audio source, the system default is used.
User Hold MOH Audio Source	Choose the audio source that plays when an application starts a hold action. If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool. If the device pool does not specify an audio source, the system default is used.
Use Trusted Relay Point Required Field *	Enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. This field is mandatory. Choose one of the following values: • **Default** - If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • **Off** - Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **On** - Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Tip: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, select this check box. If you do not select this check box, the device uses the Calling Party Transformation CSS that you configured in the CTI Route Point Configuration window.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

2.36.3. CTI Route Points Line Fields

Field	Description
Directory Number *	Enter a dialable phone number. Values can include route pattern wildcards and numeric characters (0 to 9). Special characters such as a question mark (?), exclamation mark (!), backslash (\), brackets ([ ]), plus sign (+), dash (-), asterisk (*), caret (^), pound sign (#), and an X are also allowable. Special characters that are not allowed are a period (.), at sign (@), dollar sign ($), and percent sign (%). This field is mandatory. At the beginning of the pattern, enter \+ if you want to use the international escape character +. For this field, \+ does not represent a wildcard; instead, entering \+ represents a dialable digit.
Route Partition *	Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the Directory Number field is unique within the partition that you choose. If you do not want to restrict access to the directory number, choose <None> for the partition.
Index	This field is the line position on the device. If left blank, an integer is automatically assigned.
External Phone Number Mask	Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number, the international escape character +, and “X” characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.
Line Text Label	Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line and phone combination. Suggested entries include boss name, department name, or other appropriate information to identify multiple directory numbers to a secretary or assistant who monitors multiple directory numbers.
Display (Internal Caller ID)	Leave this field blank to have the system display the extension. Use a maximum of 30 characters. Typically, use the username or the directory number. If using the directory number, the person receiving the call may not see the proper identity of the caller.
ASCII Display (Caller ID)	This field provides the same information as the Display (Internal Caller ID) field, but limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the ASCII Display (Internal Caller ID) field.
Ring Setting (Phone Active)	If applicable, the ring setting that is used when this phone has another active call on a different line. Choose one of the following options: • **Use system default** • **Disable** • **Flash only** • **Ring once** • **Ring** • **Beep only**

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Field	Description
Ring Setting (Phone Idle)	If applicable, the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Choose one of the following options: • **Use system default** • **Disable** • **Flash only** • **Ring once** • **Ring**
Recording Option	This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled. Choose one of the following options: • **Call Recording Disabled** - Calls made on this line appearance cannot be recorded. • **Automatic Call Recording Enabled** - Calls made on this line appearance are recorded automatically. • **Selective Call Recording Enabled** - Calls made on this line appearance can be recorded using a softkey or programmable line key that is: – assigned to the device – a CTI-enabled application – both interchangeably
Recording Profile	This field determines the recording profile on the line appearance of an agent.
Recording Media Source	This field determines the recording media source option on the line appearance. Choose one of the following options: • **Gateway Preferred** - Voice gateway is selected as the recording media source when the call is routed through a recording enabled gateway. • **Phone Preferred** - Phone is selected as the recording media source.
Monitoring Calling Search Space	The monitoring calling search space of the supervisor line appearance must include the agent line or device partition to allow monitoring the agent.
Visual Message Waiting Indicator Policy	Use this field to configure the handset lamp illumination policy. Choose one of the following options: • **Use System Policy** (The directory number refers to the service parameter “Message Waiting Lamp Policy” setting.) • **Light and Prompt** • **Prompt Only** • **Light Only** • **None**
Audible Message Waiting Indicator Policy	Use this field to configure an audible message waiting indicator policy. Choose one of the following options: • **Off** • **On** - When you select this option, you receive a stutter dial tone when you take the handset off hook. • **Default** - When you select this option, the phone uses the default that was set at the system level.
Log Missed Calls	If selected, Cisco Unified CM logs missed calls in the call history for the shared line appearance on the phone.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

2.37. Configure Time Periods and Schedules

2.37.1. Configure Time Periods

A time period specifies a time range that includes a start time and end time. Time periods also specify a repetition interval either as days of the week or a specified date on the yearly calendar. You define time periods and then associate the time periods with time schedules. A particular time period can be associated with multiple time schedules.

Note: VOSS-4-UC provides one **All the time** time period. The **All the time** period is a special, default time period that includes all days and hours, and cannot be deleted.

---

1. Sign in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to the node where you want to configure the new time period.
3. Perform one of these options as appropriate:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Time Periods**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > Time Periods**.
4. Perform one of these options as appropriate:
   - To add a new time period, click **Add**, then go to Step 5.
   - To edit an existing time period, choose the time period to be updated by clicking it in the list of time periods, then go to Step 6.
5. If the **Network Device List** popup window appears, choose the NDL for the time period from the drop-down menu. The window appears when you are on a nonsite hierarchy node. If you are at a site hierarchy node, the NDL associated with the site is automatically used.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Note:

The **Network Device List** drop-down menu only appears when a time period is added; it does not appear when you edit a time period.

6. Enter a unique name for the new time period in the **Name** field, or modify the existing Name if desired. This field is mandatory. Enter a name in the **Time Period Name** field. The name can comprise up to 50 alphanumeric characters. It can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

   Use concise and descriptive names for your time periods. The hours_or_days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, office_M_to_F identifies a time period for the business hours of an office from Monday to Friday.

7. Complete the other fields as appropriate.

Option	Description
Description	Enter a description for the time period.
Time of Day Start	From the drop-down list, choose the time when this time period starts. The available listed start times comprise 15-minute intervals throughout a 24-hour day. Default: No Office Hours Note: To start a time period at midnight, choose the 00:00 value.
Time of Day End	From the drop-down list, choose the time when this time period ends. The available listed end times comprise 15-minute intervals throughout a 24-hour day. Default: No Office Hours Note: To end a time period at midnight, choose the 24:00 value.

8. Choose one of these repetition periods and complete the required information:

   Note:

   If you choose to repeat the time period by the week, the **Repeat Every Year** fields are dimmed and cannot be edited. If you choose to repeat the time period by the year, the **Repeat Every Week** fields are dimmed and cannot be edited.

   Repeat Every Week - For time periods defined by the week

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

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

   Repeat Every Year - For time periods defined by the year

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

   b. Enter a number from 1 to 31 in the **Start Date** field to define the day of the month on which this time period starts.

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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. To save the new or updated time period, click **Save**.

Associate time periods with time schedules. See “Configure Time Schedules”.

Note:

You cannot delete time periods that time schedules are using. 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.

2.37.2. Configure Time Schedules

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.

Once you have configured a time period in **Configure Time Periods**, perform this procedure to assign the time period to a time schedule.

Note: VOSS-4-UC 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.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy path is set to the node where you want to create the new time schedule.
3. Perform one of the following:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Time Schedules**.
   - If you logged in as a customer administrator, choose **Device Management > Advanced > Time Schedules**.
4. Perform one of the following:
   - To add a new time schedule, click **Add**, then go to Step 5.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- To edit an existing time schedule, choose the time schedule to be updated by clicking it in the list of time schedules. Go to Step 6.

5. If the **Network Device List** popup window appears, select the NDL for the time schedule from the drop-down menu. The window appears when you are on a nonsite hierarchy node. If you are at a site hierarchy node, the NDL associated with the site is automatically used.

   Note:

   The **Network Device List** drop-down only appears when a time schedule is added; it does not appear when you edit a time schedule.

6. Enter a unique name for the new time schedule in the **Name** field, or modify the existing Name if desired. This field is mandatory. The name can comprise up to 50 alphanumeric characters. The name of the time schedule can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
7. (Optional) Enter a description for the time schedule in the **Description** field.
8. Click + to open the **Time Periods** form.
9. From the **Time Period** drop-down box, choose a time period for the time schedule.
10. Repeat Steps 8 and 9 to add another time period to the time schedule.

    Note:

    - If multiple time periods are associated with a schedule where the time periods overlap, time periods with Day of Year settings take precedence over time periods with Day of Week settings. Day of Year is applicable when Year Start value is set and the End value is left blank.

      Example: If a Time Period configured for January 1 is configured as No Office Hours and another time period is configured for the same day of the week (for example, Sunday to Saturday) as 08:00 to 17:00, the time period for January 1 is used. In this example, No Office Hours takes precedence.

    - Time interval settings take precedence over No Office Hour settings for the same day of the year or day of the week.

      Example: One time period specifies for Saturday as No Office Hours. Another time period specifies Saturday hours of 08:00 to 12:00. In this example, the resulting time interval specifies 08:00 to 12:00 for Saturday.

    - If multiple time periods are associated with a schedule where the time periods overlap, time periods with Day of Week settings take precedence over time periods with Range of Days settings. Range of Days applies to when Year Start and End values are set, even if they are configured for the same day.

      Example: If a Time Period configured for Day of Week (for example, Sunday to Saturday) is configured as No Office Hours and another time period is configured for January 1 until December 31 as 08:00 to 17:00, the time period for Day of Week is used. In this example, No Office Hours takes precedence.

11. To save the new time schedule, click **Save**. To save the updated time schedule, click **Update**.
12. Repeat Steps 3 to 11 to configure another time schedule.

What to Do Next

You cannot delete time schedules that partitions are using. Before deleting a time schedule that is currently in use, perform either or both of the following tasks:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- Assign a different time schedule to any partitions that are using the time schedule that you want to delete.
- Delete the partitions that are using the time schedule that you want to delete.

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

2.38. Clone an Instance of a Cisco Unified CM Device Model

2.38.1. Clone an Instance of a Cisco Unified CM Device Model

To save time, make a copy of an existing instance of a device model rather than adding a new one. To do this, use the clone operation. When you create a clone, give it a new unique name and modify other device model fields as needed before saving.

Note: You can clone an instance of a device model to the same Cisco Unified CM or to a different Cisco Unified CM.

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

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Do one of the following:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > {device_model_type}**.
   - If you logged in as customer administrator, choose **Device Management > Advanced > {device_model_type}**.
3. From the device model list, click the instance to be cloned.
4. Click **Action > Clone**.
5. Depending on the device model, do one of the following:
   - When prompted, choose the NDL that contains the target Cisco Unified CM.
   - choose the target Cisco Unified CM from the **CUCM** drop-down menu.
6. Enter a unique name for the new instance of the device model in the **Name** field.
7. Modify other fields as required.

   For more detailed information about the fields, see the corresponding topic on configuring a new instance of the device model. For example, if you are cloning a SIP trunk, see under *How to Configure SIP Trunks* for the SIP trunk field descriptions.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

8. Click **Save** to save the cloned instance.

The new instance appears in the list. The new instance is created on the target Cisco Unified CM.

2.39. Load Balancing

2.39.1. Load Balancing: Overview

Cisco Unified Communications Manager (Unified CM) groups provide both call-processing redundancy and distributed call processing. You can distribute devices, device pools, and Unified CMs among the groups to improve redundancy and load balancing in your system.

A Cisco Unified Communications Manager Group specifies a prioritized list of up to three Unified CMs. The first Unified CM in the list serves as the primary Unified CM for that group, and the other members of the group serve as secondary and tertiary (backup) Unified CMs.

Each device pool has one Unified CM 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) Unified CM in the group that is assigned to its device pool. If the primary Unified CM is not available, the device tries to connect to the next Unified CM that is listed in the group, and so on.

Load balancing is a manual process on Unified CM requiring you to perform the following tasks:

1. Add new, custom Unified CM groups and device pools.
2. Synchronize the groups and device pools into VOSS-4-UC.
3. Choose the appropriate group and device pool in the Subscriber or Phone configuration for the site. To create more than one configuration for a site, create at least two Unified CM groups, then associate a device pool to the appropriate Unified CM group.

To determine if load balancing is required for your network, you can check the current device traffic load in Unified CM using the System > Device Pool menu path. 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”.

2.39.2. Load Balancing Using Site Default Device Pool

A default device pool is created for each site when the site dial plan is deployed for the Type 1 through 4 dial plan schema groups. This procedure uses the default site device pools, so you do not need to create any additional device pools directly on Cisco Unified Communications Manager (Unified CM). Perform this procedure to load balance using the default site device pool. In this procedure, the default device pool is updated to point to the appropriate Cisco Unified Communications Manager group.

Note: 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 Cisco Unified Communications Managers, providing failover redundancy. Devices in different sites home to different sequences of Cisco Unified Communications Managers, providing load balancing across the sites.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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. You can determine the default device pool for a site in VOSS-4-UC by choosing **Site Management > Defaults**.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose the site from the hierarchy node breadcrumb at the top of the view in (VOSS-4-UC).
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 Cisco Unified Communications Manager groups on Cisco Unified Communications Manager. See Cisco Unified Communications Manager Administration Guide.
5. From VOSS-4-UC, perform a sync operation of the Cisco Unified Communications Manager using the **Administration Tools > Data Sync** menu path. This sync updates the VOSS-4-UC cache and makes the Cisco Unified Communications Manager groups that were added directly on Cisco Unified Communications Manager available to VOSS-4-UC.
6. Perform Associate Cisco Unified Communications Manager Group to a Device Pool, choose a Unified CM group other than the default group in the **Call Manager Group** drop-down list.

   Note:

   To verify that the phone or subscriber uses the device pool as expected, choose a subscriber from the list of subscribers in VOSS-4-UC (**Subscriber Management > Subscribers**) and choose the required **Device Pool Name** setting from the drop-down under the **Phones** tab.

2.39.3. Associate Cisco Unified Communications Manager Group to a Device Pool

Use this procedure to associate a Cisco Unified Communications Manager (Unified CM) 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 Unified CM group based on the call type. You cannot use this procedure to add or delete device pools.

Procedure

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

   Warning:

   When associating a Unified CM 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 Unified CM group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.
2. Perform one of the following:
   - If you logged in as provider or reseller administrator, choose **Device Management > CUCM > Device Pools**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- If you logged in as customer administrator, choose **Device Management > Advanced > Device Pools**.

3. Click the device pool to be associated.
4. From the **Unified CM Group** drop-down, choose a specific Unified CM group or leave the **Unified CM Group** as **Default**.
5. To save the new Unified CM group association, click **Save**.

2.40. Update the USA Device-Based Routing Dial Plan

2.40.1. Update the USA Device-Based Routing Dial Plan

Use this procedure if you deployed the United States country dial plan using VOSS-4-UC 10.1(1) and are 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. For example, if you performed this procedure when you upgraded to Unified CDM 10.6(1), do not perform it again when upgrading to a later release.

---

1. Log in to Cisco Unified Communications Manager.
2. Navigate 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**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7. After updating all calling search spaces, log in to Unified CDM and perform a Cisco Unified Communications Manager import operation:
    a. Log in to Unified CDM as provider or customer administrator.
    b. Navigate to **Device Management > Advanced > Perform Publisher Actions**.
    c. Select Action Import, App Type CUCM Device and select the appropriate Cisco Unified Communications Manager cluster.
    d. Click **Save**.

2.41. Sharing Lines Across Sites

2.41.1. Shared Line Across Sites

This feature allows lines to be shared across sites, and is accomplished by introducing the concept of an "Inventory site" in addition to the normal 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 not provisioned in the Inventory site; they are only provisioned on the real sites.

This 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. The lines used in Hunt Groups and Call Pickup Groups that are provisioned in the Inventory site can span multiple real sites (in other words, they are 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 *Shared Line Across Sites Example* is optional and is only required when sharing lines across sites.

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.

2.41.2. Definitions for Shared Line Across Sites

Many of the terms used for the Shared Line Across Sites feature have a number of different meanings depending on the context. To help remove some ambiguity in the procedures documented in this section, please review the following definitions in the context of the Shared Line Across Sites feature:

- **Directory Number (DN)** - This number can be assigned to a user and can be dialed. It may be composed of an extension prefix and/or a site location code and/or extension, but the DN is the final form of the internal dialable number. The DN is not the E.164 number, although they may coincide.
- **DN Inventory** - A list of DNs configured in VOSS-4-UC that can then be used in a line configuration. The DN inventory resides only in VOSS-4-UC and is not pushed to Cisco Unified Communications Manager. DNs may also be used as feature pilot numbers (for example, Hunt Pilot or Call Pickup patterns). When used as a service number, the DN is marked as unavailable and it cannot be used in

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

a line configuration. DN inventory is configured at the Site or Customer hierarchy level. However, to configure DN inventory at a customer hierarchy, the customer dial plan must be configured not to use site location codes (“flat dial plan”).

- **E.164 Number** - The globally routable phone number that includes country code and country-specific format. This number is used for offnet Public Switched Telephone Network (PSTN) calls.
- **E.164 Inventory** - A list of E.164 numbers configured at a site hierarchy. This list only resides in VOSS-4-UC and is not pushed to Cisco Unified Communications Manager.
- **Line or Line Relation** - The line configured from menu item **Subscriber Management > Lines** which is pushed to Cisco Unified Communications Manager. A line is also pushed to Cisco Unified Communications Manager when it is referenced in a phone, extension mobility profile, or single number reach profile and doesn’t already exists on the Cisco Unified Communications Manager. On Cisco Unified Communications Manager, a line corresponds with the items under **Call Routing > Directory Number**. It is also called a “line relation” because this is the technical term for the construct within VOSS-4-UC.
- **Line Appearance** - A line appearance is the assignment of a line to a phone. One line can have many line appearances. If a line has more than one line appearance, it is considered a shared line.
- **Class of Service (CoS)** - This term refers to a Calling Search Space (CSS) that is specifically used to define call routing and feature processing for a line or a phone. Refer to *Class of Service for Shared Line Across Sites* for more information.
- **SLC-based Dial Plan** - A site location code (SLC)-based dial plan is one that uses unique, site-specific dialable location codes that are embedded in the DN along with the extension. For example, the default Type 1 through Type 3 Cisco dial plans are SLC-based. Only the Type 4 dial plan is not SLC-based; Type 4 dial plan is commonly referred to as a “flat” dial plan because DNs are the actual extensions. This distinction between types of dial plans is important, because to support the Shared Line Across Sites feature, where devices at different sites can share a line that supports intra/intersite dialing from every site, an SLC would not allow a line to span multiple sites (because multiple sites can’t have the same SLC). The Shared Line Across Sites feature requires the customer to deploy a non-SLC based dial plan.
- **DNR** - Directory Number Routing allows an administrator to make their DN inventory inter- and intra-site routable by adding the necessary translation patterns on Cisco Unified Communications Manager when deploying a non-SLC-based dial plan. Normally, for the SLC-based dial plans, because each site requires a unique SLC, these translation patterns can automatically be deployed. This is not the case for non-SLC (flat) dial plans. In this case, DNR instances can be created when DN inventory is added to make these internally routable.
- **E.164 Associations** - Allow the customer’s DNs to be reachable from the PSTN network (DDI routing). The Administrator creates an E.164 (PSTN)-to-DN (internal extensions) association to provide the DDI mapping.

2.41.3. Shared Line Across Sites Example

Phones are always configured on the 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:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.
- **Subscribers** - configured from **Subscriber Management > Subscribers**, or **Subscriber Management > Quick Add Subscriber**.
- **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.

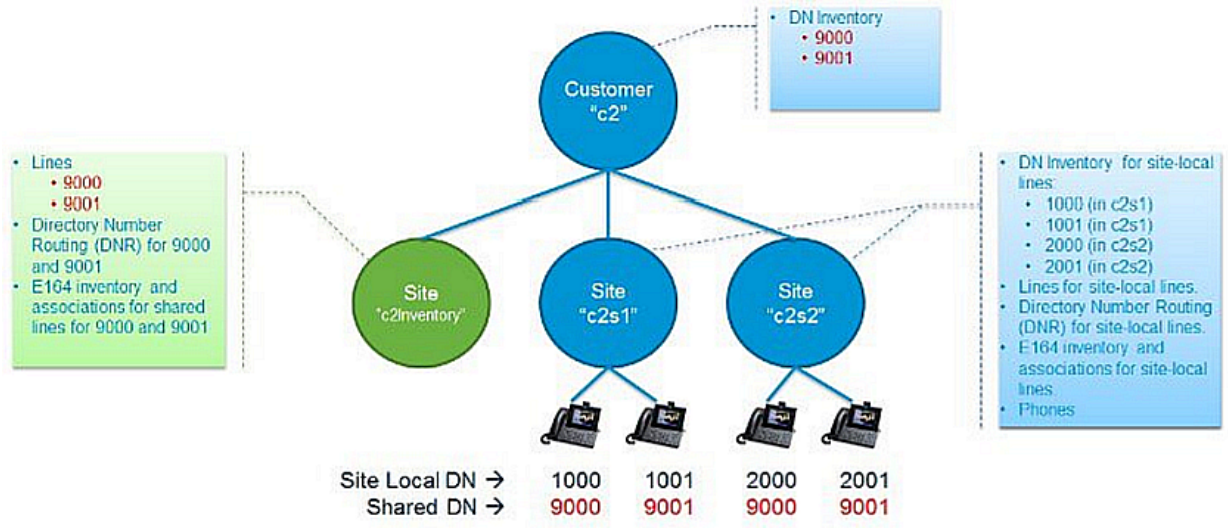
Fields in VOSS-4-UC which reference DNs, such as the **Pattern** field in the **Line** tab of a Phone, are in a drop-down list of DN inventory. The drop-down list of DNs includes inventory defined at the customer level, combined with the inventory defined at the current site context. The administrator can chose either a cross-site shared DN or a site-local DN.

2.41.4. Shared Line Across Sites Example Diagram

The following figure provides a basic Shared Line Across Sites configuration using one Inventory site ("c2Inventory") and two real sites ("c2s1" and "c2s2"). In this example there are 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 level to make them visible to all

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

the 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. Notice that both shared DNs and non-shared DNs can co-exist for the same customer.



2.41.5. Inventory Site

It is important to understand that an Inventory Site is only an Inventory Site by name, not by type. An Inventory Site is just a regular site, and is no different than any other site, except that it does not have an **Inventory Site** check box, and is deployed exactly the same as any other site. It is only by convention that we're calling this an Inventory Site and designating this site as the repository for lines to be shared across sites.

The Inventory Site is created from the **Site Management > Sites** menu. 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

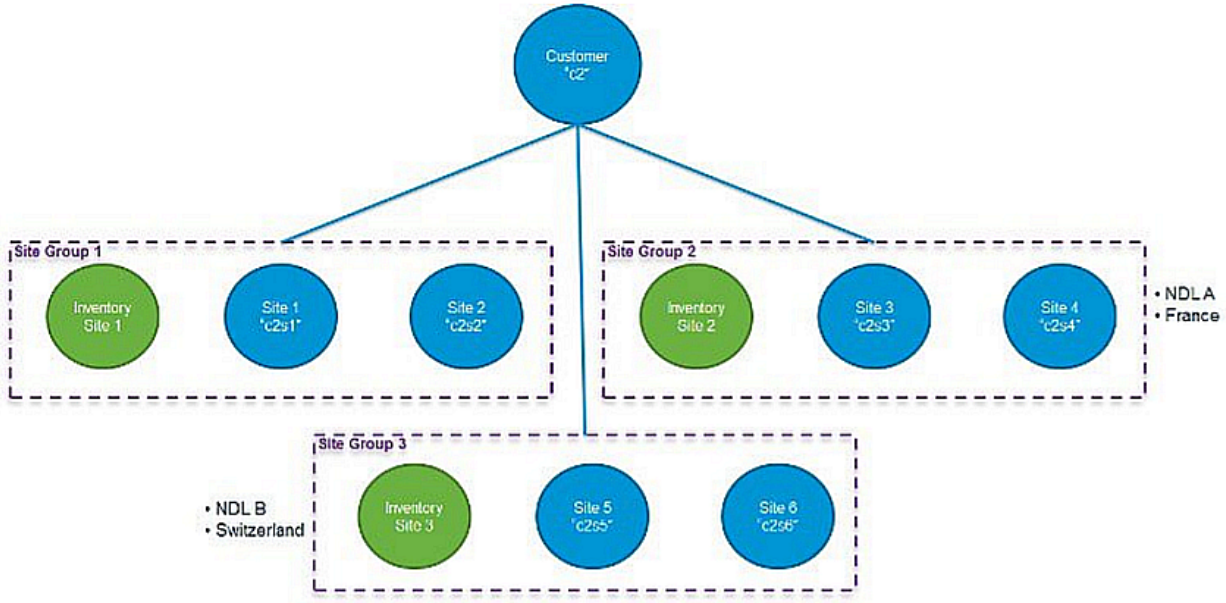
Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

2.41.6. Inventory Site Diagram

The following diagram shows a customer with three Site Groups.



2.41.7. Dial Plan Type for Shared Line Across Sites

The Shared Lines Across Sites feature only works if you are using a flat dial plan (Type 4), or a custom dial plan that is not site-specific). The reason is that the other dial plans (Types 1 to 3) have site location codes in the DN which do not work if the DN is shared by multiple sites.

If you're using the predefined dial plans, do not select the **Site Location Code** check box when deploying the Customer dial plan.

2.41.8. 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. There are a number of CSSs defined when a customer and site dial plan are deployed, and some of the CSSs are only used internally and should not be selected in the CSS drop-down list on a line or phone configuration page.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

The Class of Service CSSs are listed in the **Dial Plan Management > Site > Class of Service** menu item. 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.

COS is used in two places:

1. **Line Calling Search Space** - which appears in VOSS-4-UC at **Subscriber Management > Lines > Directory Number Basic Information tab > Calling Search Space**
2. **Device Calling Search Space** - which appears in VOSS-4-UC at
    - **Subscriber Management > Phones > Phone tab > Calling Search Space Name**
    - **Subscriber Management > Subscribers > Phones tab > Calling Search Space Name**

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.

	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 subscriber numbers are not variable length and there is no site-specific area codes (only national dialing), then most of

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

In order to decide how to distribute routing and feature processing between the line COS and the device CoS, refer to the table that follows.

	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 subscriber 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.

Table: Routing and Feature Processing between Line CoS and Device CoS

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**

2.41.9. 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

2.41.10. Phone, Subscriber, and Quick Add Subscriber use for Shared Line Across Sites

Phones and Subscribers should only be created at real sites, not Inventory Sites. This is not enforced in the workflows, but will help facilitate ongoing management of the configuration data for the customer. Lines referenced in the **Phone** screen, the **Subscribers** screen, or the **Quick Add Subscriber** screen are created automatically if they have not already been provisioned in the Inventory Site and pushed to Cisco Unified Communications Manager. 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.

The fields of interest on the **Phone** screen are on the **Phone** tab and the **Lines** tab. The **Phone** tab is where you specify the Calling Search Space Name; this is the device-based routing class of service (CoS). By default this is the emergency routing CSS. Depending on choices made above in the Class of Service section, you might chose a different CSS here.

The **Lines** tab is where you pick the DN (Pattern) from the drop-down list, and where you configure the E.164Mask used for line presentation. The DN drop-down list includes DNs from the Customer DN inventory combined with the current site DN inventory. The E.164Mask is a free-form field and is not tied to the E.164 inventory currently; it must be manually entered. These are the only fields that are pertinent to the Shared Line Across Sites feature.

The Route Partition Name is automatically populated with the correct directory number partition based on the Pattern (DN) that is selected. Similar fields exist in the **Subscribers** tabs.

2.41.11. Hunt Groups and Call Pickup Groups for Shared Line Across Sites

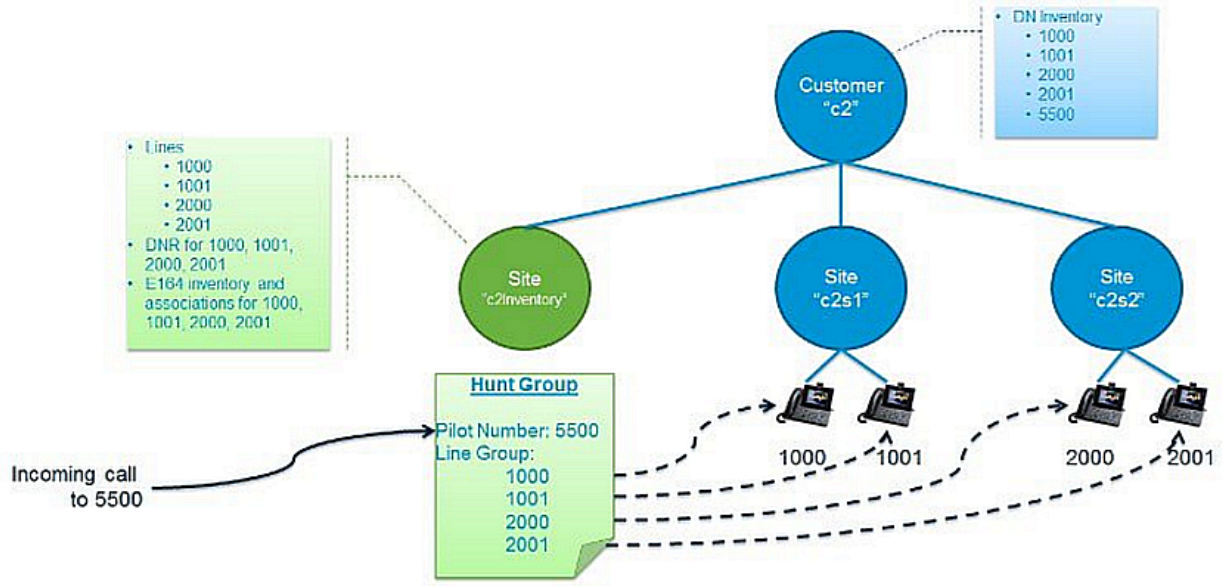
Hunt Groups and Call Pickup Groups can be configured in either the Inventory Site or the real sites. If configured in the Inventory Site, the Hunt Groups and Call Pickup Groups can include any line configured in the Inventory Site, but cannot include lines created in other sites. Likewise, if configured in the real site, the Hunt Groups and Call Pickup Groups can include any line configured in the real site but not other sites.

We recommend that you configure Hunt Groups and Call Pickup groups in the Inventory Site if they need to include lines that are not all isolated to one site.

2.41.12. Hunt Groups and Call Pickup Groups for Shared Line Across Sites Example

The following figure provides an example of a Hunt Group that uses lines spanning multiple sites.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



Note that lines 1000, 1001, 2000, and 2001 are not themselves shared across sites. However, because all lines in one Hunt Group must exist at the same site, all four lines must be configured in the Inventory Site to be included in the one Hunt Group with Hunt Pilot 5500.

Also note that the Hunt Pilot DN inventory is at the customer level. Once the Hunt Pilot is assigned, that DN is marked as unavailable for any other usage (that is, it cannot be assigned to a device as a line, nor can it be used for another service pilot number).

2.41.13. Site Short Codes

Site short codes work the same for deployments that use shared lines across sites as they do for “real site” deployments. That is, short codes can be added to a site to allow shorter, convenient numbers to be dialed that are transformed into longer directory numbers. Normally, short codes are added to real sites that contain devices in order to allow users of those devices to dial shorter numbers to reach exiting directory numbers.

Because the inventory site doesn’t contain devices, but only line inventory, site codes don’t need to be added to the inventory site. Short code translation patterns are created on a site’s Allow Internal (AInt) route partition.

2.41.14. Handling Voice Mail to Secondary Shared Lines

To handle Voice Mail 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 VOSS-4-UC. There are no separate manual configurations required in Cisco Unity Connection or Cisco Unified Communications Manager.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Note: One additional license is required for the shared line user mailbox.

2.41.15. Shared Line Across Sites Configuration Procedures

Most of the configuration for Shared Lines Across Sites is the same as with conventional lines, but this section provides procedures to highlight the differences.

For conventional site-local lines, the lines can be configured automatically as part of the Phone, Subscriber, or Quick Add Subscriber workflows; the lines do not need to be configured separately first.

For lines to be shared across sites, they must be configured first in the Inventory Site, then referenced from Phone, Subscriber, or Quick Add Subscriber workflows.

Configure Shared Line Across Sites - 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 Unified Communications Manager and Cisco Unity Connection 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) because 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 (**Dial Plan Management > Number Management > 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 - 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. Refer to *Class of Service for Shared Line Across Sites* for more information.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

4. Configure Directory Number Routing (DNR) for the shared lines (**Dial Plan Management > Site > Directory Number Routing**).
5. Create line relations for each shared line (**Subscriber Management > Line**).
6. Create E.164 inventory (**Dial Plan Management > Number Management > Add E164 Inventory**).
7. Associate E.164 to DN (**Dial Plan Management > Number Management > E164 Associations (N to N)**.
8. Configure Hunt Groups that use shared lines (**Subscriber Management > Hunt Groups**).
9. Configure Call Pickup Groups that use shared lines (**Subscriber Management > Call Pickup Groups**).

Configure Shared Line Across Sites - Real Site

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. Refer to *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 subscribers and phones (**Subscriber Management > Subscribers, Quick Add Subscriber**, or **Phones**).
    a. When configuring normal lines (lines that are not 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.

2.41.16. Notes and Limitations

The following summarizes some of the limitations concerning the Shared Lines Across Sites feature:

- A new Inventory Site is required for each new combination of NDL and Country (a “site group”). In other words, the lines configured at the Inventory Site are specific to the NDL and Country defined for that site.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- 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 VOSS-4-UC.
- Shared lines cannot span countries or NDLs. This is necessary because Cisco Unified Communications Manager 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 VOSS-4-UC.
- When configuring a phone or subscriber 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. In other words, 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 is 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 cannot be moved. To move the line, delete the line 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.
- An Site Administrator logged in to a real site is not able to see the line configuration that exists at the Inventory Site. A Customer Administrator or above can see the line configurations at all of the sites.
- The Shared Lines Across Sites feature only works when using a flat dial plan. The reason is that other dial plans have site location codes in the DN which won't make sense if the DN is shared by multiple sites. The default VOSS-4-UC template bundle includes a Type 4 flat dial plan, but other custom dial plans that are not site-specific can be used.
- Self-provisioning does not work for DNs defined at the customer level.
- Although an Administrator can delete Inventory Sites, we do not recommend it. If the Inventory Site is deleted, all hunt groups, call pickup groups, voice mail 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 which 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.

2.41.17. Configure Tail End Hop Off

Note: The following task is applicable only if you are using VOSS-4-UC 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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, RoutList: 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. Select **Device Management > CUCM > 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).

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3 Advanced Management

3.1. Macros

3.1.1. Macros in VOSS-4-UC

Macros can be used in VOSS-4-UC 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 as shown in the table that follows. 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. Note that there are no spaces in a named macro.

This table provides a list of Named Macros currently available. This list will be expanded as new macros become available.

Named Macro	Description
HcsDpCustomerName	Name of the customer (as specified when you create your customer)
HcsDpCustomerId	Systemwide, unique internal customer ID generated when you create a customer
HcsDpSiteName	Name of the site (as specified when you create a site under a customer)
HcsDpSiteId	Systemwide, unique internal site ID generated when you create a site
HcsDpUniqueCustomer PrefixMCR	Default unique Cisco HCS customer prefix in the form 'Cu{{ macro.HcsDpCustomerId }}'
HcsDpUniqueSite PrefixMCR	Default unique HCS site prefix in the form 'Cu{{ macro.HcsDpCustomerId }}Si {{ macro.HcsDpSiteId }}'
HcsDpSiteCountryMCR	Returns the country associated with a specific site
HcsDpSiteCountryIso	Returns the ISO 3166-1 alpha-3 three-letter country code associated with the country that is associated with a specific site
HcsDpPstnBreakout	Returns the PSTN prefix digit for the country that is associated with a specific site
HcsDpSiteAreaCode InLocalDialingMCR	Returns True if a specific site requires area code for local PSTN dialing
HcsDpSiteNatTrunk PrefixMCR	Return the national trunk prefix associated to a particular site
HcsDpDefaultSite DevicePoolMCR	Default Cisco HCS site device pool Cisco Unified Communications Manager element name
HcsDpDefaultSite LocationMCR	Default Cisco HCS site location Cisco Unified Communications Manager element name
HcsDpDefaultSite RegionMCR	Default Cisco HCS site region Cisco Unified Communications Manager element name

The following macros 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

3.2. Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3.2.1. 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 VOSS-4-UC 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 VOSS-4-UC

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.

3.3. Create Schemas

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3.3.1. Create Schemas

Use this procedure to configure a customized group of related dial plan elements in Cisco Unified Communications Manager, 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 you configure a dial plan schema using this procedure, the elements are not made available on the Cisco Unified Communications Manager until after the dial plan schema has been placed in a Dial Plan Schema group (refer to Create Schema Groups), and the group is associated with a customer (refer to Associate Custom Schemas to Customers).

Duplicate entries in dial plan hinders the deployment of dial plan, in such a scenario ensure that all dial plan entries are unique.

---

1. Log in to VOSS-4-UC as the Provider or Reseller Administrator.
2. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema**.
3. Click **Add** to add a custom schema.
4. Enter a unique name for the schema in the Dial Plan Name field.
5. (Optional) Enter a description for the schema in the Description field.
6. Click the **Time Periods** tab to add time periods for the schema.
7. Perform the following to add time period information for the schema:
    a. Click + on the right side of the grid to add a new row.
    b. Enter a Time Period Name and Description (optional) for the time period.
    c. From the Time of Day Start and Time of Day End drop-down menus select the start and end time for the time period.
    d. (Optional) From the Start Day, End Day, Start Month, End Month drop-down menus, select the day and month characteristics of the time period if desired.
    e. (Optional) Enter a Start Day of the Month and End Day of Month in the Start Day of Month and End Day of Month fields if desired.
8. Click the **Time Schedules** tab to add time schedules for the schema.
9. Perform the following to add time schedule information for the schema:
    a. Click + on the right side of the grid to add a new row.
    b. Enter a Time Schedule Name and Description for the time schedule.
    c. Click the Time Periods More button to enter more information about the time period associated with this time schedule.
10. Click the **Partitions** tab to add or modify partition information for the schema. Modify a partition's characteristics by changing the information in the grid. Click + on the right side of the grid to add a new row. You can use macros if desired to add partition information. For more information on using macros as part of the Partition Names, Descriptions, or Time Schedules, see Macros.
11. Click the **Calling Search Spaces** tab to add CSSs for the schema.
12. Perform the following to add or modify a calling search space's characteristics as follows:
    a. Click + on the right side of the grid to add a new row.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

b. Using macros if desired, enter a CSS Name and Description (optional) for the calling search space. For more information on using macros, see Macros.

c. Enter the reason for the CSS in the Partition Usage field.

d. Click the Class of Service box if this CSS is used in a Class of Service.

e. Click the Partitions More button to enter more information about the partitions associated with this CSS.

13. Click the **Translation Patterns** tab to add translation patterns for the schema.
14. Complete fields in this tab to add or modify translation patterns.
15. Click the **Calling Party Transformation Patterns** tab to add calling party transformation patterns for the schema.
16. Complete fields in this tab to add or modify calling party transformation patterns.
17. Click the **Called Party Transformation Patterns** tab to add called party transformation patterns for the schema.
18. Complete fields in this tab to add or modify called party transformation patterns.
19. Click the **CTI Route Points** tab to add CTI route points for the schema.
20. Complete fields in this tab to add or modify CTI route points.
21. Click the **Route Lists** tab to add route lists for the schema.
22. Complete fields in this tab to add or modify route lists.
23. Click the **Route Patterns** tab to add route patterns for the schema.
24. Complete fields in this tab to add or modify route patterns.
25. Click the **SIP Route Patterns** tab to add SIP route patterns for the schema.
26. Complete fields in this tab to add or modify SIP route patterns.
27. Click **Save** to save the new dial plan schema. The new dial plan schema appears in the list of Dial Plan Schemas.

What to Do Next

Perform Create Schema Groups to add dial plan schemas to a schema group.

3.4. Clone Dial Plan Schemas

3.4.1. Clone Dial Plan Schemas

Use this procedure to copy 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 VOSS-4-UC as the Provider or Reseller Administrator.
2. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3. From the list of dial plan schemas, choose the one to be cloned, by clicking on its box in the leftmost column. For more information on the default dial plan schemas, refer to Default Dial Plan Schemas.

   Note: There may be duplicate dial plan schemas in the list because some of the dial plan schemas may have been auto-cloned to the Provider hierarchy node. For more information, see Auto-Cloning of Dial Plan Schemas and Schema Groups to the Provider Hierarchy Node.

4. Click **Action > Clone**.
5. From the **General** tab, enter a new unique name for the cloned dial plan in the Dial Plan Name field.
6. If desired, add a description of the new cloned dial plan schema in the Description field.
7. Modify or add time periods, time schedules, partitions, calling search spaces, translation patterns, calling party transformation patterns, called party transformation patterns, CTI route points, route lists, route patterns, and SIP route patterns as desired by clicking on the appropriate tab.
8. Click **Save**. The new dial plan schema appears in the list of Dial Plan Schemas.

3.5. Modify Site Defaults

3.5.1. Overbuild Site Defaults: Overview

Important: System Integrator Support Recommended - For all Managed Services: Day 2 Overbuild Projects, we recommend support from a System Integrator.

While Customers and Sites have access to Site Defaults under the Site Management menu, the Overbuild Defaults tab is only visible to Provider and Reseller Administrators.

The settings on the Overbuild Defaults tab of Site Defaults determine if and how imported objects are moved to the site hierarchy during an Overbuild process.

The settings on this tab work as follows:

- Include Site for Overbuild: If selected, the site is included in the Overbuild and all the settings on the Site Defaults tabs apply.

  The list of defaults when the menu **Site Management > Defaults** is selected, show “true” in the Include Site for Overbuild column.

- Create Internal Number Inventory at Customer: If clear, the internal number inventory is created at site level only. If selected, the internal number inventory is created at customer level only, and will be used by all sites belonging to that customer, default = cleared.

Caution: If Overbuild has already been run for a site and the Internal Number Inventory has been created for the Site, if the option ‘Create Internal Number Inventory at Customer’ is enabled and Overbuild is run for the same Site, then a duplicate set of Internal Number Inventory will be created at the Customer. The same applies if the ‘Create Internal Number Inventory at Customer’ is enabled when Overbuild is run for the Site, if it is then disabled and Overbuild is run again, a duplicate set of Internal Number Inventory will be created at the Site.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- Additional Device Pools: By default, if a site is included for the Overbuild process, the Default CUCM Device Pool on the General Defaults tab has to match the Device Pool of the phones that have been imported in order for these and their related objects to be moved to the site at which the Site Defaults Doc exists. The Run Overbuild tool uses the Device Pool in order to determine which devices and models are to be moved to the site where the site defaults are defined.

  However, additional Device Pools can be added, so that more than one Device Pool from those of the imported phones can be moved to the same site. Additional Device Pools are selected from the Device Pool Name drop-down list as instances of the Additional Device Pools group control.

  The names of the additional Device Pools can be renamed to the Default Device Pool name as entered on the General Defaults tab if the Replace with Default Device Pool box is selected.

- Overbuild Device Control:
  - Move All Devices: If selected, all matching and related imported devices are moved to the site.
  - Limit Moved Devices: If selected, check boxes appear for selecting devices to import to the site. This corresponds with the controls and logic on the Run Overbuild interface. For details on the interdependency and available options when check boxes are selected, see *Run Overbuild: Overview*.

3.5.2. Run Overbuild: Overview

Run Overbuild processes Unified CM imported objects for all sites in the current customer. It must be run at the Customer hierarchy.

A device model is moved to a site on condition that there is a Network Device List Reference (NDLR) referencing the device at the site.

Note: The line goes to the first site that the Run Overbuild tool finds. The site selection is not deterministic.

The conditions for creating or updating the INI (Internal Number Inventory) during Overbuild are listed in the table below:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Given	Then
• INI exists at Site. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear.	The lines in the INI at the Site are updated to “Used”.
• INI exists at Customer. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear.	The lines in the INI at the Customer are updated to “Used”.
• No INI exists. • Site Defaults “Create Internal Number Inventory at Customer” check box is clear.	The INI is created at the Site.
• INI exists at Customer. • Site Defaults “Create Internal Number Inventory at Customer” check box is selected.	The lines in the INI at the Customer are updated to “Used”.
• INI exists at Site. • Site Defaults “Create Internal Number Inventory at Customer” check box is selected.	The lines in the INI at the Site are updated to “Used”.
• No INI exists. • Site Defaults “Create Internal Number Inventory at Customer” check box is selected.	The INI is created at the Customer.

The options available in the **Overbuild Action** drop-down are:

- **All Enabled Sites Using Settings Below**
  - All selected devices on the **Run Overbuild** form are included.
  - The Site Defaults Doc for each site contains an **Overbuild Defaults** tab. If the **Include Site for Overbuild** check box is selected, the site is included.
  - An internal number inventory is created at customer level if the **Create Internal Number Inventory at Customer** check box is selected or at site level if the check box is cleared (if **Lines** are included).
  - The Device Pools are from the **General Defaults** tab of the Site Defaults Doc and the Additional Device Pools from the **Overbuild Defaults** tab.
  - The devices displayed when the **Limit Move Devices** option is selected on the **Overbuild Defaults** tab are ignored. Runs Overbuild for all sites, and uses the devices selected on the **Run Overbuild** form.

    When the Run Overbuild tool executes with this option, it will apply to all sites and use the devices selected on the **Run Overbuild** form. Run Overbuild devices supersede the devices selected in **Limit Move Devices**.
- **All Enabled Sites Using Site Defaults Doc Overbuild Settings**

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

  - Selected devices on the **Run Overbuild** form are hidden and ignored. All selected devices when **Limit Moved Devices** is chosen on the **Overbuild Defaults** tab of Site Defaults are moved.
  - The site is included only if the **Include Site for Overbuild** check box is selected.
  - An internal number inventory is created at customer level if the **Create Internal Number Inventory at Customer** check box is selected or at site level if the check box is clear (if **Lines** are included).
  - The Device Pools are from the **General Defaults** tab of Site Defaults and the Additional Device Pools from the **Overbuild Defaults** tab will be used.
- **Single Enabled Site Using Settings Below**
  - Overbuild is applied to the single site specified in the **Select Site** drop-down, which is exposed when this Overbuild option is selected.

    Only sites that have the **Include Site for Overbuild** check box selected in the Site Defaults Doc are available in the drop-down.
  - All selected devices on the **Run Overbuild** form are included.
  - An internal number inventory is created at customer level if the **Create Internal Number Inventory at Customer** check box is selected or at site level if the check box is clear (if **Lines** are included).
  - The Device Pools are from the **General Defaults** tab of the Site Defaults Doc and the Additional Device Pools from the **Overbuild Defaults** tab.
  - The devices displayed when the **Limit Move Devices** option is selected on the **Overbuild Defaults** tab are ignored. Runs Overbuild for the selected site, and uses the devices selected on the **Run Overbuild** form.

    When the Run Overbuild tool executes with this option, it applies to the selected site only, and uses the devices selected on the **Run Overbuild** form. Run Overbuild devices supersede the devices selected in **Limit Move Devices**.

Available device types include:

- Phones
- Phone Remote Destinations
- Users:
  - `device/cucm/User`
  - `device/hcmf/User` (only if HCM-F is installed)
- Device Profiles
- Remote Destination Profiles (RDP)
- RDP Remote Destinations
- Lines (a number inventory entry is also added for all `device/cucm/Line` instances that are in the system at the customer or site level)
- CUC Users
- Webex Teams Users
- Contact Center Agents

The specific device models that are affected by the Overbuild move, are:

- device/cuc/User
- device/cuc/UserPassword

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- 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/hcmf/User (only if HCM-F is installed)
- device/spark/User
- device/uccx/Team
- device/uccx/Skill
- device/uccx/ResourceGroup
- device/uccx/Agent

Data models affected when the user is moved during Overbuild:

- data/User
- data/LdapUser
- data/SsoUser
- data/NormalizedUser
- data/HcsUserProvisioningStatusDAT
- data/HCSHcmfUserDAT

The availability of certain device type check boxes depends on the status of other device type check boxes. For example, the **Dual-Mode Remote Destinations**, **Users**, and **Lines** check boxes are only available if the **Phones** check box is selected. The **Device Profiles**, **Remote Destination Profiles**, and **CUC Users** check boxes are only available if the **Users** check box is selected.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Overbuild workflows do not stop on any transaction failures and no transaction rollback takes place on errors. For example, device instance move operations to Sites continue for all selected devices. Inspect the transaction log for errors.

In the Transaction log, subtransactions of a successful overbuild workflow show their Status as “Fail” if a model (such as a User) already exists. The subtransaction logs also show details of the duplicate model and an “ignore error code” information message.

3.5.3. Overriding Unified CM Group

The default Unified CM 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 the users to use a Unified CM Group other than “Default” when deploying their site dial plan. The steps allow you to override the Default CM 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 (Subscriber 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. Navigate to **Dial Plan Management > Advanced Configuration > 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 Unified CM groups in any workflow at the site hierarchy.

Note: If you delete the Default Unified CM group from the Unified CM, deployment of the Unified CM 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>
```

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3.6. Create Schema Groups

3.6.1. Dial Plan Schema Group

Use this procedure to bundle 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 VOSS-4-UC as the Administrator, Provider, or Reseller.
2. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema Group**.
3. From the list of dial plan schema groups, choose the one to be cloned, by clicking on its box in the leftmost column.

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. If desired, 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.
    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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

3.6.2. Cisco Shell Schema Groups: Overview

To deploy your own existing dial plan rather than one of Cisco's out-of-the-box dial plans, use the shell schema group to enable core functionality without deploying a preconfigured VOSS-4-UC schema group. The shell schema group provides a starting point for you to build your own dial plan. The shell schema group has no preset site default values other than Default Device Pool and Default CUCM Group. The shell schema group does not contain any default core schemas, features schemas, or country schemas. You can clone the shell schema group instance and tailor all other settings to your own specifications.

On the Custom Workflows tab, the shell schema group provides default workflows for the following registry events used to create customer inventories and associations:

- addDnInventory - allows you to create DN inventory without enforcing any rules or constraints on the DN numbers
- addE164Inventory - allows you to create E164 inventory without enforcing any rules or constraints on the E164 number other than enforcing the country code prefix for a given site
- associateE164ToDn - allows E164 to DN number association (N to N) on VOSS-4-UC without configuring anything on Cisco Unified CM
- unassociateE164ToDn - removes E164 to DN number association (N to N) from VOSS-4-UC without removing anything on Cisco Unified CM
- associateE164ToSingleDn - allows E164 to DN number association (N to 1) on VOSS-4-UC without configuring anything on Cisco Unified CM
- unassociateE164ToSingleDn - removes E164 to DN number association (N to 1) on VOSS-4-UC without removing anything on Cisco Unified CM

For more information on configuring schema groups and associating them with customers, refer to the Provider HCS Dial Plan Management Support Guide.

3.7. Associate Custom Schemas to Customers

3.7.1. Associate Custom Schemas to Customers

Use this procedure to bundle a set of schemas together to form a Type 1 to Type 4 dial plan that can be applied to a customer. 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 VOSS-4-UC as the Administrator, Provider or Reseller.
2. Select **Dial Plan Management > Advanced Configuration > 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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** to save the new dial plan schema group. The new dial plan schema group appears in the list of groups.

3.8. Default Dial Plan Schemas

3.8.1. Default Dial Plan Schemas

A number of default dial plan schemas are predefined in VOSS-4-UC 10.x/11.5(x). 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 VOSS-4-UC 10.x/11.5(x) at Dial Plan > Dial Plan Schema.

Note: The HcsDefaultAddVoiceMailE164NumberSchema and HcsDefaultLboSchema default schemas are available only in VOSS-4-UC 10.6(2) or later.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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	• 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	• 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Schema Name	Description	When Deployed
CustomerToDCLIPR-Feature-Vx-SCH	• 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	• 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

HcsDefaultAddCustomerSchema	Contains the following: • 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: – 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: – 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 Deployed at the Customer hierarchy node	When the first site dial plan is created for a particular customer

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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
HcsDefault-AddSiteShortCodeSchema	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
HcsDefault-AddSite-Type1Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Also contains pre-InterSiteRouting, InterSiteRouting, and AllowInteral translation patterns for Type 1 Deployed at the Site hierarchy node	Deployed to Cisco Unified Communications Manager when a Type 1 site dial plan is created
HcsDefault-AddSite-Type2Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Also contains pre-InterSiteRouting, InterSiteRouting, and AllowInteral translation patterns for Type 2 Deployed at the Site hierarchy node	Deployed to Cisco Unified Communications Manager when a Type 2 site dial plan is created
HcsDefault-AddSite-Type3Schema	Contains site specific Allow Internal partition, site specific feature partition, and default site internal CSS. Also contains pre-InterSiteRouting, InterSiteRouting, and AllowInteral 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
HcsDefault-AddSite-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 Unified Communications Manager when a Type 4 site dial plan is created
HcsDefaultAddVoiceMailPilotNu mberSchema	Contains the Voice Mail pilot Calling Search Space and Voice Mail service route list Deployed at the Customer hierarchy node	Deployed to Cisco Unified Communications Manager when a Voice Mail pilot number is created for a customer

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

HcsDefaultAddVoiceMailE164NumberSchema	Contains the route pattern for an E164 format number associated with a Voice Mail pilot number Deployed at Site hierarchy node Note: This field may not appear if you have upgraded from CUCDM version 10.6(1) to version 10.6(2). In that case, it would need to be added manually to the dial plan schema. Refer to the CUCDM Release 11.5(1) Planning and Install Guide for details.	Deployed to Cisco Unified Communications Manager when a voice mail 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 Unified Communications Manager 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: In 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 Unified Communications Manager for each country <CCC> site that is deployed for Type 1 to 4 schema groups

3.9. Emergency and CLI Settings

3.9.1. Emergency and CLI Settings

This feature, accessed from the default menu **Dial Plan Management > Advanced Configuration > 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.

When deploying an 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

This feature allows a Provider administrator (or higher) to add up to three (3) new calling party transformation patterns to provide specific translation to a DDI for those DNs having a DDI mapping. The transformations are created and deleted when either '1 to 1' or '1 to N' number associations are created and deleted. See *Associate a Set of E.164 Numbers to One Directory Number* and *Associate a Range of E.164 Numbers to a Range of Directory Numbers*

Using the HCS dialplan schema, site wide mapping is provided using a wildcard match to a site specific prefix used only for emergency calls. An example is '***156*!**'. This feature may be used to add more specific patterns such as '***156*81214000**' in order that transformations to the E164 can take place. DNs that do not have a mode specific match fall back to the wildcard match as previously set, and therefore use the site wide emergency CLI.

Note: There is no requirement to use any schema. This feature can be used wherever transformations are required as part of DN association.

The supported transformation patterns are:

- **Emergency CLI** transformation
- **CLI** transformation
- **Secondary CLI** transformation

A data model contains settings for this feature. A default set of settings is created at the `sys.hcs` hierarchy, which disables all 3 patterns. These settings must be cloned and used at a lower hierarchy to provide the settings required for each hierarchy, that is clone them to the provider level for platform wide settings, or customer level for customer specific settings.

Each of the 3 patterns can be enabled or disabled independently. The following additional controls are available:

- Macro for defining the partition
- Macro for defining the E164 number format
- Macro for defining the DN (pattern) format

There are 3 new macros that 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3.10. Default Dial Plan Event Triggers

3.10.1. Default Dial Plan Event Triggers

In VOSS-4-UC 10.x/11.5(x), 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.

Note: The associateLboGateway and unassociateLboGateway events are available only if you are using VOSS-4-UC 10.6(2) or later.

The default events are located in VOSS-4-UC 10.x/11.5(x) under the Custom Workflow tab at Dial Plan > Dial Plan Schema Group.

Default Dial Plan Event Triggers for Custom Workflows

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Dial Plan Event	When Triggered	Notes
preAddSite	When a new site dial plan is deployed, before the Add Dial Plan workflow is executed	For Type 1 to Type 4 schemas, this triggers a Cisco Unified Communications Manager (CUCM) bootstrap workflow that: • Updates the CUCM clusterwide "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 Items in the workflow are executed at the hierarchy node on which the target
		CUCM cluster is added to the VOSS-4-UC system. 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. The target cluster for this workflow is determined by the CUCM instance that is contained in the Network
		Device List Reference (NDLR) for the site on which this event was triggered.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 Unified Communications Manager (CUCM) 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Dial Plan Event	When Triggered	Notes
addVoiceMailPilotNumber	When a new voice mail pilot number is added for a customer	For Type 1 to Type 4 schemas, this triggers a Cisco Unified Communications Manager (CUCM) bootstrap workflow that • Creates the voice mail pilot on the target CUCM cluster • Creates a voice mail profile on the target CUCM cluster • Deploys a custom Cisco Unity Connection schema to provision the following on Cisco Unity Connection: – Direct routing rule and forward routing rules based on the new pilot number – The target Cisco Unity Connection cluster for this workflow is determined by the Cisco Unity Connection instance contained in the NDLR for the site on which this event was triggered The target cluster for this workflow is determined by the CUCM instance that is contanied in the NDLR for the site on which this event was triggered.
removeVoiceMailPilotNumber	When a voice mail pilot number is a customer	The target cluster for this workflow is determined by the CUCM and Cisco Unity Connection instances that are contained in the NDLR for the site on which this event was triggered. For Type 1 to Type 4 schemas, this triggers a workflow that • Removes the voice mail profile and pilot number from CUCM • Undeploys direct and forward routing rules on Cisco Unity Connection

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Dial Plan Event	When Triggered	Notes
associateVoiceMailServiceToCustomer	When voice mail service is associated to a customer	The target Cisco Unified Communications Manager (CUCM) and Cisco Unity Connection clusters for this workflow are determined by the CUCM and Cisco Unity Connection instances that are contained in the NDLR for the site on which this event was triggered.
		For Type 1 to Type 4 schemas, this triggers a workflow that • 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 Cisco Unity Connection schema to provision the port group, ports, route partition, calling search space (CSS), and the user template for voice mail service on the Cisco Unity Connection
disassociateVoiceMailServiceFromCustomer	When voice is disassociated from a	The target CUCM and Cisco Unity Connection clusters for this workflow are determined by the CUCM and Cisco Unity Connection instances that are contained in the NDLR for the site on which this event was triggered. For Type 1 to Type 4 schemas, this triggers a workflow that • On CUCM, removes Voice Mail service route group and SIP trunk if dedicated or partitioned voice mail service • On Cisco Unity Connection, deletes customer-specific route partition, css, user template, ports, and port group.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Dial Plan Event	When Triggered	Notes
addCustomer	When a customer dial plan is added	The target Cisco Unified Communications Manager and Cisco Unity Connection clusters for this workflow are determined by the Cisco Unified Communications Manager and Cisco Unity Connection 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 Cisco Unified Communications Manager (CUCM) and Cisco Unity Connection clusters for this workflow are determined by the CUCM and Cisco Unity Connection 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 Unified Communications Manager (CUCM) and Cisco Unity Connection clusters for this workflow are determined by the CUCM and Cisco Unity Connection instrances 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 Cisco Unified Communications Manager (CUCM) and Cisco Unity Connection clusters for this workflow are determined by the CUCM and Cisco Unity Connection instances that are contained in the NDLR for the site on which this event was triggered. Add the updateSite event with the HcsDpUpdateSiteAreaCodesPWF workflow to update the site dial plan. Currently not supported because site dial plan updating is not supported

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Dial Plan Event	When Triggered	Notes
addDnInventory	When an administrator provisions additional specific site	The target Cisco Unified Communications Manager (CUCM) cluster for this workflow is determined by the CUCM instance that are contained in the NDLR for the site on which this event was triggered. 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. If a Type 2 dial plan is provisioned, this executes a workflow that creates DNs where the extension is prefixed with the Intersite Prefix + Site Location Code of the site on which the event was triggered. If a Type 4 dial plan is provisioned, this executes one of the following workflows: • 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.

3.11. Manual Configuration to Correct Calling Presentation Overwrite on Calls Forwarded to PSTN

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3.11.1. Manual Configuration to Correct Calling Presentation Overwrite on Calls Forwarded to PSTN

Use this procedure to correct 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. Select **Dial Plan Management > Advanced Configuration > 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 VOSS-4-UC.
11. If there are deployed customers, then:
    a. Log in as the provider administrator.
    b. Select **Device Management > CUCM > 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

3.12. Global Settings

3.12.1. Global Settings

Provider administrators and higher have access to a **Global Settings** customization menu that allows for the configuration of a number of settings across all hierarchies or per individual hierarchy.

- On the GUI, the greyed-out value is the current setting either inherited from the hierarchy above or as a result of the selected drop-down option.
- The setting title and description provides a guide to its functionality.

Settings are enabled or disabled using a drop-down and can be one of 3 values:

- **Inherit**: the current setting is determined by the setting in the hierarchy above the current one. The greyed-out value is currently applied.
- **Yes**: enable the setting. This may change the current value.
- **No**: disable the setting. This may change the current value.

The following tabs are available:

- **Number Inventory**
  - **Include the Number Inventory description in all number drop-downs**: when the Number Inventory is managed from the **Number Management** menu, descriptions can be added to the numbers (for example, "CEO number"). Default = **No**.

    This setting controls the display where the number is listed on a form drop-down. The description will be displayed if the setting is **Yes**.
  - **Enable Number Inventory Cooling**:

    Default = **False** (not enabled).

    Choose **Yes** from the drop-down to enable number cooling. If the inherited value is set to **True**, number cooling is already enabled.

    See "Number Cooling" for more information.
  - **Number Inventory Cooling Duration (Days)**:

    Default = 30 days.

    If you want to choose a different value from the inherited value, then enter the required number of cooling duration days in this field.
- **Webex Teams**
  - For the **Retain a Webex Teams User when a Subscriber is deleted** and **Send SNMP trap message when the Webex Teams Refresh Token expires** drop-downs, the values can be inherited or set as required.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

  - For the **Webex Teams Refresh Token expires threshold (in seconds)** drop-down, the default (inherited) value is `172800`. In this case, the value itself can be changed, in other words there are no **Yes** or **No** options.

- **Email**
  - For the **Allow email to be sent to user after Quick Add Subscriber**: By default the setting is inherited from the hierarchy level directly above the current one. When set to **Yes** at a hierarchy and a SMTP server is *also* set up for a hierarchy on the **Device Management** menu, a check box is available on the **Quick Add Subscriber** input form to send an email to the subscriber. See: SMTP-server.

- **Phones**
  - For **Delete existing Unassigned Phone when re-adding an identical Phone**: by default (inherited), the setting is **False**. This means that if a Phone with the same Name and Product Type is re-added to the system during for example a QuickAddSubscriber bulk load or re-add of a Subscriber during a Subscriber update, it will *not* by default be overwritten.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

4 Basic Call Flow Overview

4.1. 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.

4.2. Multi-Site Customer with ISP Included in SLC

The Intersite Prefix (ISP) is included as the first digit of the site code. Currently, VOSS-4-UC 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	• Extension (for example, 4321) • Site Code + Extension (for example, 81134321	• 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	• PSTN Prefix + PSTN Number (for example, 919722221234 • E.164 Number (for example, +19722221234	• (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 Unified Communications Manager, Cisco Unified IM and Presence Service, and Cisco Unity Connection

4.3. 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	• Extension Prefix + Extension (for example example, 51234) • Site Code + Extension (for example, 2551234)	• 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)		-

4.4. Single Site Customer

Since this is a single site customer, it does not require a Site Code.

Single Site Customer

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	• Extension (subset of DID number) (for example, 4321 or 54321 if extension prefix is used) • Site Code + Extension for (example, 81134321	• Extension	Even though a site code has been assigned, users are not aware of it. Note: Explicit extension prefix may not be required and it can be included as the first digit of the extension.
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

4.5. Customer (Single- or Multi-Site) Without PSTN Prefix

Most of the calls made by these customers are PSTN calls. The Cisco Unified Communications Manager 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing (single site only)	• Extension Prefix + Extension (for example, *4321)	• 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)		For a multi-site customer, it is recommended that extension dialing is not supported and all calls are dialed as ISP + Site Code + Extension. Note: ISP must not conflict with PSTN dialing and is therefore limited to * or #.
PSTN Dialing	• PSTN Number (for example, 19197221234 • E.164 Number (for example, +19728134321	• 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	• Extension(Single Site) (for example, 4321) • Site Code + Extension (Multi-Site) (for example, 2554321)		

4.6. 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

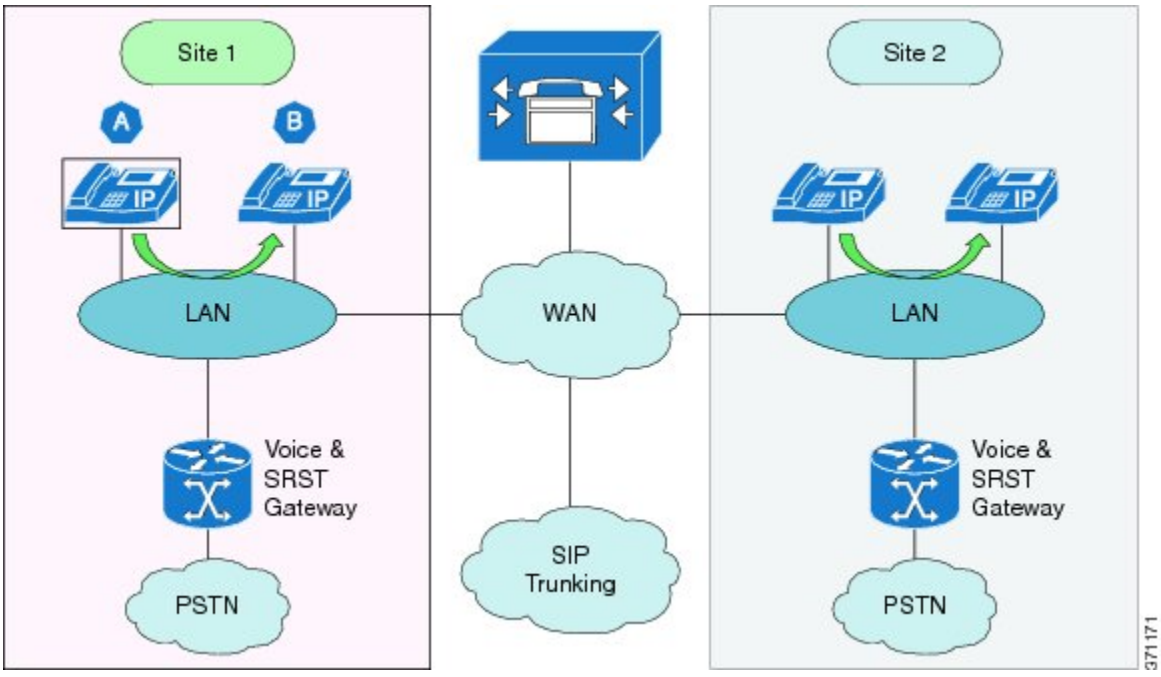
	Dialing Format (A-Party)	Display Format (B-Party)	Notes
Intra-Site Dialing	• Extension (for example, 4321 or 54321) • ISP + Site Code + Extension (for example, 82554321)	• Extension • ISP + Site Code + Extension	Intra-Site Calls can be dialed as an extension or as an ISP+ Site Code + Extension. Similarly, 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, 81134321OR ISP + Site Code + Extension (for example, 82554321)	Site Code + Extension	The DN can be constructed with or without ISP

4.7. On-Net Call Flows

4.7.1. 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)



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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 Unified Communications Manager
Default Configuration Configuration Choices	Available to all users • 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: • 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	• Cisco IP phones • Cisco ATA • Cisco VG

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 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

4.7.2. 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

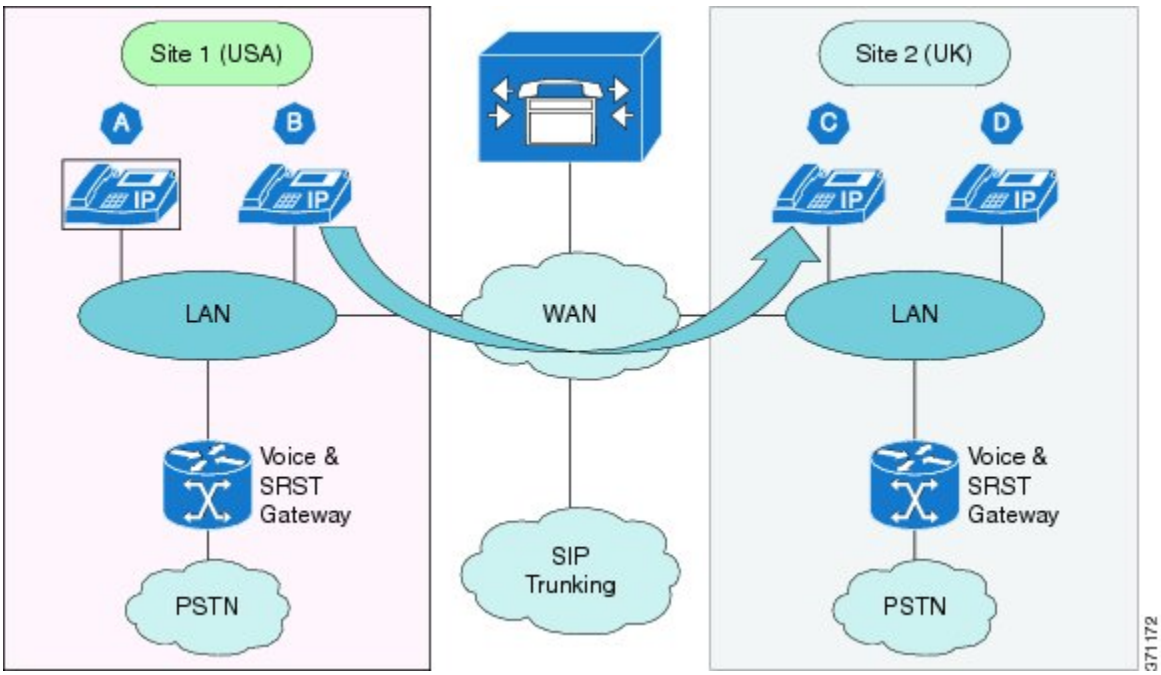
When the user dials a directory number of another user, the leaf cluster first examines the site code, and determines if the site code is for a site on the same cluster or another cluster. If the site is on the same

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 Unified Communications Manager that belongs to the same customer. As shown in the following figure, media traffic is between the endpoints.

On-Net Call (Inter-Site)



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• User can be located in the same or different countries (sites can be in different countries and or different Cisco Unified Communications Manager 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 Unified Communications Manager
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	• 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	• Cisco IP phones • Cisco ATA • Cisco VG

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

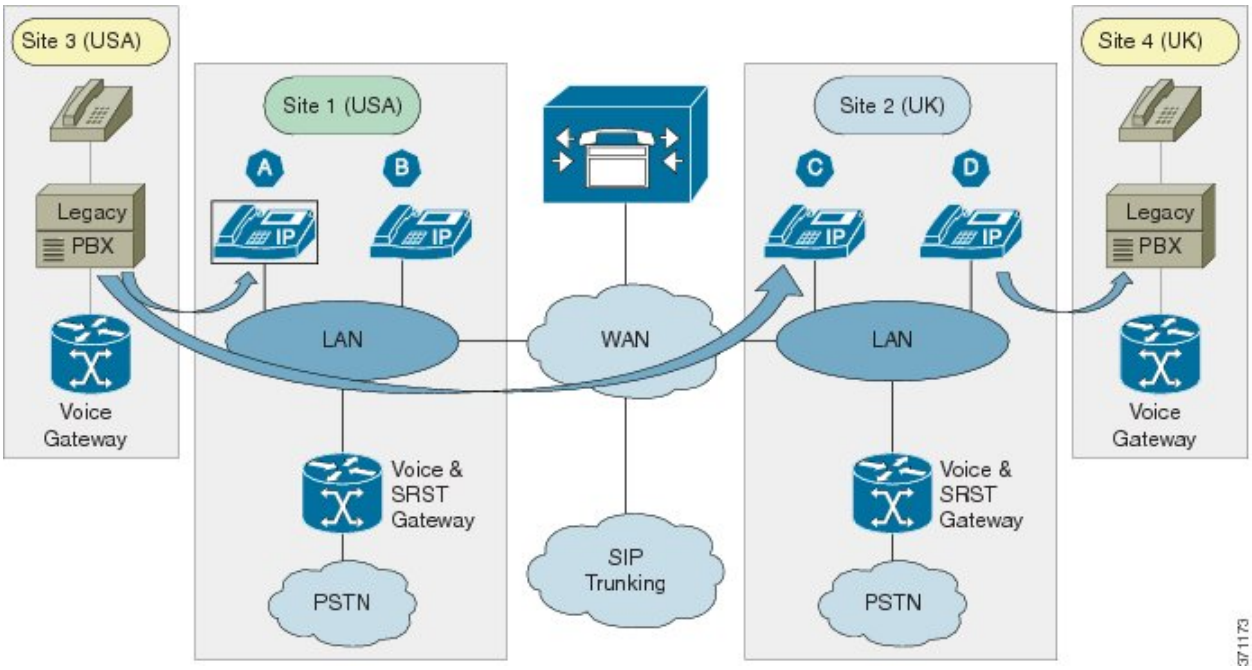
4.7.3. VoIP Trunking On-Net Call

This call type occurs between endpoints connected to Cisco Unified Communications Manager 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 Unified Communications Manager
- SIP signaling traffic between the Voice Gateway and the Cisco Unified Communications Manager
- TDM signaling traffic between the Legacy PBX and Voice Gateway
- Media traffic between the endpoint and Voice Gateway

On-Net Call (VoIP Trunking)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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 Unified Communication Manager • 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	• User can perform On-Net call from any endpoint registered with Cisco Unified Communications Manager • 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	• 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Configuration Choices	• 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	• Cisco IP phones • Cisco ATA • Cisco VG
Example	Example: Phone D (DN=8 200 6100) Dial 8 400 1234 to Legacy PBX Connected Number shows 8 400 1234 Legacy PBX (Site 3) Dial 8 100 2123 to Call A Phone C (DN=8 100 2123)

4.8. Off-Net Call Flows

4.8.1. 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

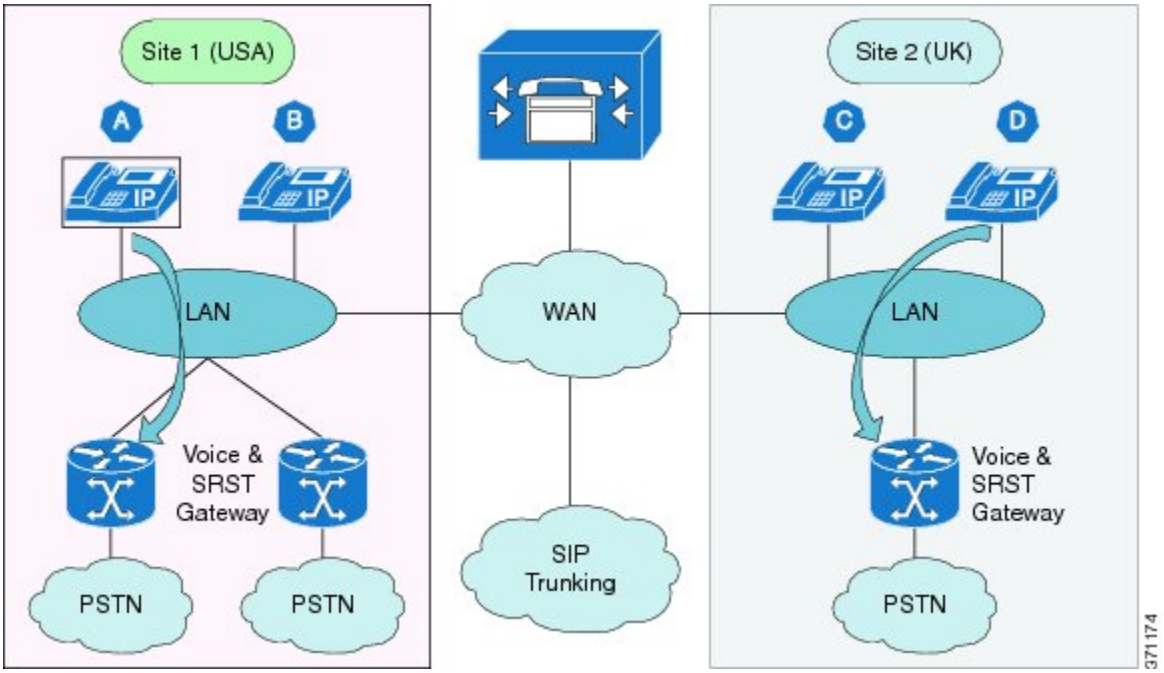
The Local Gateway is used to connect to the PSTN locally. In this case, it must be possible on a per-call basis to select the Local Gateway breakout and there must be selectable per-site routing through the Local Gateway (that is, International, National, Service, and so on).

The call type includes:

- SIP/SCCP signaling traffic for the endpoint between the endpoint and Cisco Unified Communications Manager
- SIP signaling traffic for the Local Gateway between the Local Gateway and Cisco Unified Communications Manager
- Media traffic between the endpoint and Local Gateway

Off-Net Call (Local Gateway)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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: – 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: – 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 Unified Communications Manager
Usage Example	User can dial any PSTN number from their phone
Default Configuration	• 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	• 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	Available to users in fallback mode, with the following restrictions: • Phone must be registered to the SRST gateway • No COS is available during survivability mode

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Endpoint Types Supported	• Cisco IP phones • Cisco ATA • Cisco VG
Examples	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

4.8.2. Aggregation (CBO)

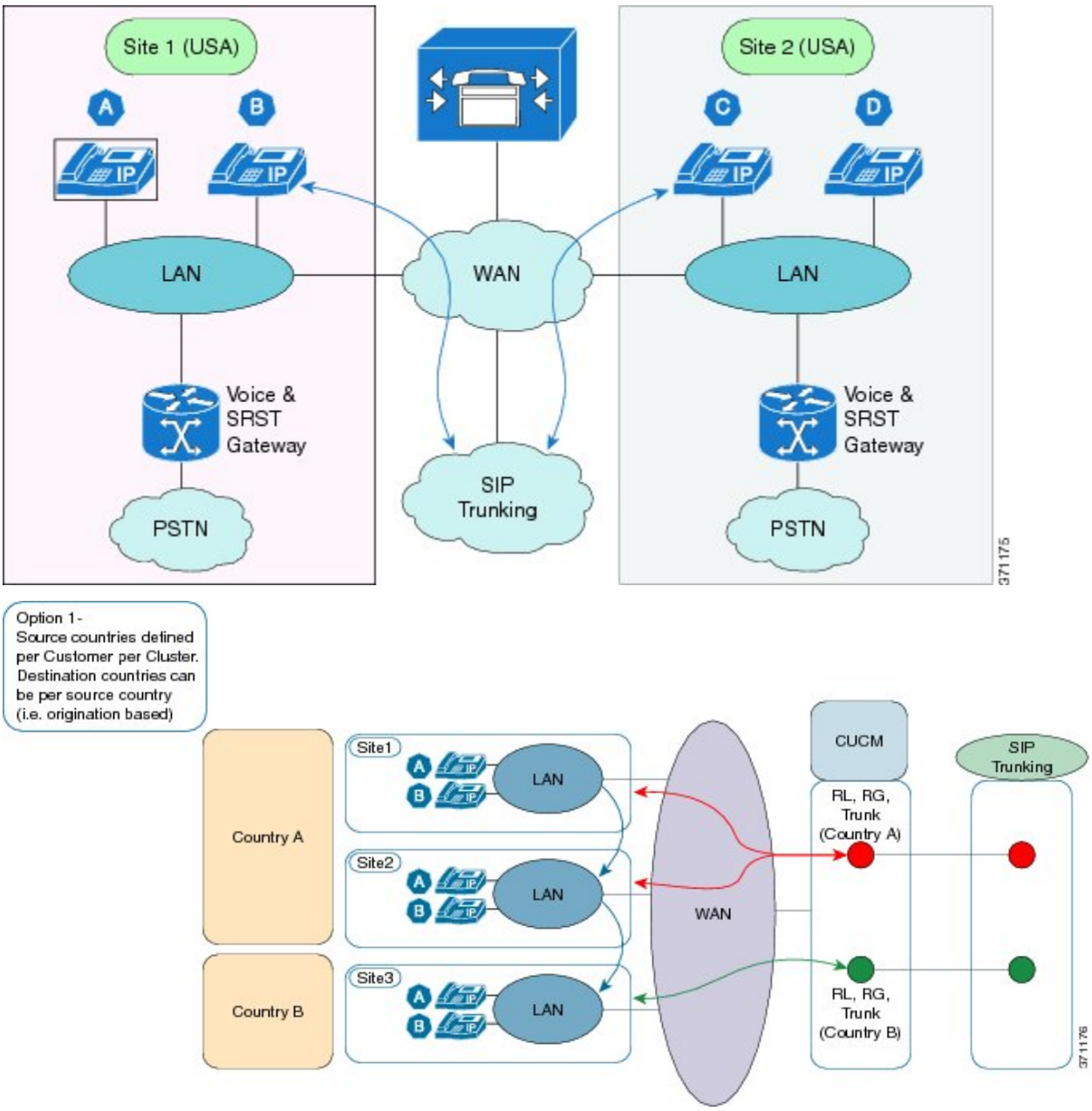
This call type occurs when an endpoint located in a Site in one country wants to reach a destination in any country through Aggregation (Central Breakout). The cluster in which the site is located must have the source country dial plan. Routing is based on the source country. It is not possible for sites 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)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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: – 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: – 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	• 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	• 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Endpoint Types Supported	• Cisco IP phones • Cisco ATA • Cisco VG
Examples	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

4.8.3. VoIP

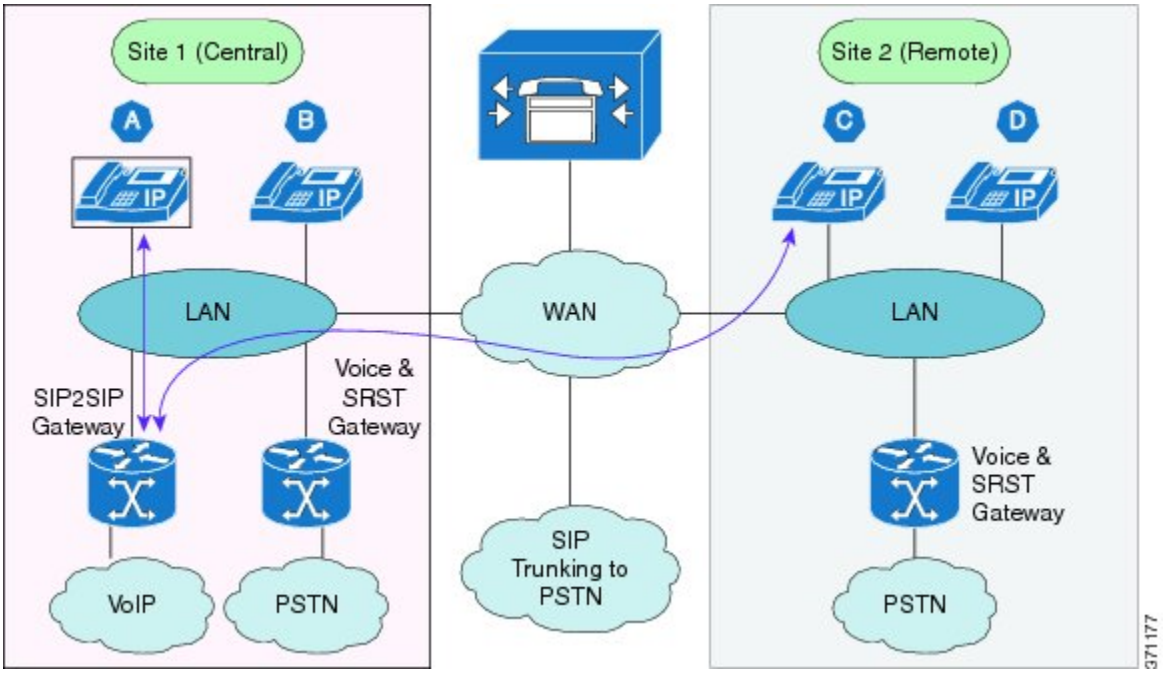
This call type occurs when an endpoint located in a site wants to reach a destination on the PSTN through the Voice over IP (VoIP) provider. The cluster in which the site is located provides the source country dial plan and routing is based on the source country.

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)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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: – 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: – 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	• 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	• 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Redundancy	Available to users without restrictions
Survivability	Not available to users in fallback mode
Endpoint Types Supported	• Cisco IP phones • Cisco ATA • Cisco VG
Examples	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

4.9. Emergency Call Handling

4.9.1. Non-CER Through Aggregation

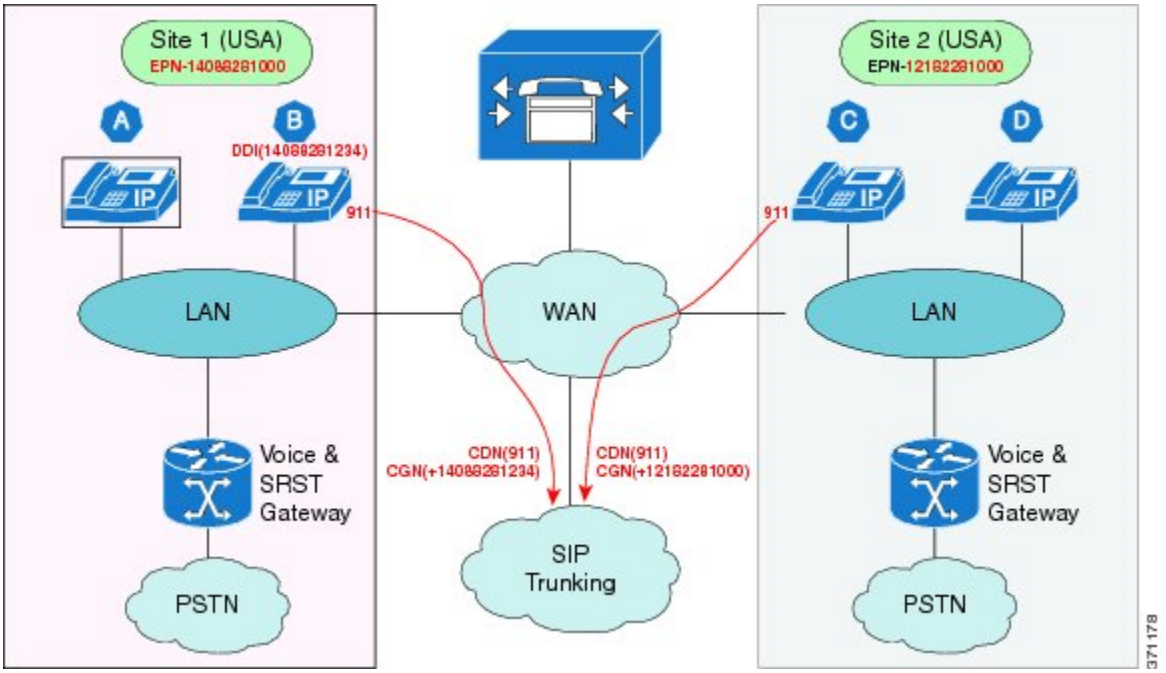
This call type is the standard enhanced emergency call to the Emergency Service Center (for example, US Enhanced 911 or 911). If configured, the call is routed through Aggregation. Emergency Calling is provided, regardless of the Class of Service, as long as the phone is registered.

Non-CER through aggregation includes:

- SIP/SCCP signaling traffic for the endpoint is between the endpoint and Cisco Unified Communications Manager
- SIP signaling traffic for SIP trunking is between the SIP trunking Session Border Controller (SBC) and Cisco Unified Communications Manager
- Media traffic is between the endpoint and SIP trunk SBC

Emergency Call (Non-CER Through Aggregation)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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: – 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 Unified Communications Manager
Usage Example	User can dial any PSTN number from their phone
Default Configuration	• Available to all registered phones • DDI of the DN is sent if available; otherwise, Site Emergency Publish Number is sent
Configuration Choices	• 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	• Cisco IP phones • Cisco ATA • Cisco VG

4.9.2. 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.

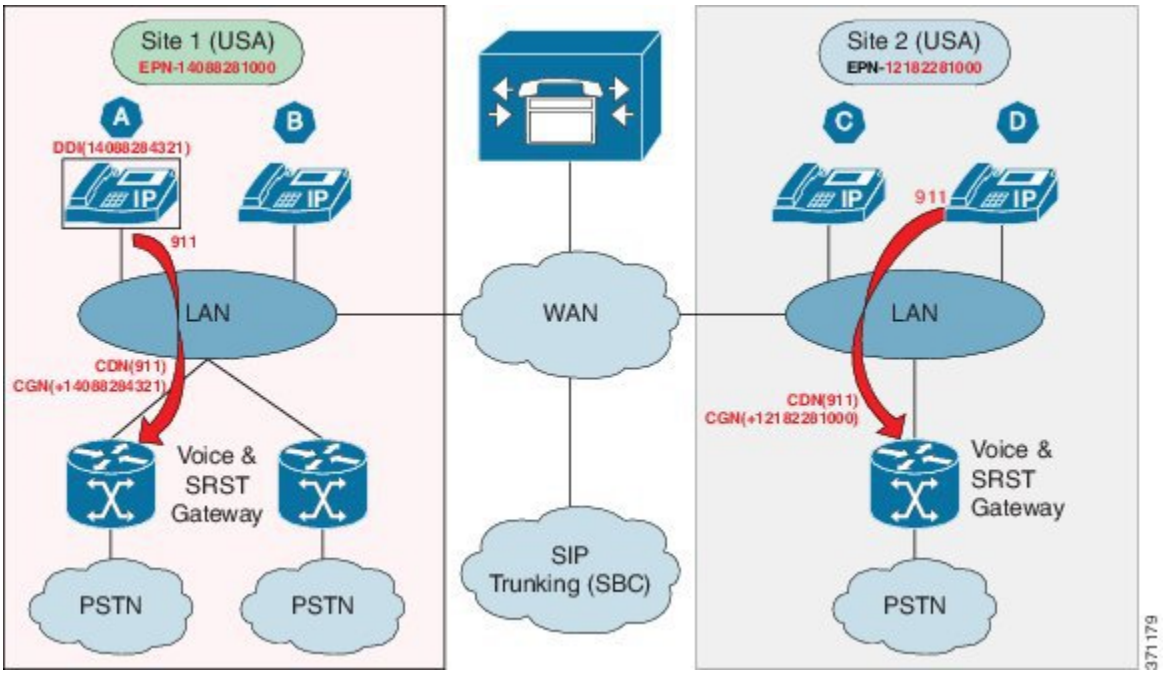
Non-CER through Local Gateway includes:

- SIP/SCCP signaling traffic for the endpoint is between the endpoint and Cisco Unified Communications Manager
- SIP signaling traffic for SIP trunking is between the local gateway and Cisco Unified Communications Manager

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- Media traffic is between the endpoint and SIP trunk SBC

Figure 8. Emergency Call (Non-CER Through Local Gateway)



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Usage	• 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: – 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 Unified Communications Manager
Usage Example	User can dial any PSTN number from their phone
Default Configuration	• Available to all registered phones • DDI of the DN is sent if available; otherwise, Site Emergency Publish Number is sent
Configuration Choices	• 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	• Cisco IP phones • Cisco ATA • Cisco VG

4.9.3. 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 Unified Communications Manager

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- SIP signaling traffic for SIP trunking is between the SIP trunking Session Border Controller (SBC) and Cisco Unified Communications Manager
- Media traffic is between the endpoint and SIP trunk SBC

Usage	• 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: – 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 Unified Communications Manager
Usage Example	User can dial any PSTN number from their phone
Default Configuration	• Available to all registered phones • DDI of the DN is sent if available; otherwise, Site Emergency Publish Number is sent
Configuration Choices	• 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	• Cisco IP phones • Cisco ATA • Cisco VG

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

5 PSTN Call Processing and Routing

5.1. Introduction to PSTN Call Processing and Routing

5.1.1. Introduction to PSTN Call Processing and Routing

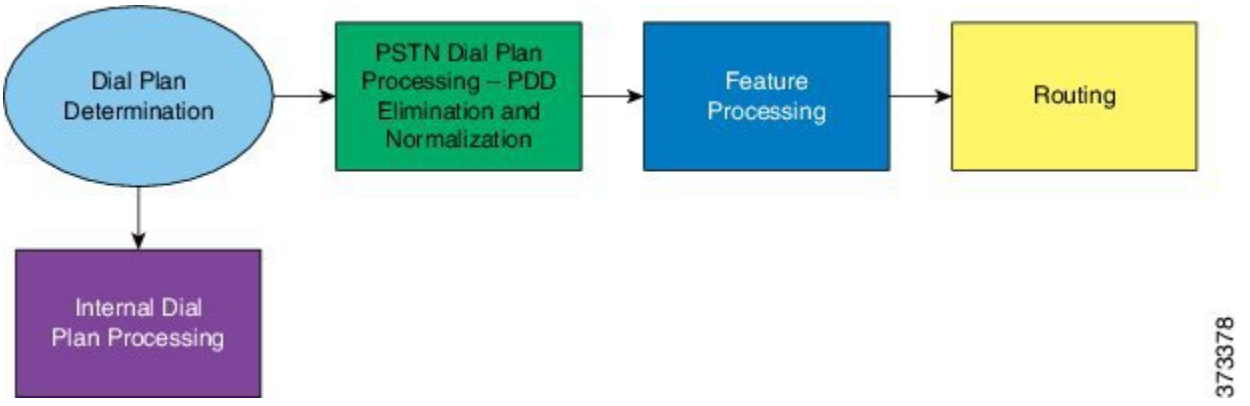
PSTN call processing and routing leverages two VOSS-4-UC 10.x/11.5(x) features:

- 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

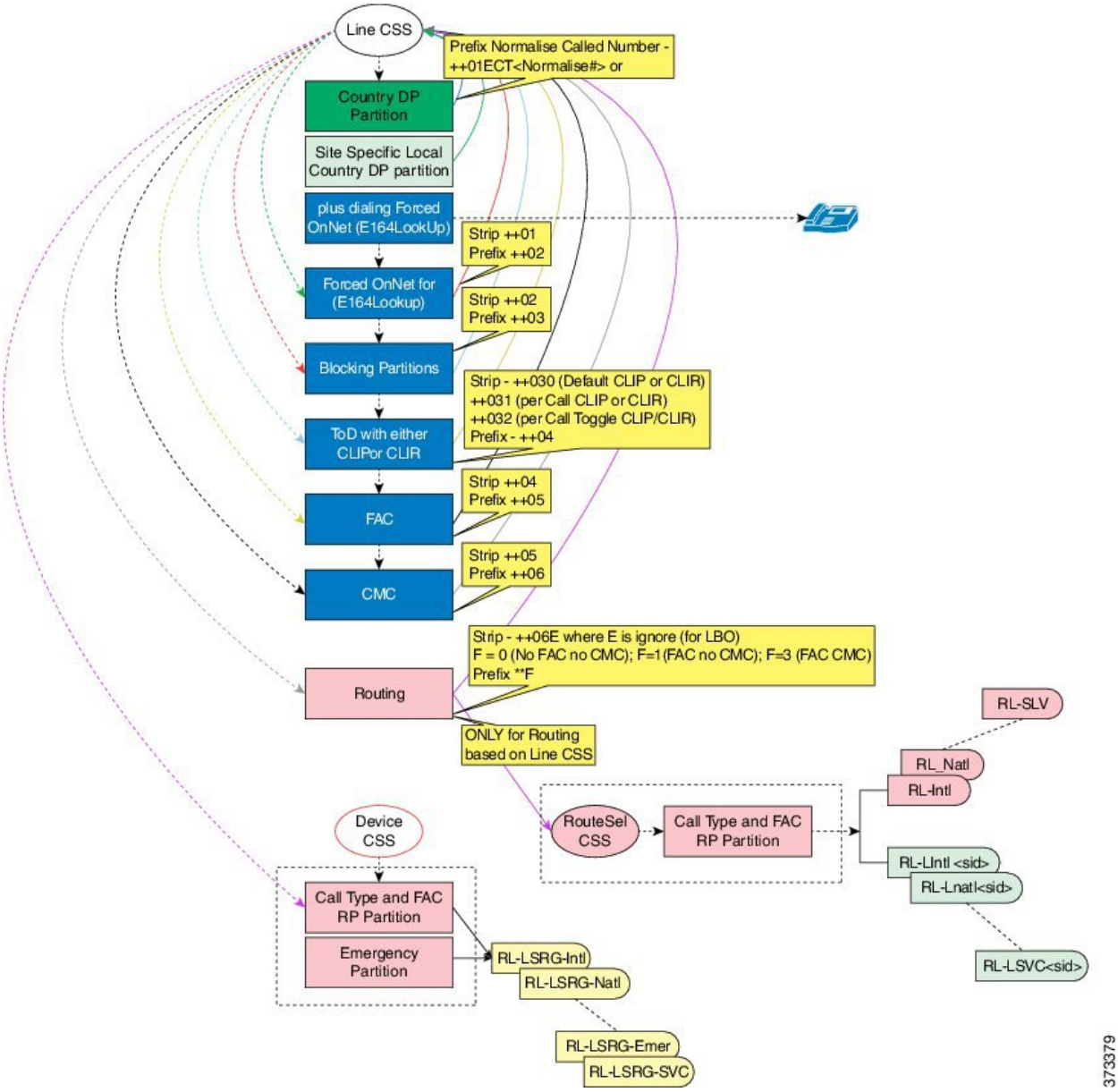


One change from CUCDM 8.1(x) is that features and routing are based on call type rather than dialed number. The biggest advantage of using call type classification is that most features are independent of the country dial plan. Adding a country dial plan defines the dialing behavior patterns, classifying 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



5.2. Dial Plan Determination

5.2.1. Dial Plan Determination

This chapter 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

Dial Plans for VOSS-4-UC 10.x and later are available at Dial Plans.

5.3. Country Dial Plan Deployment

5.3.1. 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 (Subscriber) 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.

5.3.2. Predefined Country Dial Plans

The following predefined country dial plans are shipped with VOSS-4-UC 10.x/11.5(x). However, additional country dial plans or updated versions of country dial plans may be made available between releases.

Dial Plans for VOSS-4-UC 10.x and later are available at Dial Plans.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

5.3.3. Install Country Dial Plan (.template file)

Use this procedure to install 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

4. Review the output from the app template command and confirm that the message Script /opt/platform/admin/home/template_<random_number>/install_script completed successfully appears.

What to Do Next

If installation succeeds, add the new Country Dial Plan to your customer dial plan.

5.3.4. Install Country Dial Plan (.json file)

Use this procedure to install a new Country Dial Plan using a .json file.

1. Log in as hcsadmin administrator.
2. Select **Administration Tools > Import**.
3. Browse to the .json file and select Import.
4. To monitor the status of the import, select **Administration Tools > Transaction**.

What to Do Next

If the import succeeds, add the new Country Dial Plan to your customer dial plan.

5.3.5. Add a Country Dial Plan to a Dial Plan Before Deploying to a Customer

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. Select **Dial Plan Management > Advanced Configuration > 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:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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. Select **Dial Plan Management > Advanced Configuration > 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**.

What to Do Next

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.

5.3.6. Add a Country Dial Plan to a Deployed Customer Dial Plan

Use this procedure to enable another country dial plan for a customer that already has a dial plan deployed.

1. Log in as a provider administrator.
2. Select **Dial Plan Management > Advanced Configuration > 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. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema Group**.
5. Select the schema group currently associated with the customer.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

What to Do Next

Deploy the dial plan on the site that uses the new country dial plans.

5.3.7. Called Party Number As Dialed Feature

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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

- 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 VOSS-4-UC
- 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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. Select **Dial Plan Management > Advanced Configuration > 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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. Select **Dial Plan Management > Advanced Configuration > 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. Select **Device Management > CUCM > 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.!

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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. Select **Device Management > CUCM > 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**.

5.3.8. Plus Number Dialing Customization

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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

	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 Unified CM 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 Unified CM 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. Select **Dial Plan Management > Advanced Configuration > 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. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema**.
3. Click the country dial plan schema you want to modify.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 Unified CM Translation Patterns to Suppress Outside Dial Tone

If pre-11.5.1 country dial plans have been deployed, edit the Cisco Unified CM 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. Select **Device Management > CUCM > 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 check box.
7. Click **Save**.

Edit Cisco Unified CM Translation Patterns to Enable Digit by Digit Dialing

If country dial plans have been deployed, edit the Cisco Unified CM 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. Select **Device Management > CUCM > 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 check box.
7. Click **Save**.

5.3.9. Correct Device Based Routing Class of Service to Enable Single Number Reach

Prior to VOSS-4-UC 11.5, country dial plans were configured with the PreDBRteSel-PT route partition in the site DBRDevice Calling Seach 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 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, and have not done a new install of VOSS-4-UC 11.5, 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

Use this procedure to correct site level Class of Service CSS to enable Single Number Reach.

Do this procedure for each site that you have deployed a site dial plan to.

1. Sign in as a provider administrator.
2. Set the hierarchy path to the site.
3. Select **Device Management > CUCM > Calling Search Spaces**.
4. Click the Cu<CustomerId>-<ISOCountryCode>DP-DBRDevice-CSS calling search space.
5. Click - to remove the Cu<CustomerId>-<ISOCoutnryCode>DP-PreDBRteSet-PT route partition.
6. Click **Save***.
7. Select **Dial Plan Management > Site > Class of Service**.
8. Click a device base routing (DBR) Class of Service CSS.
9. Add the Cu<CustomreId>-<ISOCoutnryCode>DP-PreDBRteSet-PT route partition.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

a. Scroll down to the last route partition.
b. Click + to add a route partition.
c. Set the Index to one more than the last index value.
d. Select Cu<CustomerId>-<ISOCoutnryCode>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

Use this procedure to update site country dial plan schemas to correct the device based routing Class of Service CSS. This correction enables Single Number Reach when the country dial plan is deployed to the customer site. Do this procedure for each affected country dial plan schema.

1. Sign in as a provider administrator.
2. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema**.
3. Click the country site schema HcsGenericSite<ISOCoutnryCode>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. Click - to 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 + next 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**.

5.4. Dial Plans for Caribbean Countries

5.4.1. 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:

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

5.4.2. 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+NXX 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.

5.4.3. 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

5.4.4. 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.

5.4.5. Installing the Dial Plan

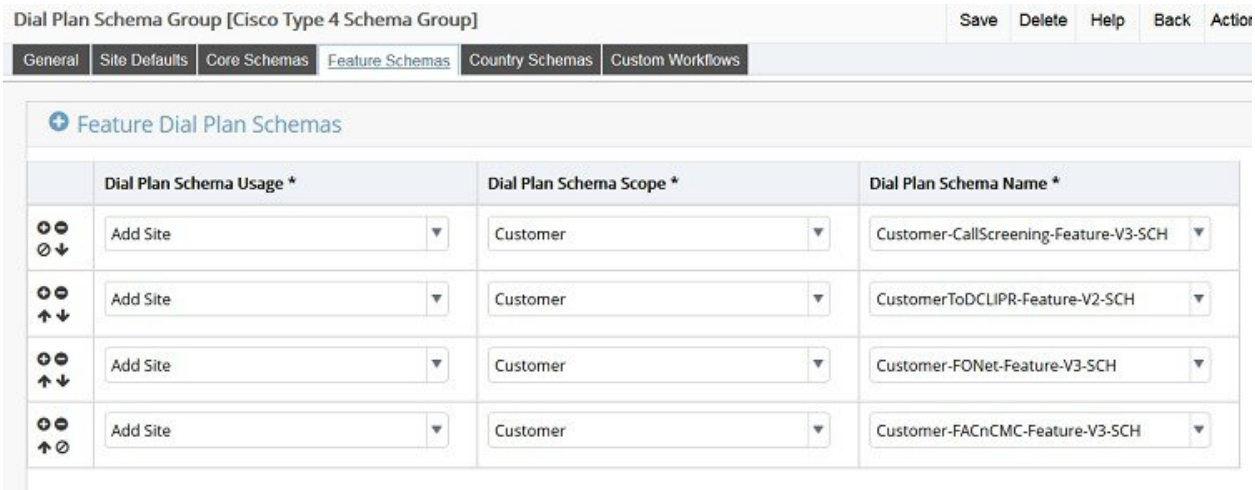
Specify Call Type 12 Feature Schema

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



Specify Site Schema

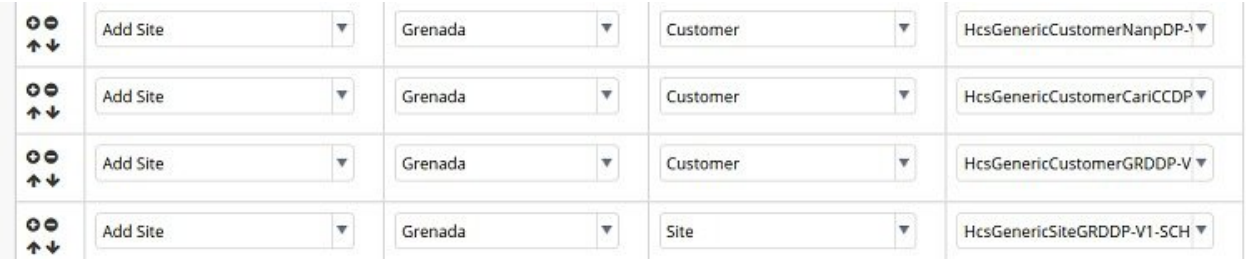
The first time you deploy a Caribbean country, the NanpDP (North American Numbering Plan Dial Plan) schema must be specified. Deploying subsequent Caribbean countries does not require this process.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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 Carribbean countries shown.

Defining the Customer Specific NanpDP Schema and CariCCDP Schema

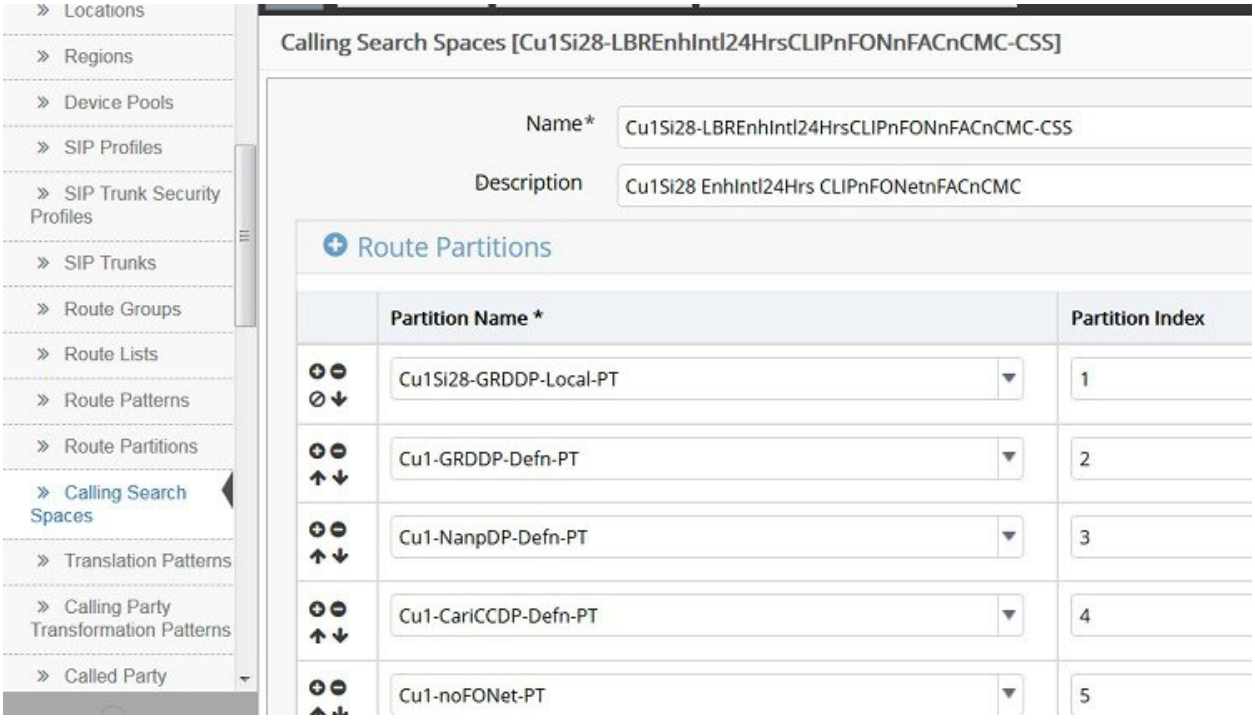


Define Calling Search Spaces

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 Aministrator. For a list of the roles and tasks that can be done at each level, see Roles and Privileges.
2. In **Device Management > CUCM > Calling Search Spaces**, insert **NANPDP Route Partitions** after the country specific Defn PT.

Calling Search Spaces Including NanDP and CariCCDP



Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Route List Required

A new Route List is required if calls to neighboring countries are to be routed over a different trunk group. The create a new Route List see 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.!	DOM Intl Call Type - no FAC no CMC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**012.!	DOM IntlRst Call Type - no FAC no CMC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**101.!	DOM Intl Call Type - FAC no CMC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**201.!	DOM Intl Call Type - CMC no FAC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL
**301.!	DOM Intl Call Type - CMC FAC	Cu1-DOMDP-LBRteSel-PT		Cu1-DOMIntl-RL

5.5. Local Breakout (LBO)

5.5.1. Local Breakout (LBO) Workflows

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. Select **Dial Plan Management > Advanced Configuration > Dial Plan Schema Group**.
3. Select the appropriate schema group that is in use by your customer.
4. Click the **Custom Workflows** tab.
5. Add the following Dial Plan Event to Workflow bindings:
    - associateLboGateway > HcsDefaultAddLBOGatewayPWF
    - unassociateLboGateway > HcsDefaultDelLBOGatewayPWF
6. Click **Save**.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

associateLboGateway Custom Workflow

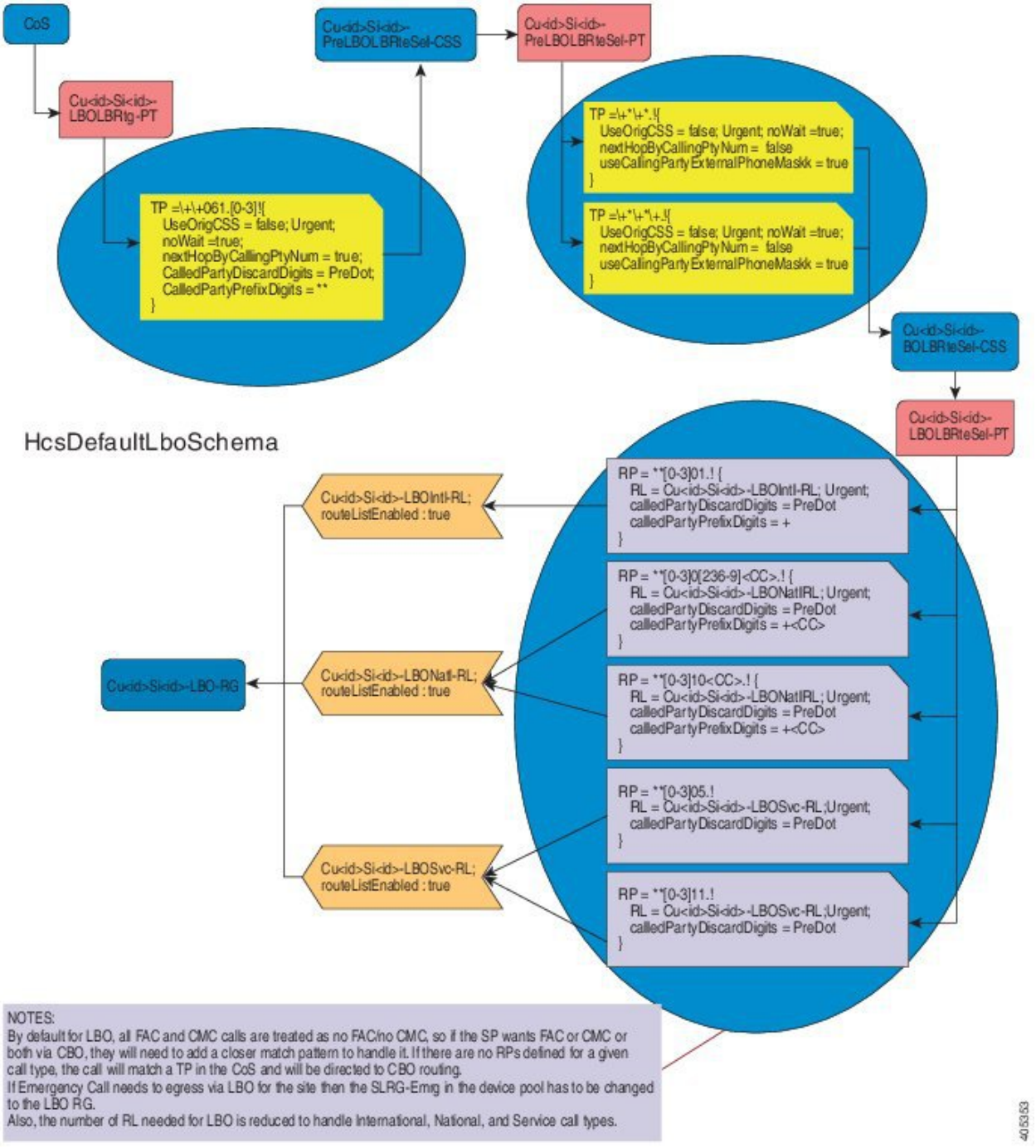
The associateLboGateway custom workflow is optional. If it is not specified in the customer's Dial Plan Schema Group, when a SIP Local Gateway is associated with a site only the IOS Command Builders are triggered.

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 doesnaEUR(TM)t 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



- 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.

unassociateLboGateway Custom Workflow

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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

6 Call Search Spaces and Partitions

6.1. 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. 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>-CGPNTransform-CSS	Per Customer CallinGPartyNumber 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>-CNPNTranform-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>-URILookUp-PT	Per customer partition containing a list of URIs associated to the DN.
Cu<cid>-IngressFromUnity-CSS	Per customer for handling Inbound Call from Cisco Unity Connection	Cu<cid>-ISR-PT	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.

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.

Partitions for Class of Service

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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: • Cu<cid>-BlkIntl-PT • Cu<cid>-BlkNatl-PT • Cu<cid>-BlkMobl-PT • Cu<cid>-BlkLocl-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: • 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: • 24HrsCLIP-PT • 24HrsCLIR-PT • WkHrsCLIP-PT • WkHrsCLIR-PT	This partition is needed to allow calls as described below: • 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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

Partition	Description
7. One of the following: • 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 Unified Communications Manager.
8. One of the following: • 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 Unified Communications Manager.
9. One of the following: • 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: • 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: • Cu<cid>-PreISR-PT per customer PreInterSiteRouting 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

The following are available for configuring Device CSSs.

Device CSSs

Calling Search Space	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.

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

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

  - 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 VOSS-4-UC 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7 Telephony Design and Dial Plan Primer

7.1. Architecture Primer

To understand the Dial Plan Model, you must have a basic understanding of the architecture and the interaction between the elements. The architecture consists of three discrete layers, the aggregation, infrastructure, and customer-premises layers, that comprise the majority of the call flow interactions. The aggregation layer handles inbound/outbound call routing between customer premises and PSTN, while all intracustomer 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

7.1.1. Aggregation Layer

The aggregation layer is responsible for the following:

- E.164 call routing
- Routing E.164 calls between two VOSS-4-UC customers
- Routing calls from the PSTN to IP Lines on Cisco Unified Communications Manager clusters
- Routing calls from IP Lines (on Cisco Unified Communications Manager 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)

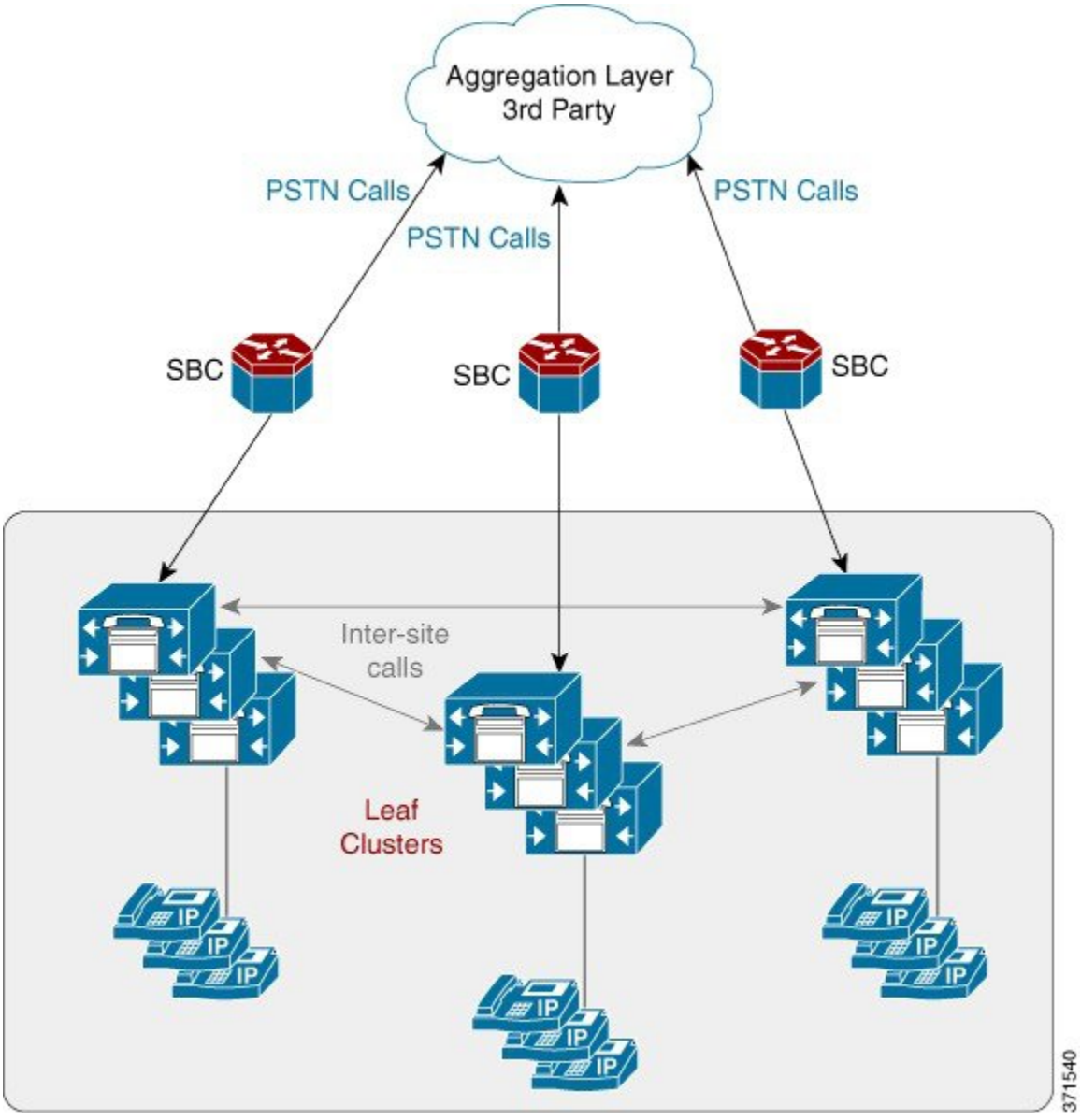
The primary use of the aggregation is to aggregate central PSTN traffic. Any call that is received at the aggregation layer must be treated as a call either from or to the PSTN. The aggregation supports PSTN breakout like SS7 and SIP.

A service provider using VOSS-4-UC 10.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 interoperating with various service provider networks. The SBC is configured manually; it is not provisioned automatically from VOSS-4-UC. 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 Cisco Unified Communications Manager 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7.1.2. 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 Unified Communications Applications as part of the Extender deployment model.

7.1.3. VoiceMail - Cisco Unity Connection

Cisco Unity Connection is connected to the leaf clusters as a SIP connection (telephony integration). For each Cisco Unified IP Phone line that exists on the leaf cluster that requires voicemail, there is also a voice mailbox definition on the Cisco Unity Connection. On Cisco Unity Connection, 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 Cisco Unity Connection. 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 Cisco Unified Communications Manager and Cisco Unity Connection.

7.2. Numbering Plan Design

7.2.1. Directory Numbers

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 Plan Configuration Type	Site Location Code (SLC)	IDP (Inter Site Prefix (ISP))	IDP in DN	Extension Dialing 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)

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7.2.2. 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.

7.2.3. 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. VOSS-4-UC 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).

7.2.4. Full National Number

In VOSS-4-UC and the Dial Plan model, Full National Number (FNN) is a subscriber 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 Unified Communications Manager.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7.2.5. E.164 Number

The dial plan is structured such that the calling and called party numbers for all inbound PSTN calls entering the Unified Communications Manager 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 Unified Communications Manager.

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

7.2.6. 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.

7.2.7. 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.

Copyright © 2020 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

8 Limitations in Cisco Unified Communications Manager

8.1. 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: • 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 Unified CM, 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 Unified CM pattern does not have the capability of that matching letter (dial plan pattern), the call fails. Also, Cisco Unified CM cannot match the dial plan pattern (for example, +*+*) because the calling party number (“+*+*anonymous”) is treated as enbloc by Cisco Unified CM.	Insert a dummy PAI in Cisco Unified CM with a Lua script. • 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

Q