VOSS-4-UC
Provider Core Feature Guide

Release 19.3.3

Mar 18, 2021

Legal Information

Please take careful note of the following legal notices:

Security Information

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

Contents

1 What's New

1.1. Provider Core Feature Guide: Release 19.3.3

- EKB-3923: Add Line Delete functionality for cases where Lines are removed from Devices. See: *Line Delete Preferences*
- EKB-4666: Implement list operation to refresh status and IP address for a list of phones. See: *Configure Phones*
- EKB-5747: Provide control over fields and format of corporate directory display. See: *Phone Services Feature Setup*
- VOSS-618: Add Enhanced Provider and Customer Menu set for Provider Deployments. See: *Best Practices Menus*
- VOSS-687: Provide Extension Mobility Management in BAP Portal (EKB-4500: Add new Device Profile Relation) . See: *Add Subscribers*

  New topic: Extension Mobility management topic added for Business Admin Portal and VOSS-4-UC.
- VOSS-687: Provide Extension Mobility Management in BAP Portal (EKB-4500: Add new Device Profile Relation) . See: *Extension Mobility*

  New topic: Extension Mobility management topic added for Business Admin Portal and VOSS-4-UC.
- VOSS-687: Provide Extension Mobility Management in BAP Portal (EKB-4500: Add new Device Profile Relation) . See: *Standalone Extension Mobility*

  New topic: Extension Mobility management topic added for Business Admin Portal and VOSS-4-UC.
- VOSS-719: Allow Auto Attendant pilot number to be modifiable and optional (EKB-5821: Callhandler: make Pilot number optional) . See: *Add Call Handler (Auto Attendant)*
- VOSS-719: Allow Auto Attendant pilot number to be modifiable and optional (EKB-5821: Callhandler: make Pilot number optional) . See: *Modify a Call Handler (Auto Attendant)*
- VOSS-719: Allow Auto Attendant pilot number to be modifiable and optional (EKB-5720: SysCallhandler: Expose 'Transfer Action' settings (under Transfer Rules tab)) . See: *Modify a Call Handler (Auto Attendant)*

2 Conventions Used in this Guide

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

3 Introduction

3.1. Overview

3.1.1. Workflow: Overview

The major change in the configuration between Cisco Unified Communications Domain Manager from 8.x and VOSS-4-UC is the location of the master data.

In CUCDM 8.x deployments, the master copy of all data was stored in the Shared Data Repository (SDR). Therefore any changes to the data were made in Cisco Unified Communications Domain Manager and then synchronized down to the UC Applications such as Cisco Unified Communications Manager.

In VOSS-4-UC, the source of master data is distributed between VOSS-4-UC and the call manager. A bidirectional sync is used to export and import data from VOSS-4-UC and the applications. This approach enables configuration changes to be made on either the VOSS-4-UC or the UC applications - giving greater flexibility and faster problem resolution.

The following chapters include content on provisioning VOSS-4-UC. Information on the provisioning steps and interactions between VOSS-4-UC and the various UC applications supported by Cisco HCS is included.

Details on User and Subscriber management, including LDAP-related move and push operations, are also available.

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

3.1.2. Supported Browsers

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

Note that:

1. Older versions of each browser may also be compatible.
2. Specific older browser versions that are not compatible with safety and security options such as with “X-Content-Type-Options: nosniff” headers, are not compatible.

OS Browser	Chrome	Edge	Firefox	IE	Safari
Windows 7	80	46	75	N/A	N/A
Windows 10 64 bit	80	46	75	11	N/A
Kubuntu 64 bit	80	N/A	75	N/A	N/A
Mac OS High Sierra	80	N/A	75	N/A	13.1

Internet Explorer 10 and 11 running on Windows 7 require adjustments to the browser's SSL/TLS settings to work:

1. In the browser, choose **Tools > Internet Options**.
2. Click the **Advanced** tab.
3. Scroll to the **Security** heading.
    - For IE 10, locate and select the **Use TLS 1.0** check box, and clear the **Use SSL3** check box if selected.
    - For IE 11, locate and select the **Use TLS 1.0** and **Use TLS 1.2** check boxes.
4. Click **Apply**, then click **OK**.

If TSL1.2 does not work, select the **Use SSL3** and **Use TLS 1.2** check boxes on both IE 10 and IE 11.

3.1.3. Cisco Compatibility Matrix

For this Release, testing was performed using the following Cisco UC apps versions.

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

UC App	Versions
CUCM	10.5.2.17900-13, 11.5.1.16900-16, 12.5.1.12900-115
CUC	10.5.2.17900-13, 11.5.1.16900-16, 12.5.1.12900-56
HCMF	11.5.4.11900-3, 11.5.5.10000-2, 12.5.1.12900-4

3.1.4. GUI Accessibility

VOSS-4-UC provides a basic level of compliance to WS3 accessibility standards by conforming to the core standards required to navigate the GUI. This ensures that VOSS-4-UC content is accessible and more usable in general to people with certain disabilities. Functions to help with disability, including people who may not be able to use a mouse or who have visual impairments, include:

- Title display in the browser

  When choosing a menu option in the GUI, the selected menu option title is also displayed in the browser tab. This helps users know where they are and also helps them move between pages open in their browser.

- Images have alternative text

  Images on buttons that perform a function have additional alternative text, which is used by people who cannot see the image. This alternative text is displayed when the mouse pointer hovers over an image.

People who are blind and use screen readers can hear the alternative text read out; and people who have turned off images to speed download or save bandwidth can see the alternative text.

- All headings given a meaningful hierarchy to ease navigation

  Web pages often have sections of information separated by visual headings. Each page typically has at least one heading. When there is more than one heading on a page, the headings have a hierarchy, which makes it easier for the user to navigate to a particular heading and to navigate between headings.

- Contrast ratio can be changed

  While some people need high contrast, for others, including people with some types of reading disabilities such as dyslexia, bright colors (high luminance) are not readable. They need low luminance. A Chrome plugin can be installed (on the Chrome browser), which allows the user to change the default colors on a page.

- Zoom capability

  VOSS-4-UC supports zooming without losing any information or functionality.

- Keyboard access and alternative visual focus

  Many people cannot use a mouse and rely on the keyboard to interact with the Web. People who are blind and some sighted people with mobility impairments rely on the keyboard or on assistive technologies and strategies that rely on keyboard commands, such as voice input.

  In a browser that supports keyboard navigation with the Tab key (for example, Firefox, IE, Chrome, and Safari):

  1. Click in the address bar, then put your mouse aside and do not use it.
  2. Press the 'Tab' key to move through the elements on the page.
  3. To move within elements such as select boxes or menu bars, press the arrow keys.
  4. To select a specific item within an element such as a drop-down list, press the Enter key or Spacebar.

3.2. Accessing the Admin GUI

3.2.1. How to Access the Admin GUI

Note: To access the Beta Admin GUI, log in to the standard GUI as below and the choose the *Preview the new portal! (Beta)* link at the top of the interface.

Standard Users

Log in with the URL: `https://{hostname}/login`

The username can be entered in either of the following formats:

`{username}@hierarchy` or `{email address}`

See *Standard Users and Login* for more details.

LDAP Users

Log in with the URL: `https://{hostname}/login`

Regardless of the login Attribute Name specified in the LDAP network connection, the user email address can be used to log in.

When logging in with LDAP credentials, the username is in the format:

`{user ID}[@hierarchy]`

See *LDAP Users and Login* for more details.

SSO Users

Log in with the URL: `https://{host name}/sso/{SSO login URI}/login`

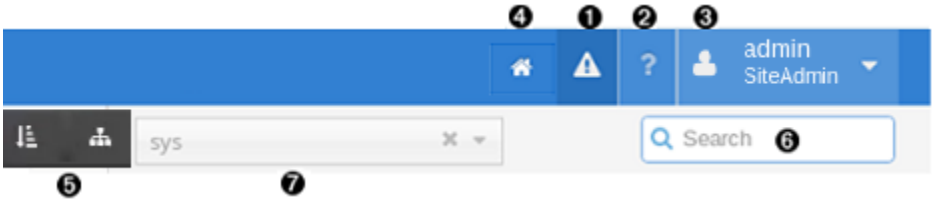
Use the relevant SSO identity provider credentials.

See *SSO Users and Login* for more details.

3.3. User Interface

3.3.1. Administrator User Interface

The main user interface presents a Menu bar with information and controls:



1. Notifications indicator with a menu to access the Transaction log and Alerts, if alerts have been enabled for the administrator. A pop-up displays when a transaction is done. The pop-up notification can be closed and the **Notifications** button can be clicked to inspect transactions.

   Alert notifications are removed when all alerts have been removed from the Alert list.

2. On-line help button to open Help in a new browser tab.
3. Display of the logged in username and role with **Logout** and **Change Password** menu items.

   Note that **Logout** and **Change Password** menu items are not available for SSO users. For detailed information about logging out from an identity provider (IdP) initiated session, see the relevant user documentation for the specific identity provider.

4. A customizable landing page and a Home navigation button to return to it. Refer to “Create a Landing Page” for more details.
   - If a user logs in for the first time, a message is shown below the welcome header of the landing page: “This is the first time that you are logging in with this account”.
   - If the user that logs in is not a SSO or LDAP user, a message is also shown below the welcome header of the landing page that indicates either no unsuccessful login attempts, or else the number of unsuccessful login attempts by the user since the last successful login.

The message is of the format:

"There have been 2 failed login attempt(s) since you last successful login on Oct 4, 2016 11:10:14 AM"

If login details cannot be retrieved, a message will show:

"We were unable to retrieve the number of failed login attempts or last successful login. Please log out and log back in. If this message persists, please contact an administrator".

For SSO or LDAP users, only the last successful login time is displayed.

5. Hierarchy tree view and pop-up buttons to display the tree or list of and available nodes. For details, see: *Navigating the Hierarchy*.
6. Search input box.
7. Hierarchy element, which displays the highest hierarchy level. The associated child hierarchy element is displayed in a similar field display box next to the main hierarchy element. If there is more than one level or node at a specific hierarchy, you can search and navigate the hierarchy. See *Navigating the Hierarchy*.

When using the application, you are presented with forms and lists.

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

The list of controls and buttons is described in the section on GUI controls.

A **Cached** slide-out notification on the right hand side of the interface shows when the locally cached data of a resource is used. This slide-out notification can be minimized to a narrow bar on the side of the screen.

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

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

Note: Since VOSS-4-UC sessions are cookie based, it is possible to share the same session across different tabs or windows of the same browser. However, it is not possible to have different authentication sessions in different tabs. In other words, login as different users in different browser tabs is not supported.

3.3.2. User Interface Controls

The main controls used in the administrator user interface are described below.

Button Bar

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

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

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

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

List View Action	Description
Export	From search results or any list view in the system, it is possible to select the entities required and export them with all attributes. The selected data can be exported to: • A JSON file that is archived into .json.zip format for external use. • Excel - an export containing data and Excel columns for all fields as shown in the JSON export format. • Excel(formatted) - an export containing data and Excel columns as arranged by any Field Display Policies that apply.
Export Bulk Load Template	Export a model structure to a MS Excel bulk load file format. The file can be used as a template to bulk load instances of the model. Refer to the Bulk Load topic help.
Field Display Policy	Add a Field Display policy to a selected model. The detail view of a Transaction displays this button to show sub-transactions.
Move	For selected model instances, move them from the current hierarchy to another hierarchy. By default only device models have a **Move** button, which is available on list and instance GUI screens. When moving device models, checks are built in to disallow moving a device model instance to a hierarchy node with a different device. For Data Models, Move is allowed by editing the Data Model's definition in the Operations section.
Clone	Make a copy of the current item. An option is available to rename the copied item.
Execute	For an executable model such as a Provisioning Workflow, Macro, Wizard or for a script, run the execution.
Import	For supported Network Devices, carry out an import of data from the device.
Export	Export a specific item with all its attributes.
Package	Create a package containing selected search results.
Refresh	Click this button on the Transaction list to refresh the list of transactions. This would for example update the Progress of the transaction.
Replay	Transactions that have failed can, under certain circumstances, be replayed. This means that the transaction is re-submitted with the original request parameters.
Edit and Replay	Available for completed transactions. Similar to the **Replay** button, but allows you to first make changes to the previously submitted form before the transaction is resubmitted.
Reset Phone	Reset a phone.
Return	Return - From the detail display of a selected instance of a model, select this button to return to the list display of the model instances.
Tag	For a selected model instance, add a tag to it.
Tag Version	For a selected model instance, add a version tag to it.
Test Connection	For instances of models representing connection parameters such as connections to devices, click the button to test the connection.
Visualize	Deprecated.

On-line Help

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

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

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

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

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

Main Page Controls

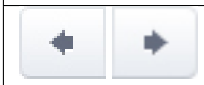
The following controls are available from the main GUI.

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

Form Controls

The following controls are available from a form.

Icon	Description
	Open another instance of the current form field or open a pop-up screen to add an item.
	Delete the current instance of a field from a form or open a pop-up screen to confirm.
	Move the selected instance on a form down in the order of field entries. In the case where a Position field is available, for example for Lines, the entered value determines the order in the object.
	Move the selected instance on a form up in the order of field entries. In the case where a Position field is available, for example for Lines, the entered value determines the order in the object.

Icon	Description
	On multi-tabbed forms, navigate to the previous or next tab.
	A warning icon, for example if a mandatory field is not filled in.
*	Next to an input control on a form, the asterisk indicates that the field is mandatory.
[Browse]	Next to an input control on a form, a button to open a file selection dialog.
[V]	Drop-down input box. Typing into the box filters the drop-down list choices.

About

The About option on the menu provides version information such as:

- Version
- Software Version
- Platform Version
- Build Time

3.3.3. Common Tasks

The user interface allows administrators to perform common tasks using various menu paths and form controls (see below).

Cloning Items

Certain items, such as roles, credential policies, devices, phones, and so on can be cloned. Cloning provides a quick way to create new items that have very similar data to the cloned item.

On the GUI, a **Clone** option is available from the **Action** button on the button bar to carry out the task. This is available on the specific item page of certain items, and not on the list view.

The cloned item is created in the system only after the user clicks **Save** on the button bar.

If an item refers to other items, only the current item is cloned, and not the referenced items. For example, if a Phone on the system is cloned, the device models (Phone and Remote Destination) that are referred to in this item are not cloned.

The cloned key field(s), for example **Name**, must be edited with new values to ensure creation of a new item in the system. An error message, “Error, Duplicate Resource Found.” is displayed if a key field is not changed.

How to Clone an Item

1. Choose the hierarchy level of the item to be cloned.
2. Choose the required item that you want to clone.
3. Click **Action > Clone** on the button bar.
4. The page refreshes and the form displays the cloned item.
5. Edit the required details, and click **Save** on the button bar when complete to create the new item.

Selecting Items

Items that have already been created can be deleted or modified as required. This can be performed either on single items or multiple items.

1. For a single item in the list view, click the required single item that you want to delete or modify.
2. For multiple items in the list view, select the check box for each item that you want to delete or modify. If the list view of items spans more than one page, items can be selected on each page as required.
3. Click a button on the button bar or select a menu item from the **Action** drop-down to carry out the task on the selected items, where relevant.

Note:

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

Bulk Delete and Modify

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

If your administrator has given you the required permissions, you can also bulk modify certain items, for example Roles. Select the check boxes of the items you want to modify and choose **Bulk Modify** from the **Action** drop-down. The input form for the item is opened. Values entered on this form are modified for all selected items when you choose **Bulk Modify** from the **Action** drop-down.

Ordering Lists

The list view of items allows for basic ordering by column.

1. Click in the column header of a list. String columns are sorted alphabetically and numeric columns are sorted numerically.
2. Click the column header name or up/down arrow to change the direction or the sort order of the column.

The ordering of a column is shown by the up/down arrow.

Note:

- When sorting, a blank value appears as if the value was “None” in terms of alphabetical order.
- With no filter applied, sort will work on any column in the list view.
- With a filter applied to a single column, sort will work on the filtered column only.
- With a filter applied to more than one column, the sort functionality will not work.
- Leading spaces on a field in the list view are dropped when rendering the list view, so this may affect the sort order.

Filtering Lists

VOSS-4-UC allows you to filter lists in order to view only data based on specific criteria. This includes Transactions and their Sub Transaction and Log lists. For transactions, refer to *Filtering Transactions*.

A **Filter** button is available next to the **Items**/**Page** drop-down at the bottom of a list. A filter icon (with the same functionality) is also available next to each column on which you can filter. This is only visible when you mouse hover on the column headings. The **Filter** button on each page defaults to the first column on the page, whereas the filter icon next to the column defaults to that specific column. Click the button (or icon) to open the multi filter dialog.

A filter instance consists of a selected column, a filter operator and a value. Available filter operators are:

- Contains
- Does Not Contain
- Starts With
- Ends With
- Equals
- Not Equal

Note:

- The Contains filter operator and the **Ignore Case** check box = Selected, are applied by default. Add more filter fields as required.
- The sorting of columns (ascending or descending) by clicking column headers while a filter is applied, is only supported for the Starts With operator.
- To filter for rows with no value in a selected Column, choose any Filter Type option, select the **Ignore Case** check box and type `None` in the Value. This works for all list views except Subscriber
- The **Located At** column will only filter on the actual hierarchy name and not the displayed text next to it, for example “site”, “customer”, and so on.

Filter instance rows can be added or removed on the dialog to create a filter. The combination of instances create a single filter where *all* instance rows are applied, in other words, in a logical AND.

String values are case sensitive, unless the **Ignore Case** check box is selected. All the filter operators apply to strings.

For Boolean values in a column, the filter is applied using any filter operators, but only with values “True”, “true”, “False” or “false”.

Number values in a column also use Equals and Not Equal filter operators. For floating point values, at least one decimal digit is required for filtering, for example `2.0`. Filtering can be applied to values with decimal values up to 7 decimals. For example, consider a list of values:

```
2.2000001
2.0000001
2.00000001
```

The filter: Not Equal to `2.00000001` displays only one value (`2.2000001`), because the filter value has more than 7 decimals.

To apply the filter, press **Enter** or click the **Apply** button. This will hide the active filter dialog and show the filtered list. An **X** button shows next to the active **Filter** button.

For model lists, actions can then for example be carried out on a selection of items from the filtered list. The filter remains active until it is removed or until the user session on the GUI ends.

For all types of filters, the **Filter** button funnel icon is black when a filter is active, and white when no filter is present.

A funnel icon also shows in the list header to indicate that a filter is active and that the list is currently filtered. An **X** button shows next to the active **Filter** button.

If a filter is active on a list, click the **Filter** button to display the multi filter dialog again.

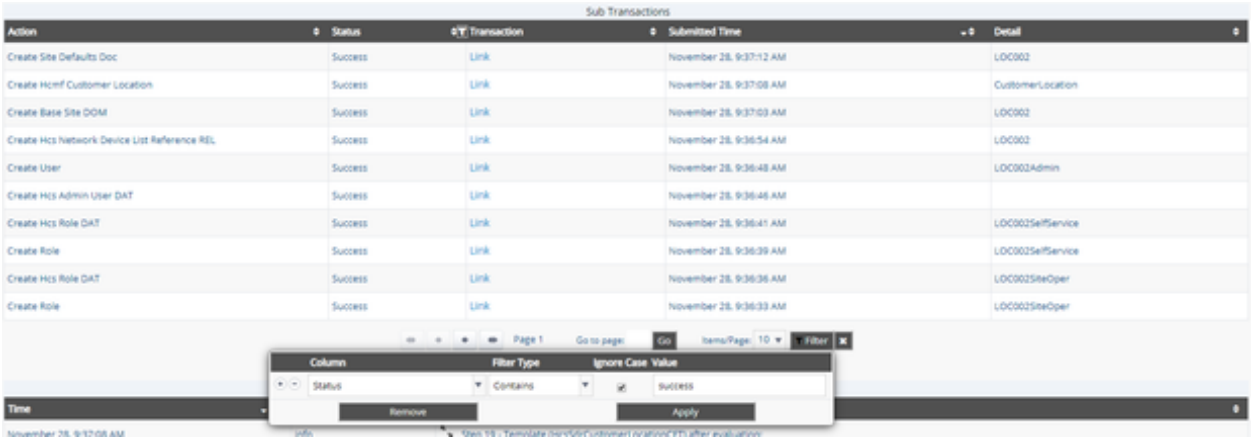
Close an unapplied filter dialog by clicking outside it. Unapplied filters are lost when the dialog is closed.

A filter remains active even when navigating away from the list. More than one filter can therefore be active on lists available in a session on the GUI.

Remove an active filter by clicking the **Remove** button on the multi filter dialog or by clicking the **X** button next to the active **Filter** button.

Important: Standard list view filters on model types will be removed and replaced by any Configurable Filters on landing page links or menu items for the corresponding model type when these are used. See: *Configurable Filters in Menus and Landing Pages*.

A filter example is shown in the figure below.



Navigating Lists

If a list contains multiple items, page navigation controls at the bottom, center of the screen allow you to:

- scroll to the next/previous page using the right/left arrow respectively.
- scroll to the first or last page of the list as required.
- Go to a specific page by entering the required page number and clicking **Go** (or pressing **Enter**).
- Specify the number of items to display on a page, 25 to 2000.
- If you are unsure of the total number of items in a particular list view, click the **Get total** button or on the last page, the **Update total** button.

For drop-down lists and transfer boxes with more than 200 items, the bottom of the list shows an item called “More choices” that can be selected to show the next items. A subsequent list will also have an item “Previous choices” at the top to navigate back through the list.

Note: Search result lists are limited to a maximum of 1,000 items. A message will show at the bottom of the list pages to indicate this. Use a more specific search query for result lists of more than 1,000 items.

Updating on Pop-up Screens

User interface forms that open pop-up screens to add or delete items carry out the Add or Delete task when the **OK** button is clicked on the pop-up screen. In these instances, you do not have to click the **Save** button on the parent user interface form to complete the task.

3.3.4. Search in a Drop-Down List

Overview

The existing search results (using 'Contains' search criteria) on a drop-down is limited to a maximum of 1000 items.

A new paginated, drop-down pop-up form is now available that allows a user to search and paginate through the list search results (using 'Starts with' search criteria) in order to select a specific item. This is particularly useful when search results in a drop-down exceed 1000 items, or if you require a more granular search capability.

The new pop-up form is available on various forms such as; Add or Modify Subscriber, Line Search, Reset UC Password, and so on.

Using the Drop-Down Search

The drop-down search capability works the same on all forms.

The following example illustrates use when searching for and adding a **Line** for a **Directory Number**:

1. Click the **Search** icon next to the **Directory Number** drop-down list ( ).
2. A pop-up table opens displaying all directory numbers at the selected hierarchy. Multiple pages may be presented depending on the quantity of directory numbers.
3. Search for, and then select the required Directory Number.
   - Click '<' or '>' to scroll through the pages.
   - Enter a value in the **Filter (starts with)** text box. The pop-up form filters the form results on the entered text.

Note: You can also enter a new **Directory Number** in the **Filter (starts with)** text box.

3.4. Search

3.4.1. Search: Overview

A search input box is always available to allow the user to search quickly for items. The default search context is across all components on the system that the user has permission to view as specified in their Access Profile, with the caveats on number of items, relations and device models listed below.

For a simple, entered string, the search matches the start of the text of a component.

Note:

- Search result lists are limited to a maximum of 1,000 items. A message will show at the bottom of the list pages to indicate this. Use a more specific search query for result lists of more than 1,000 items.
- Simple search strings will match values in data and device models (relations instances will not be returned). To search the relation model instances, specify the model as a part of the query - refer to the search syntax.
- Selecting a data or device model instance returned in a search will display the full model details, in other words, without a Field Display Policy applied.

Carry Out a Search

1. Choose a hierarchy from which to carry out the search.
2. Enter a search string (using the search syntax) in the **Search** text box (located above the button bar). By default, sub-string matches of the string will be searched for. This means that a search for “Site” will also show “Site2” in the result list.
3. Press **Enter** on the keyboard. Search results are shown in the list view.

Perform an Action on the Search Result Set

To perform an action on the search result set:

Click an entry in the list view to open the result instance, or select a specific check box and click one of the buttons on the button bar, such as **Delete**, or select one of the options from the **Action** drop-down, such as **Export** or **Tag** to carry out the associated task. The buttons and options available are dependent on the access profile of the user performing the search.

To select multiple entries, select all the relevant check boxes.

3.4.2. Search Syntax

The query input box can be used to construct a search query. This section describes the syntax of a search query.

Search queries can contain:

- Model type and model name references
- Model attribute and nested model attribute references
- Key words
- Brackets for grouping

- Query string to search for

  Valid query string characters are:

  - alphanumeric characters
  - !@#$%^&*-_=+<,.>/?|[{]}~‘
  - to search for single quote in a string, wrap the string in double quotes
  - to search for double quote in a string, wrap the string in single quotes

Since a search query is carried out on models, the specific model type and model name can be specified in the query.

The query format is indicated below:

`type/name` is the syntax for a full reference to a model type (for example relation, data, or device) and model name (for example Countries).

A number of keywords are available to construct a search query.

Keyword Types

Three types of keywords are available:

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

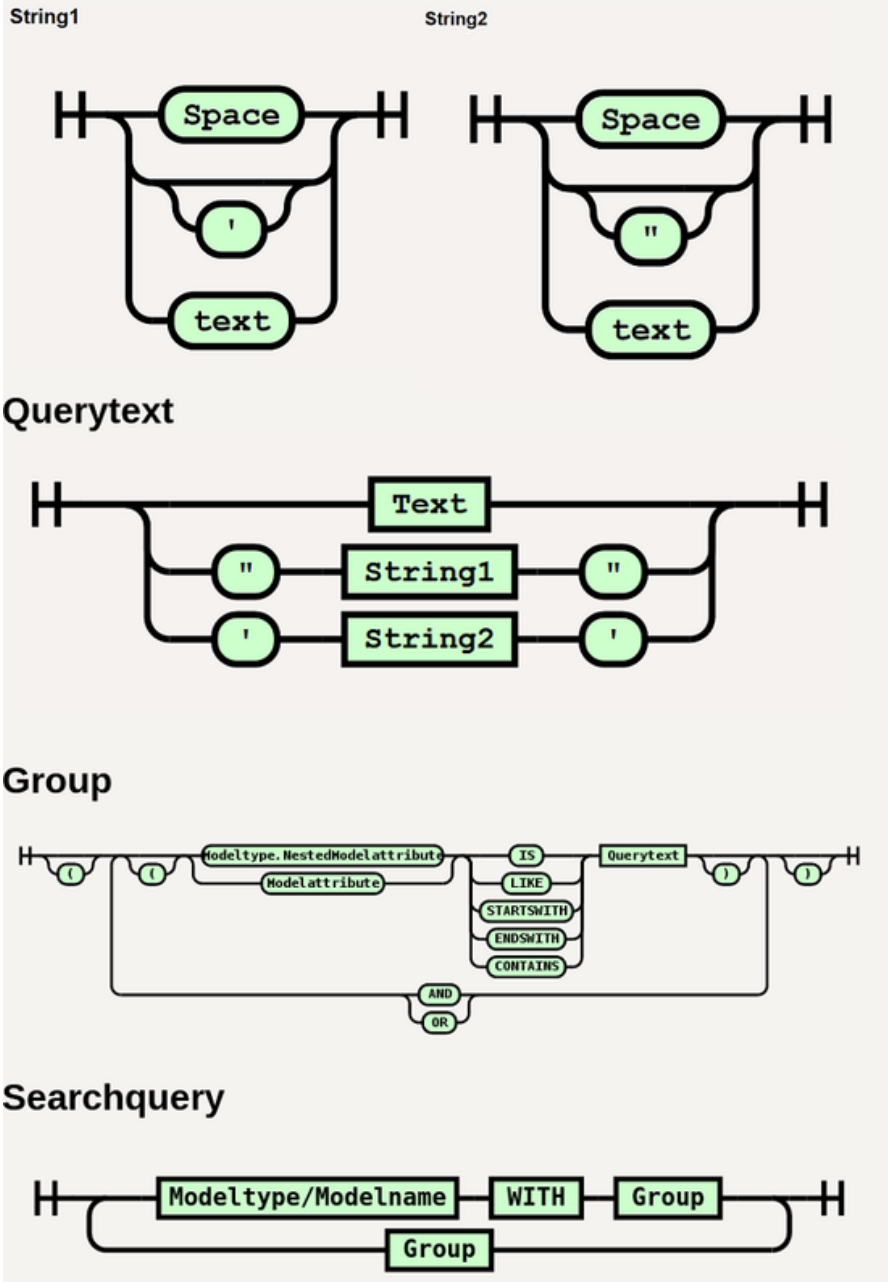
Keyword	Description and Examples
WITH	Restricts the search to look for only specific data types. In the example below we have specified the data type Countries and so only countries will be returned. `((data/Countries WITH country_name LIKE Kingdom) AND (data/Countries WITH country_name LIKE Unite ))`

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

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

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

Search Syntax Diagrams



Search Examples

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

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

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

The following query *will not* yield results:

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

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

Example Queries (line breaks added):

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

Search String Format

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

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

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

Case sensitivity Use the appropriate operator (LIKE)

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

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

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

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

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

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

  `data/CallManager WITH pkid IS 55c32b59a6165451e04f392a`

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

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

3.4.3. Searchable Fields

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

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

4 Configuration

4.1. Fulfillment Procedures Overview

The primary objective of using VOSS-4-UC is to easily onboard Customers and End Users with Collaboration Services. The fulfillment procedures to achieve this objective may involve administrators at the provider, reseller, customer and site levels of the hierarchy.

The following section shows a sample procedure for configuring VOSS-4-UC.

4.2. Example Fulfillment Procedures

The following is an example set of steps for onboarding customers and users. Customization and some optional configuration is not included in this example.

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

Shared applications are configured at the Provider or Reseller level. Dedicated applications at the Customer level.

4.2.1. Before You Begin

HCM-F and any UC Applications to be used for provisioning customer sites and users must be installed and ready.

For WebEx Cloud, the necessary licenses and accounts must be available for provisioning.

4.2.2. Procedure

1. *Create the HCM-F Device*.
2. *Create a Provider*.
3. Optionally, *Create a Reseller*
4. *Create a Customer* at the appropriate Provider or Reseller hierarchy level.
5. *Set Up Cisco Unified Communications Manager Servers*
6. Optionally, configure WebEx and UC applications at the appropriate hierarchy level:

   a. *Set Up Cisco WebEx*.
   b. *Set up Cisco Unity Connection*.
   c. *Set Up IM and Presence Service Servers*.
7. *Configure a Network Device List*.
8. *Create a Site*.
9. *Modify Site Defaults*.
10. *Create a Customer Dial Plan* and *Create a Site Dial Plan* as described under Dial Plan Management.
11. Configure Northbound Notification if desired as described under “Set Up Northbound Notification”.
12. *Set up an LDAP Server*.
13. *Define a Filter*.
14. *Set up LDAP for User Synchronization*.
15. *Move Users*.
16. *Manual User Push to Cisco Unified CM*.
17. Perform end-user Collaboration Service provisioning as described under *Add Subscribers*.

4.3. Roles

The system has a powerful Role Based Access framework that ties a User Role to Menu Layouts, Access Profiles, Landing Pages, and Themes. The system comes with a default set of Roles, Menu Layouts, Access Profiles, Landing Pages, and Themes. The default set of roles in the system is HCS Admin, Provider, Reseller, Customer, Site, and User.

For information about adding or modifying roles, see *Role Management*.

4.4. Unicode Limitations

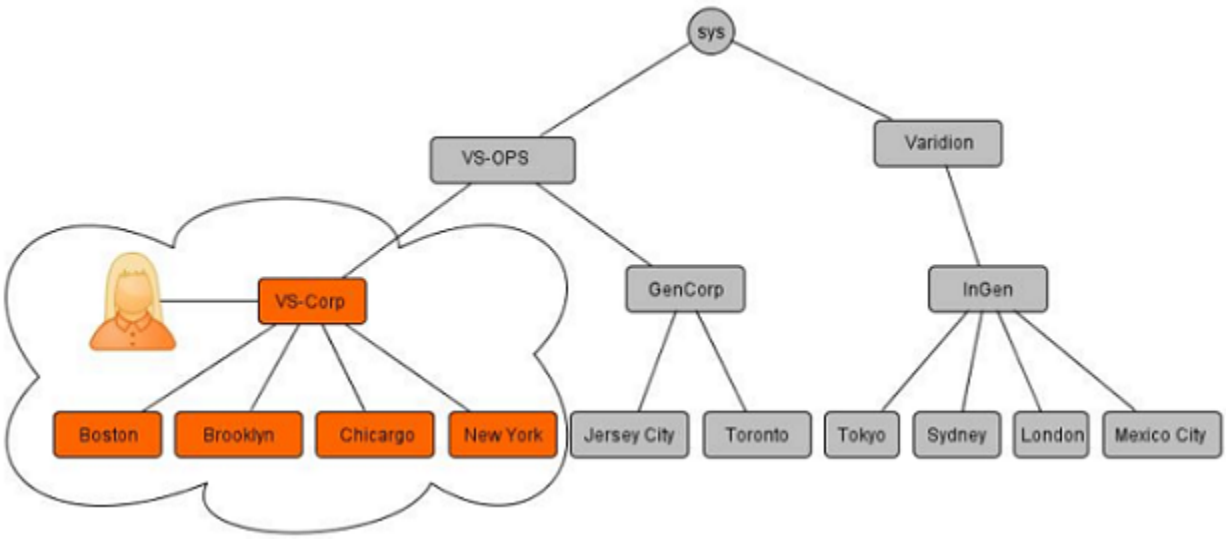
For VOSS-4-UC, Unicode characters are supported only in the following fields:

- User Information in VOSS-4-UC User Management
- Description
- Contact Information (Address, City, State, Postal Code, Country, Extended Name, External Customer ID, Account ID, and Deal IDs)
- Phone Label

5 Hierarchy Management

5.1. Data Partitioning

Data in the multi-tenant system is “partitioned” by a means of fully configurable hierarchy nodes. In the example below, the system hosts two managed service providers “Varidion” and “VS-OPS”. “VS-OPS” hosts two customers: “VS-Corp” and “GenCorp”. “VS-CORP” in turn operates from locations Boston, Brooklyn, Chicago and New York.



The system has the ability to model the hierarchical nature of various businesses and manage the allocation of infrastructure (such as network devices - refer to the topic on Network Device Allocation and Bundling.), users and other entities in the system by creating hierarchy nodes, hierarchy node types (for example: provider, reseller, customer, shared building, site, division, branch, and so on) and hierarchy rules (for example: a site can only be created under a customer) that can be applied to various models in the system.

Devolved administration is enabled by creating administrators with different roles for different types of hierarchy nodes. For example:

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

- Physical locations hold users and phones.
- End users consume services and manage their own configurable settings.

The flexible mechanism is used to define as many levels as needed. Hierarchy node instances of different types can be created and the required business rules can be defined.

5.2. Parent-Child Relationships

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

5.3. Data Access

Data security in the system is achieved by data partitioning and user roles.

With data partitioning, the system ensures that administrative users who access the system can only view and perform operations on instances of entities that are provisioned at their parent hierarchy, in other words at the same hierarchy level as they are, or at sub-trees of that hierarchy. The system restricts access to resources based on user's parent hierarchy and this restriction is enforced in API middleware for every operation that is requested. This partitioning is enforced across the various system interfaces, for example loaders, API, and the GUI.

This for example ensures that an administrator for "VS-Corp" cannot view or affect data in customer "GenCorp" within the system. The "VS-Corp" administrator can only see and affect entities assigned to "VS-Corp" or lower, for example Boston, Brooklyn, Chicago and New York in the above diagram.

Note: When an administrator navigates to a particular hierarchy and views a list of model instances, there may be instances visible that were created at a higher level. For example, a Provider administrator's view of the list of menu layouts may show instances created *above* the Provider's hierarchy.

This visibility is for example required so that a Field Display Policy can be cloned at a lower level. It does not alter a user's modify permissions on model instances created at higher hierarchies. Conversely, a Provider administrator who inspects the list at a hierarchy level *below* the provider level will still be able to modify instances created at the provider's hierarchy.

(A setting **Visible at Lower Hierarchy** is enabled when the model is designed. It is available for Data, Domain, and Relation definitions. For Relations, the setting overrides the setting in any related models. Refer to the table below.)

A user's role defines, via an access profile, the fine-grained permissions to the specific entities that the user can see and how the user can interact with these. The permissions include details of each entity type in the system, as well as the relevant privileges related to that entity type. For further details on user roles and access profiles, refer to *Role Based Access*.

From data partitioning, the hierarchy will determine the specific instances of the various entities that the user can interact with; while the role and access profile assigned to the user determines the permitted operations that can be performed on these instances.

The table below shows the list of models with the setting **Visible at Lower Hierarchy** set to true:

Name	Model Type
AccessProfile	data/DataModel
Adaptation	data/DataModel
AdaptationLog	data/DataModel
BulkAdminDataRefreshPerHierarchy	data/DataModel
BulkAdminFullDataRefresh	data/DataModel
BulkAdminScheduleDataRefresh	data/DataModel
Bundle	data/DataModel
Bundle	data/Relation
ConfigurationTemplate	data/DataModel
Countries	data/DataModel
CredentialPolicy	data/DataModel
FeatureConfigProfile	data/DataModel
FieldDisplayPolicy	data/DataModel
HcsCommandBuilderDAT	data/DataModel
HcsDeviceGroupDAT	data/DataModel
HcsDeviceTypeDAT	data/DataModel
HcsDpDialPlanSchemaDAT	data/DataModel
HcsDpDialPlanSchemaGroupDAT	data/DataModel
HcsLocalizedStringDat	data/DataModel
HcsMovePhoneCustomizationsDAT	data/DataModel
HcsMoveSubCustomizationsDAT	data/DataModel
HcsPrimeCollabREL	data/Relation
LandingPage	data/DataModel
Macro	data/DataModel
MenuLayout	data/DataModel
Patch	data/DataModel
ProvisioningWorkflow	data/DataModel
QuickAddGroups	data/DataModel
Role	data/DataModel
SelfServiceFeatureDisplayPolicy	data/DataModel
SelfServiceLinks	data/DataModel
SelfServiceTranslation	data/DataModel
Theme	data/DataModel

5.4. Navigating the Hierarchy

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

- Bread crumbs

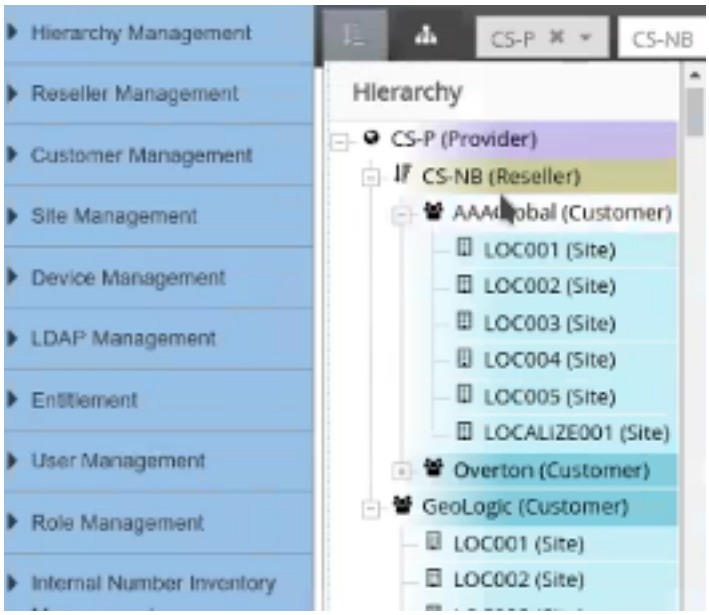
  Navigate through the hierarchy by using the hierarchy bar at the top of the page. Each hierarchy node selection from a drop-down list on the bar that is a parent node may enable a lower level drop-down list, creating a “bread crumbs” list of the hierarchy path. Long lists show a scroll bar in the drop-down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

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

- Hierarchy Tree view

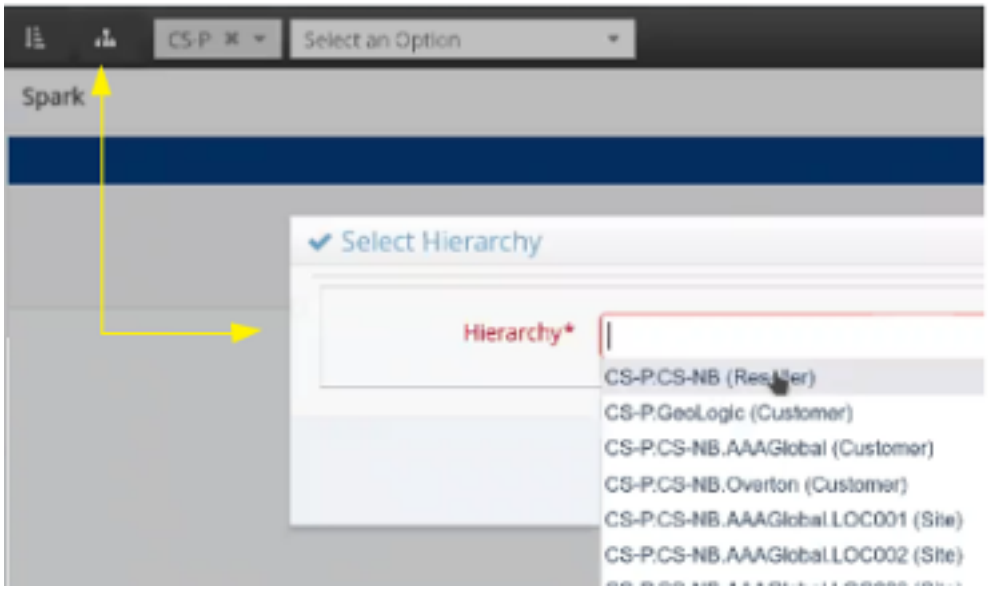
  Use the tree view icon on the hierarchy bar at the top of the page to show a tree view of the entire hierarchy. Choose a hierarchy node on the tree to easily navigate to that node.

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



- Hierarchy Pop-up view

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



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

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

- List view hierarchy links

  For list views, the hierarchy level to which an object belongs is indicated in the hierarchy column is called **Located At**. The hierarchy level name and type shows as the column hierarchy link, for example `Overton (Customer)`.

  All the entries in the list that the logged in user’s hierarchy rules allows for, will show as hyperlinks. This also applies to list views of search results.

  Clicking on the hierarchy link will set the hierarchy to the selected hierarchy in the top “bread crumbs” bar and the items in the list view are filtered accordingly.

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

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

5.5. View the Hierarchy

An administrator can view the portion of the hierarchy that the administrator has access to. The provider administrator can view the complete hierarchy, while a customer administrator can view only the customer, any intermediate nodes beneath the customer, and customer sites.

5.5.1. Procedure

1. To view the hierarchy, choose **Hierarchy Management > Hierarchy**.

   A table containing the hierarchy nodes visible to the administrator is displayed:

Field	Description
Name	Node name
Description	Node description
Hierarchy Node Type	Indicates Provider, Reseller, Customer, or Site. Is blank for an intermediate node.
Hierarchy	Shows the node location in the hierarchy in dot notation.

2. To view a subset of the visible hierarchy, you can adjust the hierarchy path.

   Example: For instance, if a provider administrator, sets the path to point to a particular customer they can see only the hierarchy nodes for that customer.

3. The hierarchy nodes can be sorted by clicking on the field headers.

   The hierarchy nodes can be searched by clicking the search icon on the field headers.

5.6. Create a Provider

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

In VOSS-4-UC, the provider name is set to the current service provider name in HCM-F.

5.6.1. Procedure

1. Log in to VOSS-4-UC as hcsadmin at sys.hcs.
2. Choose **Provider Management > Providers**.
3. Click **Add**.
4. On the **Service Provider Details** tab, complete the following fields:

Field	Description
Name	The name of the provider. The name is automatically set to the current service provider name in HCM-F. You can keep the existing name or overwrite with a more meaningful name. This field is mandatory. Note: Once you have saved the provider, you cannot change the provider name. Note: Any spaces in the provider name are converted to underscores in the provider local administrator name and email, if the **Create Local Admin** check box is selected.
Decouple SDR Name	Select to set a provider name in VOSS-4-UC that is different from the service provider name in HCM-F. Service provider names that were synchronized from VOSS-4-UC 8.1(x) or are set to "All Service Providers" can remain unchanged in HCM-F. If you leave clear, the provider name you enter in the **Name** field is synchronized into HCM-F as the service provider name.
SDR Name	The service provider name to store in the SDR on HCM-F. This field appears only if **Decouple SDR Name** is selected.
Description	A description of the provider.
Domain Name	The domain of the provider. For example, provider.com. Used when creating the default local administrator so the administrator can log in with an email ID such as ProviderAdmin@provider.com. This field is mandatory.
Create Local Admin	Controls whether a default local administrator is created.
Cloned Admin Role	The HCS default provider role used to create a new role prefixed with the provider name. The created provider role, shown in the **Default Admin Role** field, is assigned to the default local administrator. This field appears only if the **Create Local Admin** check box is selected.
Default Admin Role	The created provider role that is assigned to the default local administrator. This field is read-only and appears only if the **Create Local Admin** check box is selected.
Default Admin Password	The password to assign to the default local administrator. This mandatory field appears only if the **Create Local Admin** check box is selected.
Repeat Default Admin Password	Confirm the default local administrator password. This mandatory field appears only if the **Create Local Admin** check box is selected.

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

The provider hierarchy node in VOSS-4-UC, and optionally a default provider administrator are created.

5.7. Create a Reseller

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

After VOSS-4-UC installation, the hcsadmin Administrator must configure the HCM-F device and create the Provider. Creating a reseller is optional.

In VOSS-4-UC, if the reseller name matches an OrgUnit in the SDR you can migrate the OrgUnit as a reseller.

1. Log in as provider administrator.

   Log in with the Provider administrator's email address, which is case-sensitive. The hcsadmin Administrator can find the Provider administrator's email address by selecting **User Management > Local Admins** and then clicking the Provider.
2. Choose **Reseller Management > Resellers** from the menu.
3. Click **Add**.
4. On the **Reseller Details** tab, complete these fields:

Option	Description
Name	The name of the reseller. This field is mandatory. Note: Once you save the reseller, you cannot change the reseller name. Note: Any spaces in the reseller name are converted to underscores in the reseller local administrator name and email, if the **Create Local Admin** check box is selected. Note: If the Reseller Name matches the name of an OrgUnit that exists in the SDR, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this OrgUnit to a reseller at the current hierarchy level. The fields are populated with the values found in the SDR. If you do not want to migrate the OrgUnit, enter a different Reseller Name.
Description	Reseller description
Directory Domain	Reseller domain. This field is used to create an email address for the reseller default local administrator, for example Reseller1Admin@reseller1.com. If omitted, the domain of the provider is used.
Create Local Admin	Controls whether a default local administrator is created for the reseller.
Cloned Admin Role	The Provider role used to create a new role prefixed with the reseller name. The created reseller role, shown in the **Default Admin Role** field, is assigned to the default local administrator user. This field appears only if the **Create Local Admin** check box is selected.
Default Admin Role	The created reseller role that is assigned to the default local administrator. This field is read-only and appears only if the **Create Local Admin** 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.

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

5.8. 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.

5.8.1. 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:

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.

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.

5.9. Create a Site

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

In VOSS-4-UC, if the site name matches an HCM-F customer location, you can migrate the customer location as a site.

1. Log in as provider, reseller, or customer administrator.
2. Make sure that the hierarchy is set to the customer for whom you are creating the site.
3. Choose **Site Management > Sites**.
4. Click **Add**.
5. Complete the following fields:

Option	Description
Site Name	The name of the site. This field is mandatory. Note: Any spaces in the site name are converted to underscores in the site local administrator name and email, if the **Create Local Admin** check box is selected. Note: A customer location that has been configured in HCM-F and synced into VOSS-4-UC may exist at the sys.hcs hierarchy. If the Site Name you enter matches this customer location, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this customer location to a site at 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 location, enter a different Site Name. You cannot migrate a customer location to a site if the customer for the site is different than the customer associated with the customer location. When migrating a customer location to a site, an NDL is not selected for the site. You can set the NDL for the site later.
Description	A description for the site.
Extended Name	External clients can use the Extended Name of the site if needed. This field is not used by other components within Cisco HCS. Note: This field exists in the Customer Location record in SDR. When the customer is managed by Cisco Unified Communications Domain Manager 8.1(x), the Extended Name is synced from Cisco Unified Communications Domain Manager 8.1(x) to the Customer Location record in SDR. When the customer is managed by VOSS-4-UC, the Extended Name is synced from VOSS-4-UC to the Customer Location record in SDR.
External ID	External clients can use the External ID of the site if needed. This field is not used by other components within Cisco HCS.
Create Local Admin	Controls whether a default local administrator is created for the site.

Option	Description
Cloned Admin Role	The customer role used to create a new role prefixed with the site name. The created site role, shown in the **Default Admin Role** field, is assigned to the default local administrator user. This field appears only if the **Create Local Admin** check box is selected.
Default Admin Role	The created site role that is assigned to the default local administrator. This field is read-only and appears only if the **Create Local Admin** check box is selected.
Default Admin Password	The password to assign to the default local administrator. This field appears only if the **Create Local Admin** check box is selected.
Repeat Default Admin Password	Confirm the default local administrator password. This field appears only if the **Create Local Admin** check box is selected.
Country	The country is used to determine which dial plan to download to the site when the dial plan is configured on the site. This field is mandatory.
Network Device List	Choose the NDL containing the UC applications and WebEx to be used by the site. Once an NDL has been set for the site, it cannot be removed from the site, nor can the NDL be changed to another NDL.
Auto Push Users to CUCM	If enabled, users are automatically pushed to the Cisco Unified Communications Manager that is associated with the NDL. The default is disabled. Note: You can edit the site later, and select this check box for one of the following reasons: • To automatically push users at the site to the Cisco Unified Communications Manager. • To perform an Auto User Push when an NDL is added to the site. • To perform an Auto User Push when a Cisco Unified Communications Manager is associated with an NDL.

6. Click **Save**.

Once saved, the following occurs:

- A Site hierarchy node is created.
- A Location is created.
- A Customer Location in the SDR is created.
- Optionally, a default site administrator is created.
- If the **Auto Push Users to CUCM** check box is selected, all users associated with the NDL are pushed to the Cisco Unified Communications Manager associated with the NDL.

5.10. Create Intermediate Node

An intermediate node is an optional node in the VOSS-4-UC hierarchy that is located between the standard hierarchy nodes: provider, reseller, customer, and site. An intermediate node can be used to logically group other nodes. Intermediate nodes can be used to restrict access by administrators to a defined subset of nodes.

For example, intermediate nodes could be used to group customers by industry, or sites by geography.

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

5.10.1. Procedure

1. Log in as an administrator at the level under which you want to create the intermediate node.

   For example, to create an intermediate node to group sites, log in as the customer administrator.
2. Choose **Hierarchy Management > Hierarchy**.
3. To add an intermediate node, click **Add**.
4. Enter the following information for the node:

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

5. Click **Save**.

The intermediate node is created in the hierarchy.

5.10.2. What to Do Next

Define a local administrator for the intermediate node.

Then create nodes underneath the intermediate node that the intermediate node local administrator can manage.

5.11. Delete a Hierarchy

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

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

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

Check box options are available to:

- remove data on selected UC Apps configured on the hierarchy
- remove the hierarchy data from the VOSS-4-UC system database completely

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

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

5.12. Delete Issues and Purges

Whenever Unified CM and CUCX data is synced into VOSS-4-UC, it assumes management of the data and, as a result, that data would be deleted by any hierarchy delete performed in VOSS-4-UC. These deletes can fail if your Cisco Unified Communications Manager model dependencies don't reflect the additional data contained in existing, provisioned dial plans brought into VOSS-4-UC.

There are two ways to prevent these delete failures from happening:

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

Purging deletes all users, subscribers, phone, profiles, and devices from a brownfield customer's VOSS-4-UC while leaving these objects on the Unified CM and the Cisco Unity Connection.

To execute a purge:

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

   At this point, you can try again to migrate the customer into the Cisco Hosted Collaboration Solution by executing HcsPull from the same menu for Unified CM and Unity Connection, and then performing the Overbuild operations.

5.13. Set Localization Language at Hierarchy Node

A default language can be set at any hierarchy node. Users and local administrators will inherit the default language from the nearest hierarchy node in the hierarchy tree that has a default language set. If no default language is specified, English is used. The default language can be overridden for an individual user or local administrator under User Management.

5.13.1. Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to point to the node where you want to set a default language.
3. Choose **Hierarchy Management > Localization Language**.
4. Click **Add**.

5. From the **Language** drop-down, choose the default language.
6. Click **Save**.

As an example, a provider has not set a default language at the provider level. The provider has a reseller in Germany, so the default language at the reseller is German. But that reseller has a customer in France, so the default language at that customer level is set to French. In addition, the customer in France has a site in Italy, so the default language for that site is set to Italian. In this scenario, users that are not under the reseller has English as their language by default.

6 Device Management

6.1. HCM-F Device

6.1.1. Create the HCM-F Device

Note: This section is only applicable to HCM-F.

Before You Begin

- Install and configure HCM-F.
- Verify that the NBI REST SDR Web Service is running:
  1. Log in to the HCM-F CLI as the user administrator.
  2. Run the **utils service list** command. Verify that the Cisco HCS NBI REST SDR Web Service is running.
  3. If not running, start it with the utils service start Cisco HCS NBI REST SDR Web Service command.

After you create the HCM-F device, data synchronization begins if there is a network connection and the NBI REST service is running on the HCM-F server.

Procedure

1. Log in to VOSS-4-UC as hcsadmin at sys.hcs.
2. Create a new HCM-F instance:
   a. Choose **Device Management > HCM-F** and click **Add**.
   b. Enter the HCM-F hostname.
   c. Enter the HCM-F administrator Username.
   d. Enter the HCM-F administrator Password.
   e. Choose the HCM-F Version from the drop-down list.

   Note: Once the HCM-F Version is set to a new version, it cannot be changed to an older one.

   f. Click **Save**.
3. If the previous step fails:

- Verify that HCM-F Hostname is correct
- Verify that HCM-F administrator Username and administrator Passwords are correct
- Verify that HCM-F Version is correct
- Verify that the domain is set correctly using the VOSS-4-UC CLI:
  1. ssh platform@<v4uc hostname>
  2. network domain

4. After a couple of minutes, verify that the initial synchronization between VOSS-4-UC and HCM-F is successful:
   a. Choose **Provider Management > Advanced > SDR Service Provider**.
   b. The sync is successful if the default entry, “Service Provider Name”, appears.

What to Do Next

If the initial sync is not working after following the previous steps, verify that the HCM-F REST API is working by browsing to the following:

`http://<hcmf_app_node_host>/sdr/rest/<hcmf_version>/entity/ServiceProvider`

This command returns the JSON representation of the predefined ServiceProvider instance in the HCM-F Shared Data Repository (SDR). If you get an error, log in as the administrator on the HCM-F app node CLI and verify that the REST service is running:

To display the services, run the command: **utils service list**.

In the output, you see Cisco HCS NBI REST SDR Web Service[STARTED].

If this service is not started, start it with the command: **utils service start Cisco HCS NBI REST SDR Web Service**

For data sync failures, try importing the new HCM-F:

1. Choose **Device Management > HCM-F** and click the HCM-F device.
2. Update the Hostname and click **Save**.
3. Import the new HCM-F:
   a. Choose **Device Management > Advanced > Perform Publisher Actions**.
   b. From the **Action** drop-down, choose **Import**.
   c. From the **App Type** drop-down, choose the HCM-F server.
   d. Click **Save** and wait a few minutes.
4. Check the provider under **Provider Management > Advanced > SDR Service Provider**.

6.2. Unified CM Configuration in VOSS-4-UC

6.2.1. Cisco Unified Communications Manager Configuration in VOSS-4-UC

Overview

Cisco Unified Communications Manager devices provide the core call processing capabilities for HCS, and are a critical part of the VOSS-4-UC provisioning workflows. You must configure the Unified CM devices before you complete the dial plan (if applicable), user, subscriber, line, and phone configuration.

Unified CM devices can be dedicated to a specific customer, or they can be shared between multiple customers. Unified CM devices must then be assigned to one or more Network Devices Lists (NDLs), and the NDL is then assigned to one or more sites. The NDL is used to select which Unified CM is used for configuration based on the site selected in the hierarchy context.

Shared versus Dedicated

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

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

Servers within a Cisco Unified Communications Manager Cluster

Within a Unified CM cluster, you can configure the following nodes:

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

Configure a Cisco Unified Communications Manager Publisher node before configuring any other type node.

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

Synchronization with VOSS-4-UC

Configuring a Unified CM device on VOSS-4-UC creates a scheduled data sync to import model data from the device into VOSS-4-UC. The scheduled data sync ensures that the VOSS-4-UC cache maintains the most current view of the configured device. Any changes to the configuration occurring on the device, including additions, deletions, or modifications, will be reflected in VOSS-4-UC after the next data sync.

Note:

- There is no immediate data sync upon Update or Modification.
- The scheduled data sync fails if the Unified CM administrator account credential has expired. Expiration of the administrator account credential can cause failures in Subscriber Management activities as well.
- Some license-related models will now be excluded from CUCM imports by default:
  - `device/cucm/LicensedUser`
  - `device/cucm/LicensingResourceUsage`

- `device/cucm/HcsLicense`

The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule from **Device Management > CUCM > Schedules**. When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync. You can also manually run the data sync at any time from **Device Management > Advanced > Perform Publisher Actions**, or from **Administration Tools > Data Sync**.

Important: Allow the initial data sync to complete before doing more configuration on VOSS-4-UC that requires information from Unified CM.

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

When you set up an IM and Presence Service server, VOSS-4-UC does not communicate directly with the IM and Presence Service server. The information provided is pushed to HCM-F and Service Assurance (if installed) for monitoring purposes.

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

For details on Change Notification Sync in VOSS-4-UC and on switching between Full Sync and Change Notification Sync, refer to the topic on the Change Notification Feature (CNF) following *Change Notification Feature Overview*.

Field Mappings in Unified CM

When setting up a Unified CM device with LDAP integration, you can map Unified CM user data to VOSS-4-UC user data for any field, based on the Field Mappings in the Unified CM server. These mappings are configured at the LDAP Directory in Unified CM. The mapped user data, for example location data, can later be used in a filter used to move users to sites.

On the Field Mappings tab, you can modify the mappings except for hard-coded mappings. Hard-coded mappings appear in gray and are read-only.

Note: The field name entered in the mapping on VOSS-4-UC must exactly match the field name entered in the mapping in the Unified CM in the Custom User Field Name field. If the field names do not match, the field is skipped during the sync.

6.2.2. Set Up Cisco Unified Communications Manager Servers

Use this procedure to configure Cisco Unified Communications Manager servers within a Unified CM cluster.

Procedure

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

1. Log in as the appropriate hierarchy administrator.

   Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

2. Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

3. Choose **Device Management > CUCM > Servers**.

4. Click **Add**.

5. Enter the Unified CM server name in the **CUCM Server Name** field.

   Note: A Unified CM server that has been configured in HCM-F and synced into VOSS-4-UC may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

6. From the **Server Type** drop-down, choose **Voice/Video**.

7. To configure a publisher node, select the **Publisher** check box.

   On the **Publisher** tab, you can specify the following information:

Field	Description
Prime Collab	Choose the Prime Collaboration management application monitoring this cluster. To unassociate Prime Collaboration for this cluster, choose **None**.
Call Processing ID	The Call Processing ID of this cluster
SDR Cluster ID	The SDR CUCM cluster ID, as shown on **SDR Configuration > SDR CUCM Clusters**.
Multi-Tenant	Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.
Version	Choose the version of the Unified CM Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Port	The port on the Unified CM server to connect to. Default is 8443.
User Move Mode	Choose **Automatic** to automatically move synced in users to sites, based on the filters and filter order defined in **User Management > Manage Filters**. Choose **Manual** if you want an Administrator to manually move synced in users to a Site.
User Entitlement Profile	Choose the Entitlement Profile that specifies which devices and services users synced from this Unified CM are entitled to. Note: A violation of the Entitlement Profile does not prevent a user from being synced to VOSS-4-UC from Unified CM. However, subsequent updates to the user fail until the user's configuration satisfies the restrictions set in the Entitlement Profile.
Enable Change Notification Sync	Select this check box to enable Change Notification. By enabling this, a Change Notification data sync and corresponding Schedule will be created. The Schedule is initially created as Disabled and needs to be manually enabled from the Scheduling menu. The Change Notification Sync interval is set to 14 days by default. See the note below this table.

Refer to the topic on the Change Notification Feature (CNF) following *Change Notification Feature Overview*.

8. For a Unified CM Publisher node, fill in the **Cluster Name** field with the name you want for this cluster. A new cluster is created with this name. This field is required. For Unified CM Subscribers, choose the Unified CM cluster from the **Cluster Name** drop-down menu.
9. Expand **Network Addresses**.
    a. Choose the SERVICE_PROVIDER_SPACE address space.
    b. The **Hostname** field is automatically populated with the Unified CM Server Name. Edit it if necessary.
    c. Enter the IP address of the Cisco Unified Communications Manager Server in the **IPv4 Address** field. Note: Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. VOSS-4-UC cannot validate an entry that contains a blank space at the end of the hostname or IP address.
    d. Fill in the domain of the Unified CM application.
    e. Provide an optional description for the network address.

    If NAT is used, also configure an APPLICATION_SPACE network address.
10. Expand **Credentials**.
    a. Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
    b. Fill in the user ID and password that you configured when you installed the Unified CM.
    c. Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
    d. Provide an optional description for the credential.

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

    Note:

    Expiration of the ADMIN account results in failed data syncs between Unified CM and VOSS-4-UC
11. On the **Field Mappings** tab, complete field mappings as desired. Hard-coded mappings appear in gray and cannot be modified.
12. Click **Save**. A Unified CM network device is created in VOSS-4-UC. A cluster and Unified CM are created in the SDR.
13. Test the connection between Unified CM and VOSS-4-UC
    a. Choose **Device Management > Advanced > CUCM Network Device**.
    b. Click the Unified CM you just added.
    c. Choose **Action > Test Connection**.

    If the test fails, and you used a hostname, make sure VOSS-4-UC has the correct DNS and Domain set.
    a. Log in to the platform CLI.
    b. Query the current DNS setting: **network dns**.
    c. Set the DNS if needed: **network dns <dns_server_ip_address>**.
    d. Query the current domain setting: **network domain**.

e. Set the domain if needed: **network domain <domain>**.

Note:

Use the **CUCM Network Device** page only for testing the connection. Do not edit Unified CM from this page. To change any configuration of the Unified CM, edit it from the **Device Management > CUCM > Servers** page in VOSS-4-UC.

6.2.3. Set Up IM and Presence Service Servers

Use this procedure to configure IM and Presence Service servers within a Cisco Unified Communications Manager cluster.

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

Procedure

1. Log in as the appropriate hierarchy administrator.

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

   Note: An IM and Presence Service server that has been configured in HCM-F and synced into VOSS-4-UC may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.
6. From the **Server Type** drop-down, choose **IM_P**.
7. To configure a publisher node, select the **Publisher** check box.

   Note:

   The **Publisher** tab is not populated for an IM and Presence Service publisher node.
8. Select the Cisco Unified Communications Manager cluster from the **Cluster Name** drop-down.
9. Expand **Network Addresses**.
   a. Select the SERVICE_PROVIDER_SPACE address space.
   b. The **Hostname** field is automatically populated with the IM and Presence Service Server Name. Edit it if necessary.
   c. Enter the IP address of the IM and Presence Service server in the **IPv4 Address** field.

      Note: Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. VOSS-4-UC cannot validate an entry that contains a blank space at the end of the hostname or IP address.

d. Fill in the domain of the IM and Presence Service application.

e. Provide an optional description for the network address.

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

10. Expand **Credentials**.

    a. Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.

    b. Fill in the user ID and password that you configured when you installed the IM and Presence Service.

    c. Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.

    d. Provide an optional description for the credential.

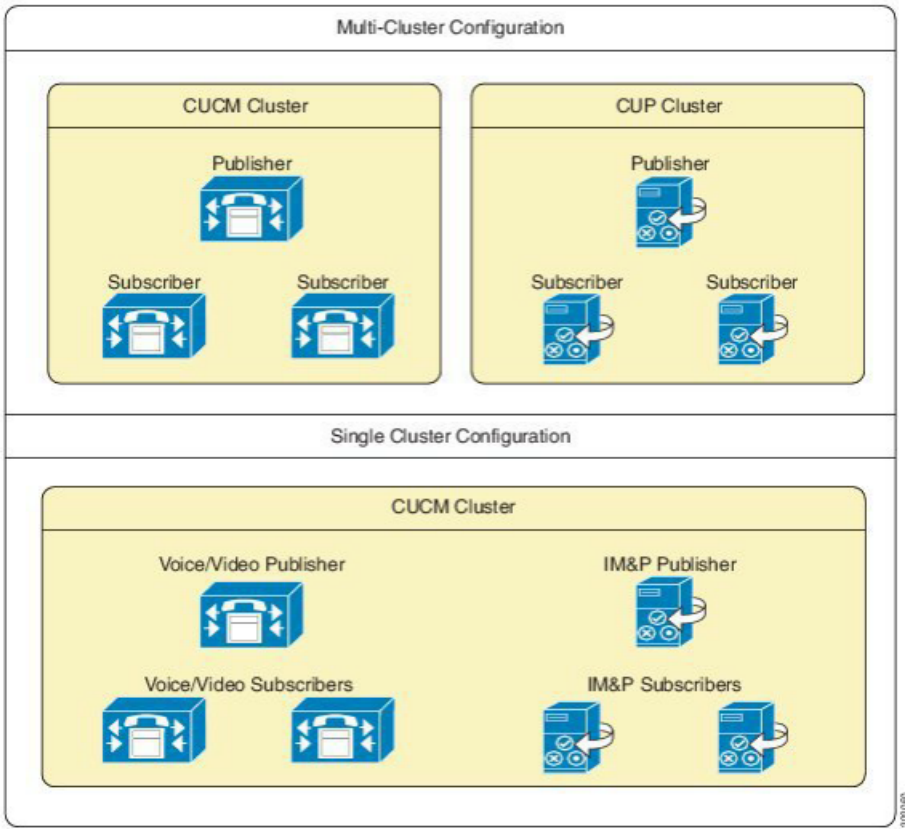
    ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage IM & Presence Service. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

11. Click **Save**.

6.2.4. CUP Cluster Migration

IM and Presence Service (previously known as CUP) was set up in a cluster separate from the Cisco Unified Communications Manager cluster. This configuration is called a multicluster configuration. However, the IM and Presence Service servers are set up as part of the Unified CM cluster itself, in what is called a single-cluster configuration. The single-cluster configuration correctly represents the Unified CM cluster with its IM and Presence Service servers in the management layer. This configuration eliminates the confusion that multicluster configurations can cause for administrators when Cisco Prime Collaboration Assurance and other tools show these servers in different clusters.

Multi-Cluster vs. Single Cluster Configuration



Although the use of multicluster configurations is deprecated and highly discouraged, VOSS-4-UC continues to support multicluster configurations for backward compatibility and upgrades. Service providers are encouraged to use the single-cluster configuration for new clusters. Convert existing multicluster configurations to single-cluster using the migration tool under Device Management.

6.2.5. Migrate CUP to a Cisco Unified CM Cluster

Use this tool to migrate your CUP (also known as IM and Presence Service) nodes to a Cisco Unified Communications Manager cluster, which is the recommended configuration. Migrating CUP nodes to a Unified CM cluster is hierarchy-specific. A Customer CUP node can only be migrated to a Customer Unified CM cluster and not to a Provider or Reseller cluster. A Publisher IM_P node is added first, then Subscriber nodes.

When migrating your CUP to a Unified CM cluster, the following conditions apply:

- Cluster versions must be the same for both the clusters.
- The IPv4 address or hostname and domain configuration must not be duplicated within the cluster.
- Two devices cannot have the same server name.
- No more than one CUP publisher can be migrated to the same Unified CM cluster.
- Multiple subscribers can be migrated to the same Unified CM cluster.

Procedure

1. Log in as provider, reseller, or customer administrator, depending on the hierarchy level where the CUP cluster was configured.
2. Set the hierarchy path to the hierarchy node where the CUP cluster was configured. For a shared configuration, this would be a provider or reseller node. For a dedicated configuration, this would be a customer node.
3. Choose **Device Management > CUP (deprecated) > Migrate CUP to CUCM Cluster**.
4. From the **From CUP Cluster** drop-down menu, choose the CUP cluster you want to migrate.
5. From the **To CUCM Cluster** drop-down menu, choose the Unified CM cluster to which you want to migrate the CUP cluster.
6. Click **Save**.

The migrated CUP server is removed from the list under **Device Management > CUP > Servers** and now appears under **Device Management > CUCM > Servers** as server type **IM_P**. The cluster name for the migrated servers is now the same as the Unified CM cluster name.

6.2.6. Cisco Unified Communications Manager Server Deletion

Deleting a Cisco Unified Communications Manager Server in VOSS-4-UC also deletes local data that has been synced to it from the Cisco Unified Communications Manager Server, including:

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

6.2.7. Configure Regions

Regions can only be added at the customer or site hierarchy level but can be modified at any hierarchy level. Regions added directly on Cisco Unified Communications Manager are synced in at the hierarchy level the Cisco Unified Communications Manager is configured at in VOSS-4-UC.

Procedure

1. Log in as provider, reseller or customer administrator.
2. Choose **Device Management > CUCM > Regions**.
3. Perform one of the following:
   - To add a new Region, click **Add**.
   - To edit an existing Region, click on the name of the Region to be updated.
4. From the **CUCM** drop-down menu, choose or modify the Cisco Unified Communications Manager that corresponds to the Region.
5. Enter a unique name for the new Region in the **Name** field, or modify the existing Name if desired.

6. In the **+ Related Regions** section, configure the following options:

Option	Description
Region Name	Drop-down menu with list of available regions. This field is mandatory.
Audio Codec Preference Lidst	This is a drop-down containing available Audio Codec Preference Lists. The default codec is G.711.
Audio Bandwidth	Maximum Audio Bit Rate (kbps). This field is mandatory.
Video Bandwidth	Maximum Session Bit Rate for Video Calls (kbps). This field is mandatory.
Immersive Video Bandwidth	Maximum Session Bit Rate for Immersive Video Calls (kbps). This field is mandatory.

7. To save a new or updated group, click **Save**.

6.2.8. Delete Region

Regions can be deleted at any hierarchy level. Related regions cannot be removed from a region. They exist until either region is deleted.

Procedure

1. Log in as provider, reseller or customer administrator.
2. Choose **Device Management > CUCM > Regions**.
3. From the list of Regions, click the name of the Region to be deleted.
4. Click **Delete** on the button bar.
5. From the popup window, click **Yes** to confirm the deletion.

6.2.9. Softkey Templates

Introduction

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

- standard
- customized

VOSS-4-UC includes the following Unified CM system softkey templates, which cannot be modified or deleted:

- Cisco Assistant with Feature Hardkeys
- Cisco Chaperone Phone with Feature Hardkeys
- Cisco Feature with Feature Hardkeys Standard
- Cisco Manager with Feature Hardkeys Standard
- Cisco Protected Phone with Feature Hardkeys

- Cisco Shared Mode Manager with Feature Hardkeys
- Cisco User with Feature Hardkeys
- Personal Conference User
- Public Conference User
- Standard User

A reseller administrator (or higher) can create customized softkey templates from the standard templates, make modifications as required and save them at the required hierarchy level, i.e. customer or higher.

How to Manage Customized Softkey Templates and Related Softkey Layout Configurations

---

Note: The following device models need to be imported from Unified CM post upgrade before Softkey Templates can be managed.

This can be done by either performing a full import of Unified CM or using the "CUCM Softkey Templates" Model Type List which is available from Release 19.3.1. See: *Controlling a Data Sync with a Model Type List*.

```
device/cucm/SoftKeyTemplate
device/cucm/SoftKey
device/cucm/SoftKeyCallState
device/cucm/SoftKeySet
```

---

1. Browse to the required hierarchy.
2. Click **Add** to add a new customized softkey template.
3. From the **Create a softkey template based on** drop-down, choose an existing softkey template on which to base the customized template.
4. Enter a unique **Name** and **Description** for the customized template. The description can be a maximum of 50 characters but cannot include ", %, &, <, or >.
5. Select or clear the **Is Default** check box. If selected, this softkey template becomes the default standard softkey template.
6. Click **Save** to save the customized softkey template and simultaneously add it to the **Softkey Template** list view.
7. Select the newly created softkey template and configure the required softkey layout by modifying the designated softkeys for each call state.
   a. CUCM baseline softkey templates cannot be updated. Any change to such a template will result in a failed transaction.
   b. Some of the selected softkeys of the different call state are mandatory and cannot be removed from the CUCM standard set of templates. For example, template Standard User-Custom, Call State – On Hook, Softkey – NewCall.

   When a mandatory softkey is deleted, the transaction will be successful but the softkey will not be removed - when opening the template again it will still be there.
8. Click **Save** when complete.

Note: To modify a customized softkey template, select it from the **Softkey Template** list view and update as described in the above procedure.

Before deleting a softkey template, which has been marked as **Is Default**, a different softkey template must first be set as **Is Default**.

6.3. Cisco Unity Connection

6.3.1. Set up Cisco Unity Connection

Overview

Cisco Unity Connection devices provide voicemail services for HCS deployments, and can be dedicated to a customer or shared across multiple customers. To dedicate a Cisco Unity Connection to a single customer, configure the Cisco Unity Connection at the customer hierarchy node. To share a Cisco Unity Connection across multiple customers, configure the Cisco Unity Connection at a hierarchy node above the customer (reseller, provider, or intermediate node). The Cisco Unity Connection device must be included in one or more Network Device Lists (NDLs), and the NDL must be assigned to one or more sites.

Synchronization with VOSS-4-UC

Configuring a Cisco Unity Connection device on VOSS-4-UC creates a scheduled data sync to import model data from the device into VOSS-4-UC. The scheduled data sync ensures that the VOSS-4-UC cache maintains the most current view of the configured device. Any changes to the configuration occurring on the device, including additions, deletions, or modifications, will be reflected in VOSS-4-UC after the next data sync.

Note:

- There is no immediate data sync upon Update or Modification.
- Some license-related models will now be excluded from Cisco Unity Connection imports by default:
  - `device/cuc/Handler`
  - `device/cuc/GlobalUser`
  - `device/cuc/LicenseStatus`
  - `device/cuc/TenantUserLicense`
  - `device/cuc/UserLicense`

The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule from **Device Management > CUC > Schedules**. When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync. You can also manually run the data sync at any time from **Device Management > Advanced > Perform Publisher Actions**, or from **Administration Tools > Data Sync**.

Important: Allow the initial data sync to complete before doing more configuration on VOSS-4-UC that requires information from Cisco Unity Connection.

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

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

Procedure

1. Log in as the appropriate hierarchy administrator.

   Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

2. Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.
3. Choose **Device Management > CUC > Servers**.
4. Click **Add**.
5. Enter a Cisco Unity Connection server name in the **CUC Server Name** field.

   Note: A Cisco Unity Connection server that has been configured in HCM-F and synced into VOSS-4-UC may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

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

   Note:

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

   On the **Publisher** tab, you can specify the following information:

Field	Description
Prime Collab	Select the Prime Collaboration management application monitoring this cluster. To unassociate Prime Collaboration for this cluster, select None.
Call Processing ID	The Call Processing ID of this cluster
Cluster ID	The Cluster ID of this cluster.
Multi-Tenant	If creating at provider level, this field is read-only and set to Shared. If creating at customer level, you can choose between Dedicated and Partitioned.
Version	Select the version of Cisco Unity Connection Servers in this cluster. The available versions depend on the version of HCM-F that has been configured.
Port	The port on the Cisco Unity Connection server to connect to. Default is 8443.

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

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

8. Expand **Network Addresses**.

a. Choose the SERVICE_PROVIDER_SPACE address space.

b. The **Hostname** field is automatically populated with the Cisco Unity Connection Server Name. Edit it if necessary.

c. Enter the IP address of the Cisco Unity Connection Server in the **IPV4 Address** field.

Note: Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. VOSS-4-UC cannot validate an entry that contains a blank space at the end of the hostname or IP address.

d. Fill in the domain of the Cisco Unity Connection application.

e. Provide an optional description for the network address.

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

9. Expand **Credentials**.

a. Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.

b. Fill in the user ID and password that you configured when you installed the Cisco Unity Connection.

c. Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.

d. Provide an optional description for the credential.

- ADMIN credentials are used by VOSS-4-UC to access the Cisco Unity Connection REST API interface for provisioning synchronization.
- PLATFORM credentials are used by HCM-F (HLM service) to set the deployment mode and restart the publisher.
- ADMIN, HTTP, and SNMP are required for PCA to manage Cisco Unity Connection. These credentials must be manually configured in Cisco Unity Connection, then configured in VOSS-4-UC's **Device Management > CUC > Servers > Credentials** section.
- PLATFORM and ADMIN are required for Service Inventory to generate reports for UC applications.

10. Click **Save**.

6.3.2. Cisco Unity Connection Server Deletion

Deleting a Cisco Unity Connection Server in VOSS-4-UC also deletes local data that has been synced to it from the Cisco Unity Connection Server, including:

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

6.4. Set Up Cisco Emergency Responder

6.4.1. Set Up Cisco Emergency Responder: Overview

Complete this procedure at any time to configure Cisco Emergency Responder (CER) on VOSS-4-UC. For more information on CER installation and setup, refer to the Cisco Emergency Responder Administration Guide.

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

Procedure

1. Log in as the appropriate hierarchy administrator.
2. Set the hierarchy path to the correct level. Shared instances are created at the provider, reseller, or customer level. Dedicated instances are created at the customer level.
3. Choose **Device Management > CER > Servers**.
4. Perform one of the following:
   - To add a new Cisco Emergency Responder (CER) in VOSS-4-UC, click **Add**.
   - To modify an existing CER, click its name in the list of Cisco Emergency Responders.
5. Enter a name for the Cisco Emergency Responder in the **CER_Virtual Server Name** field.

   Note:

   A Cisco Emergency Responder server that has been configured in HCM-F and synced into VOSS-4-UC may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to VOSS-4-UC** check box is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.
6. Select the **Publisher** check box if you are configuring a publisher node.

   Note:

   The **Publisher** tab is populated only when the **Publisher** check box is selected.
7. Expand **Network Addresses**.
   a. Choose the SERVICE_PROVIDER_SPACE address space.
   b. Enter the IP address of the CER Server in the **IPV4 Address** field.

      Note:

      Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. VOSS-4-UC cannot validate an entry that contains a blank space at the end of the hostname or IP address.
   c. The **Hostname** field is automatically populated with the CER Name. Edit it if necessary.
   d. Fill in the domain of the CER application.
   e. Provide an optional description for the network address.
8. Expand **Credentials**.
   a. Add credentials for PLATFORM and ADMIN credential types. Click + to add more credentials.
   b. Fill in the user ID and password that you configured when you installed the CER.

c. Choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.

d. Provide an optional description for the credential.

PLATFORM and ADMIN are required for license management.

9. On the **Publisher** tab, you can specify the following information:

Field	Description
Version	Select the version of the Cisco Emergency Responder Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Multi-Tenant	Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.

10. Click **Save**.

What to Do Next

Associate CER with Customers

6.4.2. Associate CER with Customers

Before You Begin

A customer must be configured before performing this procedure. Perform this procedure at any hierarchy level at or above where the CER is configured, when you configure the VM in Cisco Unified Communications Domain Manager 10.6(x), or perform it at any time after the VM has been created.

Procedure

1. Log in as a Provider or Reseller administrator.
2. Choose **Device Management > CER > Servers**.
3. Click the name of the CER cluster to associate with a customer.
4. Click the **Customer Association** tab.

   Note:

   The list of customers that appear on this tab are those at, and below your current hierarchy. For example, if you are at the Provider level, and the CER is at Reseller1, you can see all customers at the Provider level and below. An error will occur if you try to associate a customer out of the CER's scope.
5. Select the check box to the left of each customer to be associated with the CER cluster.

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

6.4.3. View Associated Clusters on CER Servers

Before You Begin

Customers must be associated with the Cisco Emergency Responder (CER) cluster in order to be viewed in this procedure, unless the CER is created at customer level. If the CER is created at the customer level, customer information is automatically filled in for the customer where the CER exists.

Procedure

1. Log in as a Provider, Reseller, or Customer administrator.
2. Make sure that the hierarchy is set to the customer you wish to view.
3. Choose **Device Management > CER > Servers**.
4. Click the name of the CER cluster to be viewed. Information appears about the CER cluster. You can view a list of customers associated with the CER server by selecting the Customer Association tab.

6.5. UCCX

6.5.1. Contact Center Servers

Contact Center Management

Reseller level and higher administrators can view and manage Cisco Unified Contact Center Express (UCCX) servers, typically from the **Device Management** menu.

Note:

- Network Device Lists must always be updated to include the UCCX server, even when a single server is used per customer.
- Multiple UCCX servers can be configured for a single customer. In this case, the relevant Network Device Lists be updated with the UCCX server references.
- Cisco Unified CM and UCCX server integration should also be carried out as pre-configuration for this feature to work correctly.

Set Up a Contact Center Server

1. Log in as provider administrator or higher and navigate to the required hierarchy.
2. Click the **Add** button and fill in the server details on the input form.
    - The current supported **Version** is 11.6.x.
    - Set the **Application User ID** values of the server. These are Cisco UCM Application users to be used for agent device association. Typically this would be the RMCM application user (UCCX Resource Manager, Unified CM Telephony user), but could also include others for call recording and so on.

Data Sync of Contact Center Server

When the Contact Center server is added, you can run a pull data sync from the server to VOSS-4-UC. This can be done from the Contact Center Server input interface menu: **Actions > Sync**.

In addition, VOSS-4-UC also automatically creates two default Data Sync instances to manage and schedule data synchronization between the device and VOSS-4-UC. These can be seen from the **Data Sync** list view:

- *SyncUccx-<host>*: use this sync to schedule or manually sync data between the server and VOSS-4-UC.
- *PurgeUCcx-<host>*: disabled by default to avoid accidental purges. It and can be enabled by changing the Sync Type to “Purge Local Resources” from “Pull from Device” and by unchecking the **Disabled Operations**.

The Data Sync instances will be removed automatically when the server is deleted. The purge sync will also be executed on server deletion, thereby removing any configuration from the VOSS-4-UC system.

6.6. WebEx

6.6.1. WebEx: Overview

WebEx is a web conferencing facility used for collaboration with colleagues across your organization.

The support for Cisco WebEx is as follows:

- Hosted WebEx Cloud.
- Ability to create user accounts and meetings using WebEx versions:
  - 6.0 API and 27.00 server
  - 8.0 API and 29.13 server
- User and Meeting APIs are exposed and available, so that user capability can be managed. However, system setup, Site addition, and meeting functions, are done with the WebEx application.

Parameters are selected or entered when adding WebEx instances of Network Devices on the GUI.

Note: These conditions apply to users of both WebEx and CMR.

6.6.2. WebEx Field Reference

Title	Field Type	Description
Type*	type	The type of WebEx server. It can be **Cloud-Based**.
Protocol*	protocol	The protocol that is used for communication with the WebEx server The protocol can either be 'https' or 'http'.
Address*	address	The address of the WebEx server. For example, Site-name.webex.com.
Port	port	The port that is used for communication with the WebEx server.
Site Name	site_name	The name of the site to be managed. This name is typically the same as the start of the WebEx address. This field is mandatory if Site ID is not specified.
Site Id	site_id	An Id for the site being managed, typically received from the Cisco WebEx Site Provisioning group. This field is mandatory if Site Name is not specified.
Partner Id	partner_id	Partner ID typically received from the Cisco WebEx Site Provisioning group.
Partner Credentials	partner_ credentials_ override	Partner credentials to use for this set of connection parameters.
REST URI*	rest_uri	The relative URI of the XML service of the WebEx server. For example, WBXService/XMLService
WebEx	webex_id	The WebEx Id of an administrator of the site. This is used to connect to to the server for administrative tasks such as adding or deleting users.
Email	email	A valid email for the administrator. Required if no WebEx Id is provided.
Password*	password	The password for the administrator with the supplied WebEx Id.
Version	version	Supported WebEx server versions. The supported server versions can either be '27.00' or '29.13'.

6.6.3. Device Model Mapping

A data model is maintained in VOSS-4-UC where its instances map network device types to data models. For example, the network device device/cucm would have a mapping to data/CallManager. These target data models are used to maintain network device data in VOSS-4-UC, and any of their default connection parameters.

6.6.4. WebEx Overrides

We may want WebEx credentials to be defined at a higher hierarchy level than the actual connection parameter models defined in the data/DeviceModelMapping instance for data/WebEx.

The parameters can be shared among the connection parameter models at lower hierarchy levels. For example, we may want multiple data/WebEx model instances at various customers lower in the hierarchy to share WebEx credentials at the Provider hierarchy.

For WebEx, the Override Model instances can be maintained in data/WebExPartnerCredentials. An instance of this model is then selected in the Partner Credentials drop-down list when an instance of data/WebEx is added.

The values in the selected Override Model then override any connection parameters defined in the data/WebEx instance.

6.6.5. Set Up Cisco WebEx

For additional information about conferencing, see *Conferencing: Overview*.

Procedure

1. Log in as provider or reseller administrator.
2. Choose **Device Management > WebEx > Servers**.
3. Click **Add**.
4. Complete, at minimum, the mandatory *WebEx Server Fields*.
5. Click **Save**.

What to Do Next

To test the connection to the WebEx server, select **Device Management > Advanced > WebEx Network Device**. Click the WebEx server, then choose **Action > Test Connection**.

WebEx Server Fields

Field	Description
Type *	WebEx server type. Read-only field set to Cloud-Based.
Protocol *	Protocol used to communicate with WebEx server. This field is mandatory and defaults to https.
Address *	The IP address or hostname of the WebEx server. This field is mandatory. Example: site-name.webex.com
Port	The port used to communicate with the WebEx Server. Defaults to 443.
Site Name	The name of the site to be managed. Usually matches the start of the WebEx address.
Site Id	An ID for the site being managed. Typically received from Cisco WebEx Site Provisioning group. Provide this field before testing the connection to the WebEx server.
Partner Id	Typically received from Cisco WebEx Site Provisioning group.
REST URI *	The relative URI for the XML service on the WebEx server. This field is mandatory and defaults to WBXService/XMLService.
WebEx Id	WebEx administrator ID. Either the WebEx Id or the Email field is mandatory.
Email	Email address of WebEx administrator. Either the WebEx Id or the Email field is mandatory.
Password	Password for the provided WebEx administrator. This field is mandatory.
Repeat Password	Confirm password for the provided WebEx administrator. This field is mandatory.
Version *	Supported WebEx version.

6.7. Customer Equipment

6.7.1. Set up Customer Equipment

Use this procedure to associate customer equipment with the Prime Collaboration application that monitors it.

1. Log in as customer or site administrator.
2. Set the hierarchy path to the appropriate site.
3. Choose **Device Management > Customer Equipment**.
4. Click **Add**. The following fields appear:
    - Customer Equipment Name
    - Description
    - Media Device
    - Gateway
    - SRST

- Router
- Prime Collaboration
- Network Addresses
- Credentials

Note:

The only required fields are Customer Equipment Name, at least one network address, and one credential if associating Prime Collaboration. Ensure that the network address does not contain a trailing blank space. VOSS-4-UC cannot validate an entry that contains a blank space at the end of the hostname or IP address.

Note:

To unassociate Prime Collaboration for this customer equipment, choose **None**.

5. Click **Save**.

6.8. IOS Device Management

6.8.1. IOS Device Management: Overview

In VOSS-4-UC, you can set up IOS devices such as SIP Local Gateways and Analog Gateways. You can set up Command Builders to generate the appropriate IOS commands for you to copy to the IOS device CLI.

6.8.2. Command Builders Overview

You can build a repository of IOS commands to be run when certain events, such as adding an IOS device, occur. Each set of IOS commands and associated event is known as a Command Builder. For a list of events with default set of IOS commands and available variables, see *Local Break Out and Analog Gateway Events, IOS Commands, and Variables*. The default Command Builders exist at the sys.hcs hierarchy level.

You can define customized Command Builders at any hierarchy node. When an event occurs, Command Builders nearest (at or above) the hierarchy node of the event are checked first. For instance, if an event occurs at a customer hierarchy level, Command Builders at the customer level are checked before Command Builders at the provider or sys.hcs level. Command Builders at a higher level are checked only if no builders match at a nearer hierarchy level. If no customized Command Builders are defined, the default Command Builders at sys.hcs are checked. Multiple Command Builders may be run for the same event at the same hierarchy node.

6.8.3. IOS Device Management Workflow

The following is a possible workflow for setting up Local Break Out using a SIP Local Gateway. This workflow copies IOS commands to the IOS device CLI after each step. Alternatively, you can use the consolidate commands tool to create one set of IOS commands to run all at once.

Procedure

1. Create customized Command Builders for events. Either add new ones, or clone the default ones and update the clones. See *Set up a Command Builder* or *Clone a Command Builder*.
2. Add an IOS device at customer hierarchy level. See *Set up an IOS Device*.
3. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS Commands Log*.
4. Add SIP Local Gateways at customer hierarchy level. See *Set up SIP Local Gateway*.
5. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS Commands Log*.
6. Perform manual configuration on the SIP Local Gateway. See *IOS Gateway Manual Configuration*.
7. Associate SIP Local Gateways to sites. See *Associate a SIP Local Gateway to a Site*.
8. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS Commands Log*.
9. Create E.164 Associations. See *Associate a Set of E.164 Numbers to One Directory Number* or *Associate a Range of E.164 Numbers to a Range of Directory Numbers*.
10. View the IOS Commands log and copy commands to the IOS device CLI. See *View IOS Commands Log*.

6.8.4. LBO and Analog Gateway Configuration and Generated Events

LBO and Analog Gateway Configuration and Corresponding Events

LBO and Analog Gateway Configuration Action	Generated LBO and Analog Gateway Events
Add an IOS Device	HcsAddIOSDeviceEVT
Delete an IOS Device	HcsDeleteIOSDeviceEVT
Add an Analog Device	HcsAddAnalogGatewayEVT
Add an Analog Gateway Endpoint	HcsAddAnalogGatewayEndpointEVT
Add an Analog Gateway Endpoint Mod	HcsAddAnalogGatewayEndpointModEVT
Delete an Analog Gateway	HcsDeleteAnalogGatewayEVT
Delete an Analog Gateway Endpoint	HcsDeleteAnalogGatewayEndpointEVT
Delete an Analog Gateway Endpoint Mod	HcsDeleteAnalogGatewayEndpointModEVT
Add SIP Local Gateway	HcsAddSipLocalGwEVT HcsAddSipLocalGwDialPeerEVT HcsSipLocalGwAddE164AssociationEVT or HcsSipLocalGwAddMultiE164AssociationEVT (if E164 Associations have been configured at the customer level)
Delete a SIP Local Gateway	HcsDeleteSipLocalGwEVT HcsDeleteSipLocalGwDialPeerEVT HcsSipLocalGwDelSitePstnEVT HcsSipLocalGwDelSiteAreaCodeEVT HcsSipLocalGwDelE164AssociationEVT or HcsSipLocalGwDelMultiE164AssociationEVT (if E164 Associations have been configured) HcsSipLocalGwDelVoiceMailPilotNumberEVT (if Voice Mail Pilot Number Association has been configured)
Update a SIP Local Gateway	HcsUpdateSipLocalGw1EVT HcsUpdateSipLocalGw2EVT
Associate a SIP Local Gateway with a Site	HcsSipLocalGwAddSitePstnEVT HcsSipLocalGwAddSiteAreaCodeEVT HcsSipLocalGwAddE164AssociationEVT or HcsSipLocalGwAddMultiE164AssociationEVT (if E164 Associations have been configured) HcsSipLocalGwAddVoiceMailPilotNumberEVT (if Voice Mail Pilot Number Association with a specified E164 Number has been configured on the site)

LBO and Analog Gateway Configuration Action	Generated LBO and Analog Gateway Events
Disassociate a SIP Local Gateway from a Site	HcsSipLocalGwDelSitePstnEVT HcsSipLocalGwDelSiteAreaCodeEVT HcsSipLocalGwDelE164AssociationEVT or HcsSipLocalGwDelMultiE164AssociationEVT (if E164 Associations have been configured)
Associate E164 Numbers to a Single DN	HcsSipLocalGwAddMultiE164AssociationEVT (if a site is associated with SIP Local Gateway)
Associate E164 Numbers to a Range of DNs	HcsSipLocalGwAddE164AssociationEVT (if a site is associated with SIP Local Gateway)
Disassociate E164 Numbers from a Single DN	HcsSipLocalGwDelMultiE164AssociationEVT (if a site is associated with SIP Local Gateway)
Disassociate E164 Numbers from a Range of DNs	HcsSipLocalGwDelE164AssociationEVT (if a site is associated with SIP Local Gateway)
Associate a Voice Mail Pilot Number to a Site	HcsSipLocalGwAddVoiceMailPilotNumberEVT (if the site is associated with SIP Local Gateway)
Disassociate a Voice Mail Pilot Number from a Site	HcsSipLocalGwDelVoiceMailPilotNumberEVT (if the site is associated with SIP Local Gateway)

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

Local Break Out and Analog Gateway Events

Default IOS Commands	Notes
HcsAddIOSDeviceEVT An IOS Device is added.	
conf t voice service VoIP no IP address trusted authenticate y fax protocol t38 ls-redundancy 0 hs-redundancy 0 ↪fallback **pass**-through g711ulaw modem passthrough nse codec g711ulaw voice **class codec** 1 codec preference 1 g729r8 bytes 30 codec preference 2 g711ulaw codec preference 3 g711alaw end	If you are generating the command for VG350 analog gateway, remove y from the generated commands, and then paste it to the analog gateway console.

Default IOS Commands
HcsDeleteIOSDeviceEVT An IOS Device is deleted.
conf t no voice service VoIP no voice **class codec** 1 end

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEVT An Analog Gateway is added.	
conf t stcapp ccm-group 1 stcapp stcapp feature access-code stcapp feature speed-dial sccp local {{ pwf.GatewayDAT.networkInterface }} sccp bind interface {{ pwf.GatewayDAT.networkInterface }} sccp ccm group 1 {{ macro.HcsAnalogGwCommandForCCMIdentAndAssocMCR }} ↪ ccm-manager config server {{ fn.one macro. ↪HcsCucmsAssociatedToNDLRMCR}} ccm-manager sccp local {{ pwf.GatewayDAT. ↪networkInterface }} ccm-manager sccp stcapp end	pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEndpointEVT An Endpoint is added for the Analog Gateway.	
conf t voice-port {{ pwf.PORT_NUM }} caller-id enable timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }} cptone {{ pwf.GatewayDAT.cpTone }} signal {{macro.HcsIosCmdAnalogGwSignalMCR}} no shutdown dial-peer voice {{ pwf.DIAL_PEER_NO }} pots service stcapp port {{ pwf.PORT_NUM }} end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange. pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEndpointModEVT An Endpoint Module is added for the Analog Gateway.	
conf t voice-port {{ pwf.PORT_NUM }} caller-id enable timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }} cptone {{ pwf.GatewayDAT.cpTone }} signal {{macro.HcsIosCmdAnalogGwSignalMCR}} no shutdown dial-peer voice {{ pwf.DIAL_PEER_NO }} pots service stcapp port {{ pwf.PORT_NUM }} end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway. pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands
HcsDeleteAnalogGatewayEVT An Analog Gateway is deleted.
conf t no stcapp no ccm-manager sccp local {{ input.GatewayDAT.networkInterface }} no ccm-manager sccp no sccp no sccp local {{ input.GatewayDAT.networkInterface }} no sccp ccm group 1 end

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointEVT An Analog Gateway Endpoint is deleted.	
conf t voice-port {{ pwf.PORT_NUM }} no caller-id enable no timeouts call-disconnect no cptone no signal shutdown no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots no port {{ pwf.PORT_NUM }} end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointModEVT An Analog Gateway Endpoint Module is deleted.	
conf t voice-port {{ pwf.PORT_NUM }} no caller-id enable no timeouts call-disconnect no cptone no signal shutdown no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots no port {{ pwf.PORT_NUM }} end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsAddSipLocalGwEVT A SIP Local Gateway is added.	
conf t voice class e164-pattern-map 4007 e164 \+T e164 .T voice service VoIP allow-connections sip to sip sip-ua retry invite 2 timers trying 150 application service dsapp param disc-toggle-time 20 param callHold TRUE param callWaiting TRUE param callConference TRUE param callTransfer TRUE voice translation-rule 802 voice translation-profile VOIPOUT80 translate called 802 voice translation-rule 812 voice translation-profile VOIPIN81 translate calling 811 translate called 812 no voice hunt invalid-number no voice hunt unassigned-number [CTD..]	

Default IOS Commands	Available Variables
HcsAddSipLocalGwEVT A SIP Local Gateway is added [CTD]	
[CTD] dial-peer voice 8 VoIP translation-profile incoming VOIPIN81 session protocol sipv2 incoming called e164-pattern-map 4007 fax rate 14400 no vad voice translation-rule 812 rule 97 /^\\+01\\(.*\\)/ /904\\1/ rule 98 /^\\+1\\(.*\\)/ /901\\1/ rule 99 /^\\+\\(.*\\)/ /902\\1/ rule 100 /^\\(.*\\)/ /904\\1/ voice translation-rule 9011 rule 98 /^\\+{{pwf.COUNTRYCODE}}\\(.*\\)/ /\\1/ type any national rule 99 /^\\+\\(.*\\)/ /\\1/ type any international rule 100 /^\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9021 rule 81 /^901\\(.*\\)/ /\\1/ type any national rule 82 /^902\\(.*\\)/ /\\1/ type any international rule 83 /^903\\(.*\\)/ /\\1/ type any unknown rule 84 /^904\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9022 rule 81 /^901\\(.*\\)/ /{{pwf.STDACCESSPREFIX}}\\1/ type any unknown rule 82 /^902\\(.*\\)/ /{{pwf.INTLACCESSPREFIX}}\\1/ type any unknown rule 83 /^903\\(.*\\)/ /\\1/ type any unknown rule 84 /^904\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9111 rule 1 /^\\(.*\\)/ /\+{{pwf.COUNTRYCODE}}\\1/ type national unknown [CTD...]	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsAddSipLocalGwEVT A SIP Local Gateway is added [CTD]	
[CTD] rule 2 /^\\(.*\\)/ /\+\\1/ type international ↪unknown voice translation-rule 9012 rule 98 /^\\+{{pwf.COUNTRYCODE}}\\(.*\\)/ /{{pwf.STDACCESSPREFIX}}\\1/ type any unknown rule 99 /^\\+\\(.*\\)/ /{{pwf.INTLACCESSPREFIX}}\\1/ ↪ type any unknown rule 100 /^\\(.*\\)/ /\\1/ type any unknown voice translation-rule 9121 voice translation-rule 9112 rule 1 /^{{pwf.INTLACCESSPREFIX}}\\(.*\\)/ /\+\\1/ ↪type unknown unknown rule 2 /^{{pwf.STDACCESSPREFIX}}\\(.*\\)/ /\+{{pwf.COUNTRYCODE}}\\1/ type unknown unknown voice translation-rule 9122 voice translation-profile POTSOUT9011 translate calling 9011 translate called 9021 voice translation-profile POTSOUT9012 translate calling 9011 translate called 9022 voice translation-profile POTSOUT9021 translate calling 9012 translate called 9021 voice translation-profile POTSOUT9022 translate calling 9012 translate called 9022 voice translation-profile POTSIN9111 translate calling 9111 translate called 9121 voice translation-profile POTSIN9112 translate calling 9111 translate called 9122 voice translation-profile POTSIN9121 translate calling 9112 translate called 9121 voice translation-profile POTSIN9122 translate calling 9112 translate called 9122 end	

Default IOS Commands	Available Variables	Notes
HcsAddSipLocalGwDialPeerEVT Triggers IOS Commands for each Dial Peer when A SIP Local Gateway is added.		
conf t dial-peer voice {{pwf.DIALPEER}} VoIP translation-profile outgoing VOIPOUT80 {{pwf.PREFERENCE}} voice-class codec 1 service dsapp voice-class sip options-keepalive up-interval 120 down-interval 60 retry 2 session target {{pwf.PBXIP}} destination e164-pattern-map 4007 session protocol sipv2 modem passthrough nse codec g711ulaw dtmf-relay rtp-nte fax rate 14400 no vad end	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.	One command set is generated per dial peer.

Default IOS Commands	Available Variables
HcsDeleteSipLocalGwEVT A SIP Local Gateway is deleted.	
conf t no voice translation-profile POTSIN9122 no voice translation-profile POTSIN9121 no voice translation-profile POTSIN9112 no voice translation-profile POTSIN9111 no voice translation-profile POTSOUT9022 no voice translation-profile POTSOUT9021 no voice translation-profile POTSOUT9012 no voice translation-profile POTSOUT9011 no voice translation-rule 9122 no voice translation-rule 9112 no voice translation-rule 9121 no voice translation-rule 9012 no voice translation-rule 9111 no voice translation-rule 9022 no voice translation-rule 9021 no voice translation-rule 9011 no voice translation-rule 812 no voice translation-rule 802 no dial-peer voice 8 VoIP no voice class e164-pattern-map 4007 application no service dsapp no sip-ua voice service VoIP no allow-connections sip to sip end	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables	Notes
HcsDeleteSipLocalGwDialPeerEVT Triggers IOS Commands for each Dial Peer when A SIP Local Gateway is deleted.		
conf t no dial-peer voice {{pwf.DIALPEER}} VoIP end	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.	One command set is generated per dial peer.

Default IOS Commands	Available Variables	Notes
HcsUpdateSipLocalGw1EVT Triggers IOS Commands when A SIP Local Gateway is updated.		
conf t no dial-peer voice {{pwf.DIALPEER}} VoIP end	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.	Removes configuration related to previous dial peer. One set of commands per dial peer. Note: If "Enable Command Builder" is updated from False to True, IOS commands will be regenerated for the SIP Local Gateway.

Default IOS Commands	Available Variables	Notes
HcsUpdateSipLocalGw2EVT Triggers IOS Commands when A SIP Local Gateway is updated.		
conf t dial-peer voice {{pwf.DIALPEER}} VoIP translation-profile outgoing VOIPOUT80 {{pwf.PREFERENCE}} voice-**class codec** 1 service dsapp voice-**class sip** options-keepalive up-interval 120 down-interval 60 retry 2 session target {{pwf.PBXIP}} destination e164-pattern-map 4007 session protocol sipv2 modem passthrough nse codec g711ulaw dtmf-relay rtp-nte fax rate 14400 no vad end	pwf.COUNTRYCODE - returns the Country Code based on the Country field configured on this SIP Local GW pwf.STDACCESSPREFIX - returns the Country's national trunk access prefix based on the Country field configured on this SIP Local GW pwf.INTLACCESSPREFIX - returns the Country's international access prefix based on the Country field configured on this SIP Local GW pwf.PBXIP - returns the CUCM Server's IP or hostname for dial peer pwf.PREFERENCE - returns the CUCM server's priority in the dial peer list pwf.DIALPEER - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.	Adds configuration related to new dial peer. One set of commands per dial peer. Event is triggered only if the SIP Trunk information has been updated.

Default IOS Commands	Available Variables	Notes
HcsSipLocalGwAddSiteAreaCodeEVT Triggers IOS commands for Area Code when a SIP Local Gateway is associated with a Site.		

conf t
 	
voice translation-rule 9021
 	
rule {{pwf.RULENUMBER}} /^901{{pwf.NATCODE}}\\(.*\\)//{{pwf.NATCODEFORLOCALDIALING}}\\1/ type any subscriber
 	
voice translation-rule 9022
 	
rule {{pwf.RULENUMBER}} /^901{{pwf.NATCODE}}\\ (.*\\)//{{pwf.NATCODEFORLOCALDIALING}}\\1/ type any unknown
 	
end
	{{pwf.RULENUMBER}} and {{pwf.NATCODE}} are sequence numbers and area codes that is substituted by workflow during runtime {{pwf.NATCODEFOR LOCALDIALING}} is the Area Code if the administrator selected the "Area Code Used for Local Dialing" option when deploying the site dial plan. If this option was not selected, this variable has no value.	The workflow for this event generates IOS Commands for each Area Code defined for the associated Site.

Default IOS Commands	Available Variables	Notes
HcsSipLocalGwDelSiteAreaCodeEVT Triggers IOS commands for Area Code when a SIP Local Gateway is disassociated from Site.		
conf t no voice translation-rule 9021 no rule {{pwf.RULENUMBER}} end conf t no voice translation-rule 9022 no rule {{pwf.RULENUMBER}} end	{{pwf.RULENUMBER}} is substituted as sequence number by workflow during run time	The workflow for this event generates IOS Commands for each Area Code defined for the disassociated Site. If Area Codes are shared across multiple sites and associated with the same gateway, the commands are generated only when the gateway is disassociated from the last site that shares the Area Code.

Default IOS Commands	Available Variables
HcsSipLocalGwAddSitePstnEVT Triggers IOS commands for PSTN when a SIP Local Gateway is associated with a Site.	
conf t voice translation-rule 9111 rule 3 /^\\(.*\\)/ /{{pwf.PSTNACCESSPREFIX}}\\\\1/ ↪type subscriber unknown rule 4 /^\\(.*\\)/ /{{pwf.PSTNACCESSPREFIX}}\\\\1/ ↪type unknown unknown voice translation-rule 9112 rule 3 /^\\(.*\\)/ /{{pwf.PSTNACCESSPREFIX}}\\\\1/ ↪type unknown unknown end	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site

Default IOS Commands	Notes
HcsSipLocalGwDelSitePstnEVT Triggers IOS commands for PSTN when a SIP Local Gateway is disassociated from Site.	
conf t no voice translation-rule 9111 no rule 3 no rule 4 no voice translation-rule 9112 no rule 3 end	By default, these commands are not generated to avoid deleting the voice translation rule for PSTN if the gateway is shared by multiple sites. If you need to delete the translation rules for PSTN when SIP Local Gateway is disassociated from site, clone the command builder template and set the Enabled flag.

Default IOS Commands	Available Variables
HcsSipLocalGwAddE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to 1 DN) is made.	

conf t
 	
voice translation-rule 9011
 	
rule {{ pwf.RULENUMBER }} /^{{pwf.DNESCAPE }}{{ pwf.DNPREFIX }}
\\\\ ({{ pwf.RGMASK }} \\\\ )/ /{{ pwf.DDIPREFIX }}␣
↪\\\\ 1/ type
any national
 	
voice translation-rule 9012
 	
rule {{ pwf.RULENUMBER }} /^{{pwf.DNESCAPE }}{{ pwf.DNPREFIX }}
\\\\ ({{ pwf.RGMASK }} \\\\ )/ /{{ pwf.STDACCESSPREFIX }}{{
pwf.DDIPREFIX }} \\\\ 1/ type any unknown
 	
voice translation-rule 802
 	
rule {{ pwf.RULENUMBER }} /^{{pwf.DNESCAPE }}{{ pwf.DNPREFIX }}
\\\\ ({{ pwf.RGMASK }} \\\\ )/ /\+{{ pwf.COUNTRYCODE }}{{
pwf.DDIPREFIX }} \\\\ 1/
 	
voice translation-rule 9121
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.DDIPREFIX }}␣
↪\\\\ ({{
pwf.RGMASK }} \\\\ )/ /{{ pwf.DNPREFIX }} \\\\ 1/␣
↪type national
unknown
 	
voice translation-rule 9122
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.STDACCESSPREFIX }}
↪{{
pwf.DDIPREFIX }} \\\\ ({{ pwf.RGMASK }} \\\\ )/ /{{␣
↪pwf.DNPREFIX
}} \\\\ 1/ type unknown unknown
 	
voice translation-rule 712
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.PSTNACCESSPREFIX }
↪}{{
pwf.STDACCESSPREFIX }}{{ pwf.DDIPREFIX }} \\\\ ({{␣
↪pwf.RGMASK }}
\\\\ )/ /{{ pwf.DNPREFIX }} \\\\ 1/
 	
end
	pwf.DNPREFIX - Contains the directory number prefix (DN without the mask digits)
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwf.RULENUMBER - Contains the appropriate rule index for associate/disassociate

Default IOS Commands	Available Variables
HcsSipLocalGwDelE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to 1 DN) is deleted.	
conf t voice translation-rule 9011 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9012 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 802 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9121 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9122 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 712 no rule {{ pwf.RULENUMBER }} end	pwf.DNPREFIX - Contains the directory number prefix (DN without the mask digits) pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a + pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..) pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code) pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site pwf.COUNTRYCODE - Country Code for the country associated with the site pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site pwd.RULENUMBER - Contains the appropriate rule index for associate/disassociate

Default IOS Commands	Available Variables
HcsSipLocalGwAddMultiE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to N DN) is made.	

conf t
 	
voice translation-rule 9011
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.DNESCAPE }}{{ pwf.DN }}/ /{{
pwf.DDIPRIMARY }}/ type any national
 	
voice translation-rule 9012
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.DNESCAPE }}{{ pwf.DN }}/ /{{
pwf.STDACCESSPREFIX }}{{ pwf.DDIPRIMARY }}/ type any unknown
 	
voice translation-rule 802
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.DNESCAPE }}{{ pwf.DN }}/ /\+{{
pwf.COUNTRYCODE }}{{ pwf.DDIPRIMARY }}/
 	
voice translation-rule 9121
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.DDIPREFIX }}{{pwf.RGMASK }}/
/{{ pwf.DN }}/ type national unknown
 	
voice translation-rule 9122
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.STDACCESSPREFIX }}{{
pwf.DDIPREFIX }}{{ pwf.RGMASK }}/ /{{ pwf.DN }}/ type unknown
unknown
 	
voice translation-rule 712
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.PSTNACCESSPREFIX }}{{{
pwf.STDACCESSPREFIX }}{{ pwf.DDIPREFIX }}{{ pwf.RGMASK }}/ /{{
pwf.DN }}/
 	
end
	pwf.DN - Contains the directory number
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPRIMARY - Contains the primary E.164 associate with the N:1 association (DDI without + prefix and country code) Note: this still contains the national code (area code)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for associate/disassociate

Default IOS Commands	Available Variables
HcsSipLocalGwDelMultiE164AssociationEVT Triggers IOS commands for SIP Local Gateway when an E164 Association (N to N DN) is deleted.	
conf t voice translation-rule 9011 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9012 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 802 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9121 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9122 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 712 no rule {{ pwf.RULENUMBER }} end	pwf.DN - Contains the directory number pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a + pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..) pwf.DDIPRIMARY - Contains the primary E.164 associate with the N:1 association (DDI without + prefix and country code) Note: this still contains the national code (area code) pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code) pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site pwf.COUNTRYCODE - Country Code for the country associated with the site pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site pwd.RULENUMBER - Contains the appropriate rule index for associate/disassociate

Default IOS Commands	Available Variables
HscSipLocalGwAddVoiceMailPilotNumberEVT Associate a Voice Mail Pilot Number with a Site	

conf t
 	
voice translation-rule 9121
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.DDIPREFIX }}\\\\\({{
pwf.RGMASK }}\\\\\)/ /{{ pwf.DNPREFIX }}\\\\\1/ type national
unknown
 	
voice translation-rule 9122
 	
rule {{ pwf.RULENUMBER }} /^{{ pwf.STDACCESSPREFIX }}{{
pwf.DDIPREFIX }}\\\\\({{ pwf.RGMASK }}\\\\\)/ /{{ pwf.DNPREFIX
}}\\\\\1/ type unknown unknown
 	
end
	pwf.DNPREFIX - Contains the voice mail pilot number prefix (without the mask digits)
	pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a +
	pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..)
	pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code)
	pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site
	pwf.COUNTRYCODE - Country Code for the country associated with the site
	pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site
	pwd.RULENUMBER - Contains the appropriate rule index for voice mail pilot association

Default IOS Commands	Available Variables
HscSipLocalGwDelVoiceMailPilotNumberEVT Disassociate a Voice Mail Pilot Number from a Site	
conf t voice translation-rule 9121 no rule {{ pwf.RULENUMBER }} end conf t voice translation-rule 9122 no rule {{ pwf.RULENUMBER }} end	pwf.DNPREFIX - Contains the voice mail pilot number prefix (without the mask digits) pwf.DNESCAPE - Contains a backslash escape character if the DNPREFIX contains a + pwf.RGMASK - Contains the range mask for prefix (for example if range is 100, then the value is ..) pwf.DDIPREFIX - Contains the DDI (E.164) prefix (DDI without + prefix, country code, or mask digits) Note: this still contains the national code (area code) pwf.STDACCESSPREFIX - National Trunk Prefix for the country associated with the site pwf.COUNTRYCODE - Country Code for the country associated with the site pwf.PSTNACCESSPREFIX - PSTN breakout associated with the country associated with the site pwd.RULENUMBER - Contains the appropriate rule index for voice mail pilot association

6.8.6. MGCP Analog Gateway Events and IOS Commands

MGCP Analog Gateway Events

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEVT Adds an Analog MGCP Gateway.	
conf t hostname {{pwf.GatewayDAT.domainName}} ccm-manager config server {{ fn.one macro. ↪HcsCucmsAssociatedToNDLRMCR}} ccm-manager config mgcp call-agent {{ fn.one macro. ↪HcsCucmsAssociatedToNDLRMCR}} 2427 service-type␣ ↪mgcp version 1.0 ccm-manager mgcp ! ccm-manager redundant-host ccm-manager switchback Graceful ccm-manager fallback-mgcp mgcp bind control source-int {{ pwf.GatewayDAT. ↪networkInterface }} mgcp bind media source-int {{ pwf.GatewayDAT. ↪networkInterface }} mgcp dtmf-relay voip codec all mode out-of-band mgcp modem passthrough voip mode nse mgcp package-capability sst-package no mgcp package-capability sst-package end	pwf.GatewayDAT.networkInterface - returns the Network Interface based on the configuration in the Gateway.

Default IOS Commands	Available Variables
HcsAddAnalogGatewayEndpointEVT Adds an Endpoint for the Analog MGCP Gateway.	
conf t voice-port {{ pwf.PORT_NUM }} timeouts call-disconnect {{ fn.as_string pwf. ↪GatewayDAT.disconnectTimeout }} cptone {{ pwf.GatewayDAT.cpTone }} signal {{macro.HcsIosCmdAnalogGwSignalMCR}} ring frequency 25 description {{ fn.sub_string macro. ↪HcsAnalogGatewayIOSCmdDesc, 0, 63 }} timing hookflash-in 250 80 no shutdown exit dial-peer voice {{ pwf.DIAL_PEER_NO }} pots service mgcpapp port {{ pwf.PORT_NUM }} end	pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway. pwf.DIAL_PEER_NO - returns the dial peer number that is used to generate the dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsAddAnalogMGCPGatewayEndpointModEVT Adds an Endpoint Module for the Analog MGCP gateway.	
conf t voice-port {{ pwf.PORT_NUM }} timeouts call-disconnect {{ fn.as_string pwf.GatewayDAT.disconnectTimeout }} cptone {{ pwf.GatewayDAT.cpTone }} signal {{macro.HcsIosCmdAnalogGwSignalMCR}} ring frequency 25 description {{ fn.sub_string macro.HcsAnalogGatewayIOSCmdDesc, 0, 63 }} timing hookflash-in 250 80 no shutdown exit dial-peer voice {{ pwf.DIAL_PEER_NO }} pots service mgcpapp port {{ pwf.PORT_NUM }} end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange. pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEVT Deletes an Analog MGCP Gateway.	
conf t no mgcp call-agent {{ fn.one macro.HcsCucmsAssociatedToNDLRMCR}} 2427 service-type mgcp version 1.0 no ccm-manager config server {{ fn.one macro.HcsCucmsAssociatedToNDLRMCR}} mgcp no ccm-manager mgcp ! no ccm-manager redundant-host no ccm-manager switchback Graceful no ccm-manager fallback-mgcp no mgcp bind control source-int {{ pwf.GatewayDAT.networkInterface }} no mgcp bind media source-int {{ pwf.GatewayDAT.networkInterface }} no mgcp dtmf-relay voip codec all mode out-of-band no mgcp modem passthrough voip mode nse no ccm-manager music-on-hold no ccm-manager config no mgcp package-capability rtp-package no mgcp package-capability sst-package no mgcp default-package mt-package no mgcp timer receive-rtcp no mgcp sdp simple no mgcp fax t38 inhibit no mgcp end	pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.

Default IOS Commands	Available Variables
HcsDeleteAnalogGatewayEndpointEVT Deletes an Endpoint for the Analog MGCP Gateway.	
conf t voice-port {{ pwf.PORT_NUM }} no timeouts call-disconnect default cptone default timing hookflash-**in** default description no signal default ring frequency shutdown exit no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsDeleteAnalogMGCPGatewayEndpointModEVT Deletes an Endpoint Module for the Analog MGCP Gateway.	
conf t voice-port {{ pwf.PORT_NUM }} no timeouts call-disconnect default cptone default timing hookflash-**in** default description no signal default ring frequency shutdown exit no dial-peer voice {{ pwf.DIAL_PEER_NO }} pots end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.DIAL_PEER_NO - returns the dial peer number we use to generate dial peer. It starts from 4 for the first dial peer, and increase by 1 for the next one.

Default IOS Commands	Available Variables
HcsUpdateAnalogGatewayEVT Updates the Analog MGCP Gateway.	
conf t hostname {{pwf.GatewayDAT.domainName}} no mgcp bind control source-int {{ pwf. ↪previousGatewayDAT.networkInterface }} mgcp bind control source-int {{ pwf.GatewayDAT. ↪networkInterface }} no mgcp bind media source-int {{ pwf. ↪previousGatewayDAT.networkInterface }} mgcp bind media source-int {{ pwf.GatewayDAT. ↪networkInterface }} end	pwf.GatewayDAT.networkInterface - This is the physical device network interface (Ethernet Port) for the analog gateway.

Default IOS Commands	Available Variables
HcsUpdateAnalogGatewayEndpointEVT Updates the Endpoint for the Analog MGCP Gateway.	
conf t voice-port {{ pwf.PORT_NUM }} no signal signal {{macro.HcsIosCmdAnalogGwSignalMCR}} no timeouts call-disconnect timeouts call-disconnect {{ fn.as_string pwf. ↪GatewayDAT.disconnectTimeout }} no cptone cptone {{ pwf.GatewayDAT.cpTone }} no shutdown end	pwf.PORT_NUM - This is the FXS port number of the analog gateway device. pwf.GatewayDAT.disconnectTimeout - Time in seconds for which a connection is maintained after the completion of a communication exchange. pwf.GatewayDAT.cpTone - This is the call progress tone of the country that supports each analog device in the gateway.

6.8.7. Translation Rule Numbering

The following information can be helpful to decode the number of Translation Rules included in IOS Command Builders.

- The first digit indicates if the rule is for SRST, VoIP, or TDM: 7 for SRST, 8 for VoIP, and 9 for PSTN.
- The second digit indicates if it is for incoming or outgoing call: 1 for incoming and 0 for outgoing
- The third digit indicates if it is for calling or called number: 1 for calling and 2 for called
- The fourth digit indicates if NOA is used: 1 is for NOA and 2 for no NOA and defines on the TDM trunk to the PSTN.

Examples:

- Translation-rule 9011 - for handling calling number of an outgoing call to the PSTN where NOA is used.
- Translation-rule 9022 - for handling called number of an outgoing call to the PSTN where NOA is not used.
- Translation-rule 9111 - for handling calling number of an incoming call from the PSTN where NOA is used.

6.8.8. Set up a Command Builder

Use this procedure to set up a Command Builder that contains an IOS Commands template for an event.

Note: One event can trigger multiple Command Builders.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the level where you want to define your Command Builder.

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

Field	Description
Name	Enter a unique name for the builder. This field is mandatory.
Event Name	Select the event that triggers the builder. This field is mandatory
Description	Enter a description for the builder.
Command Template	Enter the IOS Commands template for the event, one command per line. You can use macros in the IOS Commands template for variable substitution.
Enabled	Clear the **Enabled** check box to create a builder but not have it available to run.
Applicable Device Type	Select the device type that the commands can run on. This field is mandatory.

6. Click **Save**.

6.8.9. Clone a Command Builder

Use this procedure to clone a Command Builder that contains an IOS Commands template for an event. For instance, use this procedure to modify one of the default Command Builders to suit your needs.

Note: One event can trigger multiple Command Builders.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the level where you want to clone an existing Command Builder.
3. Choose **Device Management > IOS > Command Builder**.
4. Click the Command Builder name you want to clone.
5. Choose **Action > Clone**.
6. Modify the following information as needed:

Field	Description
Name	Enter a unique name for the builder. This field is mandatory.
Event Name	Select the event that triggers the builder. This field is mandatory
Description	Enter a description for the builder.
Command Template	Enter the IOS Commands template for the event, one command per line. You can use macros in the IOS Commands template for variable substitution.
Enabled	Clear the **Enabled** check box to create a builder but not have it available to run.
Applicable Device Type	Select the device type that the commands can run on. This field is mandatory.

7. Click **Save**.

6.8.10. Set up an IOS Device

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer hierarchy node where you want to set up the IOS Device.
3. Choose **Device Management > IOS > IOS Devices**.
4. Click **Add**.
5. Provide the following information:

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

6. In the **Network Addresses** pane, configure the SERVICE_PROVIDER_SPACE address space.

Field	Description
Address Space	Address Space Type. SERVICE_PROVIDER_SPACE is the default. This field is required.
IPV4 Address	Enter the IP address of the IOS Device.
Host Name	The **Host Name** field is automatically populated with the IOS Device Name. If the IOS Device Name is not the host name, you can edit this field to provide the host name, or provide an IP address in the **IPV4 Address** field. Note: Either a host name or an IP address is required. If both are provided, the host name is used. If a host name is provided must be resolvable by the IOS Device.
Domain	The domain of the IOS Device.
Description	An optional description for the network address

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

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

7. Optionally, expand **Credentials**.
    a. Add credentials for CLI, SNMP_V2, SNMP_V3 credentials types. Click + to add more credentials.
    b. For CLI and SNMP_V3, fill in the user ID and password that you configured when you installed the IOS Device. For SNMP_V2, only the password is required.
    c. For SNMP credentials, choose RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
    d. Provide an optional description for the credential.

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

Note:

SNMP configuration must be done manually on the IOS Device.

8. Click **Save**.

6.8.11. Analog Gateways

A Cisco analog gateway connects fax machines, analog phones, and modems in the SCCP/MGCP protocol. Any IOS device that has FXS ports configured as SCCP/MGCP endpoints on Cisco Unified Communications Manager is considered an SCCP/MGCP analog gateway.

An analog device contains analog phones, which are endpoints in Cisco Unified Communications Manager.

6.8.12. Set up an Analog Gateway

Before You Begin

- Add an IOS device in VOSS-4-UC at the Customer level hierarchy. To add an IOS device, see *Set up an IOS Device*.
- Ensure that the site-level dial plan is applied on the site where the gateway is being added.

Note: VOSS-4-UC supports SCCP and MGCP protocols. It does not support BRI endpoints. Do not add slots or modules or subunits for BRI.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **Device Management > IOS > Analog Gateways**.
3. Click **Add**.
4. Choose the required hierarchy path from the drop-down and click **OK**.
5. On the **Gateway** tab, complete, at minimum, the mandatory *Gateway Fields*.
6. On the **Gateway Units** tab, click + to expand **Modules**, and complete, at minimum, the mandatory *Gateway Units - Modules Fields*.
7. On the **Endpoints** tab, click + to expand the SCCP or MGSP endpoints, and complete, at minimum, the mandatory:
   - *SCCP Endpoints Fields*.
   - *MGCP Endpoints Fields*.
8. On the **Config** tab, click + to expand the **Product Specific Configuration Layout**, and complete the required *Config: Product Specific Configuration Layout Fields*.
9. Click **Save**.

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

Successful Scenario	Failure Scenario
Adding an Analog device with a phone line.	Removing the phone line from the endpoint.
Adding an Analog gateway without using enable command builder.	Adding a phone line after adding the command builder.
Removing the command builder after adding an analog gateway with command builder.	Adding an analog gateway without a phone line after adding a phone line to an endpoint. Note: Ensure to add the Directory Names to both endpoints.

Gateway Fields

Field	Description
IOS Device *	Choose the required IOS Device from the drop-down list. For example: IOS 11. This is a mandatory field. Note: The IOS device identifies the devices that are not associated with any Analog Gateways.
Product *	Choose the product from the drop-down list. For example: VG202, where VG represents Voice Gateway and 202 represents port. It has 2 ports, 0 and 1. This is a mandatory field. Note: The analog gateway supports Following models: • VG202: 2 ports • VG204: 4 ports • VG224: 24 ports • VG310: 24 ports • VG320: 48 ports • VG350: 144/160 ports
Protocol *	Choose the protocol from the drop-down list. The available protocols are **SCCP** and **MGCP**. This is a mandatory field.
Gateway Name *	Enter the MAC address of the analog gateway. For example: SKIGW0102030405, where SKI represents SCCP, GW represents gateway, and the last 10 digits represents the MAC address of the gateway. This is a mandatory field for the SCCP protocol.
Domain Name	Enter a fully qualified domain name. For example: E7C1VG310.hcsent17.com. This is a mandatory field for the MGCP protocol.
Call Manager Group *	Choose the call manager group from the drop-down list. For example: **Default**. This is a mandatory field. Note: Call Manager Group is default based on the site default device pool.
Enable Command Builder	Leave the check box clear to generate IOS commands, when Analog Gateway is added, deleted, or modified.

Note: For more information,see *Local Break Out and Analog Gateway Events, IOS Commands, and*

Variables. To view generated commands from Command Builder, see *View IOS Commands Log*.

Field	Description
Gateway Network Interface *	Enter a Gateway Network Interface. For example: **FastEthernet0/0**, **FastEthernet0/1**, **GigabitEthernet0/0**, **GigabitEthernet0/1** or ****GigabitEthernet0/2**. This is a mandatory field. Note: Check the network interface at the Physical Device, then choose the appropriate Network Interface and Port as applicable. The Network Interface is used in Command Generation. Choose **FastEthernet** for all 2x series and **GigabitEthernet** for all 3x series.
Call Disconnect Timeout *	Enter the time unit for Call Disconnect Timeout. For example: **2**. This is a mandatory field. Note: The time unit always is in seconds. Do not enter any negative timer values.
CP Tone *	Choose the call progress tone (country code) from the drop-down list. For example: **in** (for India). This is a mandatory field. Note: CP Tone is an FXS configuration parameter that supports each analog device in the gateway.
Signal *	Choose a signal from the drop-down list. For example: **loop-start** or **ground-start**. This is a mandatory field. Note: Signal is an FXS configuration parameter that supports each analog device in the gateway.

Gateway Units - Modules Fields

Field	Description
Slot *	Choose the required value from the drop-down list. For example: 0. This is a mandatory field Note: • Add only those Units (Modules) and Subunits that are listed in the drop-down list, without duplicate the units and subunit numbers. • If duplicating entry is made for a slot, then the new slot overwrites the older configuration. You may lose previously configured endpoints. • For VG310 model, do not choose any module for slot 1.
Module *	Choose the available module from the drop-down list. For example: NM-4VWIC-MBRD. Note: Only modules that are available for the slot appear in the list.
Subunits *	Click + to expand Subunits. This is a mandatory field.
Subunit Position *	Choose the subunit position from the drop-down list. For example: 0. Note: Subunit position 1 on the VG310 gateway has no available hardware by design, so choosing a value of 1 in this drop-down will not allow you to continue. Please choose a different subunit position to continue setting up your gateway.
Subunit *	Choose the subunit from the drop-down list. For example: VIC3-2FXS-E/DID-SCCP.

SCCP Endpoints Fields

Option	Description
Gateway Name	This read-only field is populated from the analog gateway for the SCCP protocol. This is a mandatory field.
Slot *	This read-only field is populated from the gateway units. This is a mandatory field.
Subunit Position *	This read-only field is populated from the gateway units. This is a mandatory field.
Port Number *	This read-only field is populated from the gateway units. This is a mandatory field.
Product Type *	Choose the product type from the drop-down ist. For example: Analog Phone. This is a mandatory field.
Device Protocol *	Choose the device protocol from the drop-down list. This is a mandatory field.
Device Name *	This read-only field is populated from the analog gateway. This is a mandatory field.
Description	When the endpoint is added, the default description is the Device Name that can be updated if required. This is an optional field and accepts a string value.
Device Pool *	Choose the device pool from the drop-down list. For example: Cu2Si2-DevicePool. This is a mandatory field.
Phone Button Template *	Choose the phone button template from the drop-down list. For example: Standard Analog. This has a specific phone button template for the analog gateway. This is a mandatory field.
Common Phone Profile *	Choose the common phone profile from the drop-down list. For example: Standard Common Phone Profile. It includes the attributes (services or features) that are associated with a particular user. This is a mandatory field.
Calling Search Space	From the drop-down list, choose the appropriate calling search space. The calling search space specifies a collection of partitions that are searched to determine how a collected (originating) number should be routed.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.
Location *	Choose a location from the drop-down list. For example: Cu2Si2-Location. This is a mandatory field.
AAR Group	Specify the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth.
Owner	Choose from the drop-down list.

Field	Description
Always Use Prime Line for Voice Message *	Choose the required options from the drop-down list. For example: On, Off or Default. This is a mandatory field. This specifies whether the device will always use the prime line for voice messages.
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.
Transmit UTF-8 for Calling Party Name	Keep the check box clear.
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. Note: If the Called Party Transformation CSS is configured as <None>, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	Select the check box.
Allow Control Of Device From CTI	Select the check box.
Logged Into Hunt Group	Select the check box.
Calling Party Transformation CSS (Caller ID For Calls From This Phone)	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Note: If the Calling Party Transformation CSS is configured as <None>, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Use Device Pool Calling Party Transformation CSS (Caller ID for Calls From This Phone)	Select the check box.
Calling Party Transformation CSS (Device Mobility Related Information)	
Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)	Select the check box.
BLF Presence Group *	Choose the presence group for busy lamp field buttons from the drop-down list. For example, **Standard Presence group** is the default value. This is a mandatory field.

Field	Description
Device Security Profile *	Choose options from the drop-down list. For example: Analog Phone - Standard SCCP Non-Secure Profile. This is mandatory field.
MLPP Domain	If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device pool of this device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	Choose options from the drop-down list. For example: **On**, **Off**, or **Default**. This is a mandatory field.
MLPP Preemption	Choose options from the drop-down list. For example: **Disabled**, **Forceful**, or **Default**. This is a mandatory field. Note: If there are any changes to be performed to analog phone line then do not refer line settings. For example: Changing CSS is done under Subscriber Management.
Line	Click + to expand **Line**.
Pattern *	Choose the route pattern from the drop-down list. For example: 08231006
Enduser	Click + to expand **Enduser**.
User ID	Choose the available user ID from the drop-down list. For example: Subscriber 1
Product Specific Configuration Layout	Click + to expand **Product Specific Configuration Layout**.
Key	Enter the Key for the product specific configuration layout. For example: stcapRegCap.
Value	Enter the Value for the product specific configuration layout. For example: 0.

Note: For more optional field information, see *Configure Phones*.

MGCP Endpoints Fields

You can configure multiple endpoints for an MGCP gateway.

Option	Description
Domain Name	This read-only field is populated from the analog gateway for the MGCP protocol. This is a mandatory field.
Slot *	This read-only field is populated from the gateway units. This is a mandatory field.
Subunit Position *	This read-only field is populated from the gateway units. This is a mandatory field.
Port Number *	This read-only field is populated from the gateway units. This is a mandatory field.
Product Type *	Choose the product type from the drop down list. For example: Analog Phone. This is a mandatory field.
Device Protocol *	Choose the device protocol from the drop-down list. For example: SCCP. This is a mandatory field.
Protocol Side *	This is a read-only field except when creating a device. This is a mandatory field.
Class *	This is a read-only field except when creating a device. This is a mandatory field.
Device Name *	This read-only field is populated from the analog gateway. This is a mandatory field.
Description	When the endpoint is added, the default description is in the format: *Endpoint for slot/subunit/port n/n/n gateway @domain* that can be updated if required. This is an optional field and accepts a string value.
Device Pool	Choose the device pool from the drop-down list. For example: Cu2Si2-DevicePool. This is a mandatory field.
Calling Search Space	Choose the calling search space name from the drop-down list. This is an optional field.
Common Device Configuration	Specify the Configuration name of the device. This is an optional field.
Network Locale	Choose the location from the drop-down list. This is an optional field.
Location *	Choose a location from the drop-down list. For example: Cu2Si2-Location. This is a mandatory field.
Media Resource Group List	Enter a media resource to allocate for a device. This is an optional field.
AAR calling search space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) from the drop-down list. This is an optional field.

Field	Description
User Trusted Relay Point	Choose one of the following values: • **Off** - Choose this value to disable the use of a Trusted Relay Point (TRP) with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **On** - Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **Default** - If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
AAR Group	Specify the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth.
Geolocation	Specify the location name. This is an optional field.
Transmit UTF-8 for Calling Party Name	Keep the check box clear.
Port Number *	Configure the ports for the MGCP Endpoint. This is a mandatory field.
Trunk *	This field value auto-populates depending on the value set for the Port Number. This is a mandatory field.
Trunk Direction *	The field value auto-populates depending on the value set for the Number. This is a mandatory field.
Trunk Level *	The field value auto-populates depending on the value set for the Number. This is a mandatory field.
Attendant DN	Specify this field for group start and loop start. This is a mandatory field.
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls.
Num Digits *	Enter the number of significant digits to collect between 0 to 32.
Expected Digits *	Enter the number of digits that are expected on the inbound side of the trunk. You can leave zero as the default value, if you are unsure.

Field	Description
SMDI Port Number (0 - 4096) *	Enter the first SMDI port number of the T1 span. If you set this parameter to a nonxero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue beyond this span.
Unattended Port	Select this check box to indicate an unattended port on this device.
Line	Click + to expand **Line**.
Label	Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line and phone combination.
E164 Mask	Indicate a phone number (or mask) that is used to send Caller ID information when a call is placed from the line. You can enter a maximum of 24 numbers, the international escape character + and 'X' characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.
Dirn, Pattern *	Choose the route pattern from the drop-down list. For example: 08231006.
Dirn, Route Partition	Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the **Directory Number** field is unique within the partition that you choose. If you do not want to restrict access to the directory number, choose <None> for the partition.
Enduser	Click + to expand **Enduser**.
User ID	Choose the available user ID from drop-down list. For example: Subscriber 1.
Index	This field is the line position on the device. If left blank, an integer is automatically assigned.
Trunk Selection Order *	Choose the order from the drop-down list to display the call routing logic for the route pattern.

Config: Product Specific Configuration Layout Fields

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

6.8.13. Set up SIP Local Gateway

Before You Begin

- You must configure an IOS Device at the customer hierarchy node.
- You must configure an NDL containing the Cisco Unified CM for the customer.
- You must configure a SIP Trunk at the customer hierarchy node.

A SIP Local Gateway is a logical gateway running on a physical IOS device.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer for which you are setting up the SIP Local Gateway.
3. Choose **Device Management > IOS > SIP Local Gateways**.
4. Click **Add**.
5. On the **SIP Local Gateways** screen, complete at minimum, the mandatory *SIP Local Gateways Fields*.
6. Click **Save**.
    - The SIP Local Gateway appears in the **SIP Local Gateway** list view.
    - The HcsAddSipLocalGwEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
    - The HcsAddSipLocalGwDialPeerEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each dial peer.

SIP Local Gateways Fields

Field	Description
Name *	Enter a name for the SIP Local Gateway. This field is mandatory.
Description	Enter a description for the SIP Local Gateway.
IOS Device *	Choose the IOS Device on which the SIP Local Gateway is located. This field is mandatory. Note: An IOS Device can have only one SIP Local Gateway. Once selected, the IOS Device cannot be changed.
Country *	Choose the country where the SIP Local Gateway is. This field is mandatory. The country selected must be the same country as the Site to which the SIP local gateway will be associated.
CUCM Publisher *	Choose the CUCM Publisher. All CUCM Publishers that are in the customer's NDL are displayed. This field is mandatory. The chosen CUCM Publisher must be the same as the CUCM Publisher in the NDL for the Site to which the SIP local gateway will be associated.
SIP Trunk *	Choose the SIP Trunk from the ones available on the CUCM Publisher. This field is mandatory. Note: Only SIP Trunks configured at the customer hierarchy are available. If the customer uses a shared CUCM, then SIP Trunks must be manually configured at the customer level in VOSS-4-UC to be selectable here.
Gateway Address	Gateway Address. This field is read-only and is derived from the selected SIP Trunk. Note: If a SIP Trunk has multiple destination addresses, only the first one is used.
Gateway Port	Gateway Port. This field is read-only and is derived from the selected SIP Trunk.
Run on Every Node	Indicates whether call processing is distributed across all CUCM subscriber nodes. This field is read-only and is derived from the selected SIP Trunk.
Dial Peer Info	If the **Run on Every Node** is cleared then the Call Manager Group members are displayed in priority order. If the **Run on Every Node** check box is selected, then all CUCM nodes in the cluster are displayed, but without priority.
Enable Command Builder *	Select this check box to have Command Builder generate commands when SIP Local Gateway is added, deleted, or modified. Default = Selected.
Override Voice Translation Limit ** Warning may invalidate Command Builder Configuration**	Select this check box to override Voice Translation Limit if E164 associations exceed 80. Default = Cleared.

6.8.14. Delete a SIP Local Gateway

Procedure

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

2. Choose **Device Management > IOS > SIP Local Gateways**.
3. Select the check box next to the SIP Local Gateway that you want to delete, and then click **Delete**.
    - The SIP Local Gateway is removed from the **SIP Local Gateway** list view.
    - The HcsDeleteSipLocalGwEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
    - The HcsDeleteSipLocalGwDialPeerEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each dial peer.
    - If the SIP Local Gateway is associated with any sites, the events for disassociating a SIP Local Gateway from a Site are generated for each associated site. See “Disassociate a SIP Local Gateway from a Site” for details.

6.8.15. Update a SIP Local Gateway

Use this procedure to update a SIP Local Gateway. Also use this procedure if you have updated the SIP Trunk associated with the SIP Local Gateway.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer whose SIP Local Gateway you are updating.
3. Choose **Device Managment > IOS > SIP Local Gateways**.
4. Click the SIP Local Gateway to update.
5. On the **SIP Local Gateways** screen you can update only the following fields:

Field	Description
Name	Enter a name for the SIP Local Gateway. This field is mandatory.
Description	Enter a description for the SIP Local Gateway.
Enable Command Builder	Select this check box to have Command Builder generate commands when SIP Local Gateway is added, deleted, or modified.

   However, you can update the SIP Trunk in **Device Management > CUCM > SIP Trunks**.
6. Click **Save**.
    - If you changed the SIP Local Gateway name, the Gateway Name for generated commands is updated in the IOS Commands log.
    - If the **Run on Every Node** check box is selected for SIP Trunk, the HcsUpdateSipLocalGw1EVT and HcsUpdateSipLocalGw1EVT events are generated.

      If the **Enable Command Builder** check box is selected, the IOS Command Builder generates the default IOS commands associated with the events.

6.8.16. IOS Gateway Manual Configuration

VOSS-4-UC does not generate any controller, interface, or dial peer commands for the gateway. This has to be manually added after the command builder has generated the gateway configuration.

The steps shown here are for adding a PRI Trunk to connect to the PSTN.

Procedure

1. Configure PRI on a channelized E1 or T1 controller with the following commands:
   a. controller <T1 or E1><slot/port>

      where slot/port is the controller location in the gateway
   b. framing <esf | sf or crc4 | non crc4>

      esf/sf for T1 and crc4/non crc4 for E1
   c. linecode <b8zs | ami or bdb3 | ami>

      b8zs/ami for T1 and hdb3/ami for E1
   d. clock source <internal/line>
   e. pri-group timeslots <1-24 | 1-31>

      Use all channel on the trunk 1-24 for T1 and 1-31 for E1
2. Configure Serial Interface with the following commands:
   a. interface serial <slot/port>:<23 | 15>

      slot/port similar to the above for controller and use 23 for T1 and 15 for E1
   b. no ip address
   c. encapsulation hdlc
   d. isdn protocol-emulate <network | user>
   e. isdn switch-type <switch-type>

      See IOS documentation for supported switch types.
   f. isdn incoming-voice voice
   g. isdn bchan-number-order <ascending | descending>
   h. no cdp enable
3. Configure POTS dial peer with the following commands:
   a. dial-peer voice 95 pots
   b. translation-profile incoming <91XX>

      For incoming call:
      - use 9111 when both called and calling number have NOA
      - use 9121 when called number does not have NOA but Calling number has NOA
      - use 9112 when calling number does not have NOA but Called number has NOA
      - use 9122 when both called and calling number do not have NOA

c. translation-profile outgoing <90XX>

   For outgoing call:

   - use 9111 when both called and calling number have NOA
   - use 9121 when called number does not have NOA but Calling number has NOA
   - use 9112 when calling number does not have NOA but Called number has NOA
   - use 9122 when both called and calling number do not have NOA

d. destination-pattern 90[1-9]T

e. incoming called-number .

f. no digit-strip

g. direct-inward-dial

h. port <slot/port>:<23 | 15>

   Similar to what is configured for serial interface

i. no register e164

Example IOS gateway manual configuration

```
controller T1 0/0/0
framing esf
linecode b8zs
clock source line
pri-group timeslots 1-24

interface serial 0/0/0:23
no ip address
encapsulation hdlc
isdn protocol-emulate user
isdn switch-type  primary-net5
isdn incoming-voice voice
isdn bchan-number-order descending
no cdp enable

dial-peer voice 95 pots
translation-profile incoming 9111
translation-profile outgoing 9011
destination-pattern 90[1-9]T
incoming called-number .
no digit-strip
direct-inward-dial
port 0/0/0:23
no register e164
```

6.8.17. Associate a SIP Local Gateway to a Site

Before You Begin

These restrictions apply:

- The SIP Local Gateway and the target site must be in the same country.
- The SIP Local Gateway and the target site must have the same CUCM Publisher.
- The target site must have a site dial plan deployed.

Use this procedure to associate a SIP Local Gateway with a site.

Note:

- A SIP Local Gateway can be associated with multiple sites given the prerequisite conditions are met.
- A site can be associated with multiple SIP Local Gateways given the prerequisite conditions are met.
- If a SIP Local Gateway is deleted, all existing site associations are disassociated.
- If a site is deleted through **Site Management > Delete Site** and at least "Remove Dial Plan Items" is selected, all SIP Local Gateway associations for that site are disassociated.
- If a site dial plan is deleted, all SIP Local Gateway associations are disassociated.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site for which you want to associate a SIP Local Gateway.

   If you do not have the path set to a site, you are prompted to select the site.
3. Choose **Site Management > Associate SIP Local Gateway**.
4. Click **Add**.
5. Select the SIP Local Gateway you want to associate with the site from the menu.

   Only SIP Local Gateways that have the same country and CUCM Publisher configuration as the site are available to be selected.
6. Click **Save**.
   - The SIP Local Gateway appears in the **Associate SIP Local Gateway** list view.
   - The HcsSipLocalGwAddSitePstnEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - For each Area Code defined on the target site's dial plan, the HcsSipLocalGwAddSiteAreaCodeEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the site has an existing E.164 to DN Association (N to N), either the HcsSipLocalGwAddE164AssociationEVT (for N to N) or the HcsSipLocalGwAddMultiE164AssociationEVT event (for N to 1) is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the site has an existing Voice Mail Pilot Number Association, the HcsSipLocalGwAddVoiceMailPilotNumberEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the Dial Plan Schema Group that is associated with the customer dial plan has the associateLboGateway custom workflow provisioned, the associateLboGateway custom workflow is executed.

- The Site association to the SIP Local Gateway creates a Route Group with the SIP Trunk created and associated to the SIP Local Gateway.

6.8.18. Disassociate a SIP Local Gateway from a Site

Use this procedure to disassociate a SIP Local Gateway from a site.

Note: Prior to VOSS-4-UC, IOS commands generated at a site were lost when the site was deleted.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **Site Management > Associate SIP Local Gateway**.
3. Select the check box next to the SIP Local Gateway you want to disassociate, then click **Delete**.
   - The SIP Local Gateway association is removed from the **Associate SIP Local Gateway** list view.
   - The HcsSipLocalGwDelSitePstnEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - For each Area Code defined on the site's dial plan, the HcsSipLocalGwDelSiteAreaCodeEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event. If Area Codes are shared across multiple sites and associated with the same gateway, the commands are generated only when the gateway is disassociated from the last site that shares the Area Code.
   - If the site has an existing E.164 to DN Association, either the HcsSipLocalGwDelE164AssociationEVT (for N to N) or HcsSipLocalGwDelMultiE164AssociationEVT (for N to 1) event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the site has an existing Voice Mail Pilot Number Association, the HcsSipLocalGwDelVoiceMailPilotNumberEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event.
   - If the Dial Plan Schema Group that is associated with the customer dial plan has the unassociateLboGateway custom workflow provisioned, the unassociateLboGateway custom workflow is executed.

Note: When a SIP Local Gateway is disassociated from a site because the site is deleted, IOS commands are copied from the site to the customer level before the site is deleted. Select **Device Management > IOS > Commands** to view the copied IOS commands.

6.8.19. View IOS Commands Log

Using the IOS Commands log, an administrator can see a list of command sets that were triggered by different events. An administrator can copy the IOS Commands template and paste it into the IOS device CLI to be executed.

By default, the command sets are listed with the most recent at the top.

Note: Deleting a hierarchy node, such as a site, deletes all IOS Command Builders and associated IOS Commands templates configured at the hierarchy node.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the level for which you want to view IOS Commands.
3. Choose **Device Management > IOS > Commands**. A table containing the Command Builders that have been triggered is displayed. The table contains this information:

Column	Description
Timestamp	The time of the event that triggered the Command Builder.
Device Name	The IOS device associated with the event that fired the Command Builder.
Gateway Name	The SIP Local Gateway or Analog Gateway associated with the event that fired the Command Builder.
Command Builder	The name of the Command Builder that was triggered. To view the IOS Commands template associated with a Command Builder, click the Command Builder name. The Command Builder configuration is displayed, including the IOS Commands template.
Description	The description of the Command Builder that was triggered.
Device Deleted	Select this check box if the associated device has been deleted.
Hierarchy	The hierarchy level of the event that triggered the Command Builder.

6.8.20. Consolidate IOS Commands

To copy IOS commands to an IOS device CLI that is generated by multiple events, follow these steps:

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer or site for which you want to consolidate IOS commands.
3. Choose **Device Management > IOS > Consolidate Commands**.
4. Click **Add**.
5. On the **Consolidate Commands** screen, complete at minimum, the mandatory *Consolidate Commands Fields*.
6. Click the required command templates listed in the **Available** list, and click **Select** to move them to the **Selected** list.

   Click **Remove** to unselect a command template.

   Note:

   You can change the order of the command templates by clicking **Move Up** and **Move Down**. However, the consolidated commands are generated in chronological order regardless of the order of the selected command templates.

7. Click **Save**.

   The new command consolidation instance appears in the list.

8. Click the command consolidation instance you created.

   In the Command Template field, all the commands from the command templates you selected appear in one window. Comments are used to separate and identify the source command templates. You can edit the consolidated commands.

   Any modifications to the Command consolidation, displays the entire list of commands in a single instance. The commands present earlier to the modification cannot be viewed separately as the commands from the earlier events are treated as a single instance.

What to Do Next

After you have consolidated the IOS commands you want, copy them from the Commands Template field to the IOS device CLI.

Consolidate Commands Fields

Field	Description
Name *	Enter a unique name for the command consolidation. This field is mandatory.
Description	Enter an optional description for the command consolidation.
IOS Device *	Choose the IOS device from which you want to consolidate commands.
Device Type *	Choose the device types for which you want to consolidate commands. **IOS Device** Choose this to get commands for the IOS device and any SIP Local Gateway or Analog Gateway hosted on that device. **SIP Local Gateway** Choose this to get commands only for the SIP Local Gateway. **Analog Gateway** Choose this to get commands only for the Analog Gateway. You do not get commands for devices that have been deleted. Note: If you select site hierarchy, only specific commands such as IOS Device or SIP Local gateway are displayed. To view both the IOS and Analog gateway commands, choose the customer hierarchy path.

6.8.21. Regenerate IOS Commands

Because the variables that are used in generating IOS commands may change, you may want to regenerate IOS commands with the latest configuration. IOS commands can be regenerated for the following devices:

- IOS Device
- SIP Local gateway
- Analog Gateway

Regenerating commands for an IOS Device also regenerates commands for any SIP Local gateway or Analog Gateway hosted on the IOS Device.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose one of the following depending on the device for which you want to regenerate IOS commands:
   - **Device Management > IOS > IOS Devices** for an IOS Device and any gateways it hosts.
   - **Device Management > IOS > SIP Local Gateways** for a SIP Local Gateway.
   - **Device Management > IOS > Analog Gateways** for an Analog Gateway.
3. Click the device for which you want to regenerate commands.
4. Choose **Action > Regenerate IOS Commands**.

IOS commands for the events that had occurred for the selected device are regenerated. All old IOS commands for the selected device are removed.

What to Do Next

View the regenerated commands in the IOS Commands log. See *View IOS Commands Log*.

6.9. Prime Collaboration Assurance

6.9.1. Role Mapping for Prime Collaboration Assurance

Service providers deploying VOSS-4-UC use role-based access control (RBAC) to restrict certain management actions to a specific set of users. Administrators at each level have access to the information in all hierarchy levels below them.

Prime Collaboration Assurance roles are hierarchical in the following order:

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

VOSS-4-UC roles map to the Prime Collaboration Assurance roles shown in the following table. You can find Roles in VOSS-4-UC under **Role Management > Roles**. The three drop-down lists that are important in VOSS-4-UC are **Hierarchy Type**, **Service Assurance Role Type**, and **HCS Component Access**.

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

Role Mapping Between VOSS-4-UC and Prime Collaboration Assurance

Hierarchy Type in VOSS-4-UC	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
Provider	Administrator	Fulfillment and Service Assurance	**Super Administrator**, System Administrator, Network Administrator	Provider roles are always the top organization unit in the VOSS-4-UC navigation tree. The Provider roles can see all devices, including shared devices such as Cisco Unified Border Element (SP Edition). A Provider with this role has Administrative level access to VOSS-4-UC and Prime Collaboration Assurance.
		Service Assurance Only		A Provider with this role has Administrative level access to VOSS-4-UC and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Provider with this role has Administrative level access to VOSS-4-UC
	Operator	Fulfillment and Service	**Operator**, Help Desk	A Provider with this role has Administrative level read-only access to VOSS-4-UC and Prime Collaboration Assurance.

Hierarchy Type in VOSS-4-UC	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
		Service Assurance Only		A Provider with this role has Administrative level read-only access to VOSS-4-UC and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Provider with this role has Administrative level read-only access to VOSS-4-UC and Hosted Collaboration Mediation-Fulfillment.
Reseller	Administrator	Fulfillment and Service Assurance	**Network Administrator**	These roles can only see the customer information that belongs to your Reseller organization. A Reseller with this role has Administrative level access to VOSS-4-UC, Hosted Collaboration Mediation-Fulfillment, and Prime Collaboration Assurance.
		Service Assurance Only	**Network Administrator**	A Reseller with this role has Administrative level access to VOSS-4-UC and Prime Collaboration Assurance.

Hierarchy Type in VOSS-4-UC	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
		Fulfillment Only	Not Applicable	A Reseller with this role role has Administrative level access to VOSS-4-UC and Hosted Collaboration Mediation-Fulfillment.
	Operator	Fulfillment and Service	**Operator**, Help Desk	A Reseller with this role has Administrative level read-only access to VOSS-4-UC and Prime Collaboration Assurance.
		Service Assurance Only	**Operator**, Help Desk	A Reseller with this role has Administrative level read-only access to VOSS-4-UC and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Reseller with this role has Administrative level read-only access to VOSS-4-UC.
Customer	Administrator	Fulfillment and Service Assurance	**Network Administrator**,	With this role you can only see your own customer information. A Customer with this role has Administrative level access to VOSS-4-UC and Prime Collaboration Assurance.
		Service Assurance Only	**Network Administrator**,	A Customer with this role has Administrative level access to to VOSS-4-UC and Prime Collaboration Assurance.

Hierarchy Type in VOSS-4-UC	Service Assurance Role Type	HCS Component Access	Prime Collaboration Assurance Role	Notes
		Fulfillment Only	Not Applicable	A Customer with this role has Administrative level access to VOSS-4-UC.
	Operator	Fulfillment and Service Assurance	Operator, Help Desk	A Customer with this role has Administrative level read-only access to VOSS-4-UC, Hosted Collaboration Mediation-Fulfillment, and Prime Collaboration Assurance.
		Service Assurance Only	Operator, Help Desk	A Customer with this role has Administrative level read-only access to VOSS-4-UC and Prime Collaboration Assurance.
		Fulfillment Only	Not Applicable	A Customer with this role has Administrative level read-only access to VOSS-4-UC and Hosted Collaboration Mediation-Fulfillment.

Rules for Creating Domain Manager Adapter and Shared Data Repository Users

1. Synchronize a DMA or SDR user into VOSS-4-UC using LDAP at the Provider hierarchy level. If you add the user manually in VOSS-4-UC, the user is not pushed to Prime Collaboration Assurance.
2. Assign each DMA user a Domain Manager Adapter (DMA) role. Check the role of the user in VOSS-4-UC (**User Management > Users** - **Base** tab), then check the HCS Component Access field (in **Role Management > Roles**) to see if the user has an Assurance role. If the user is assigned a Fulfillment role only, then the user is not pushed to Prime Collaboration Assurance.

Changes to User Roles After an LDAP Sync

If you make role changes to the user after the user is synched into VOSS-4-UC using LDAP, the changes affect the DMA SDR as follows:

- If the role change is from a DMA role to another DMA role, the SDR is updated with the new role name.
- If the role change is from a DMA role to a non-DMA role, the SDR user is deleted.
- If the SDR user is deleted, and the user is modified so that the user's role is changed to a DMA role again, the DMA SDR User is recreated with the DMA role.
- If the user is moved to a different hierarchy level, rules are applied based on the role that the user is moving to.
- If a site does not have any DMA roles, then the SDR user is deleted for any user that is moved to the Site hierarchy level.
- For DMA roles, the user must be a Provider Administrator, Reseller Administrator, Customer Administrator, or Operator on VOSS-4-UC. Site Operators are not pushed to DMA.

6.9.2. Prime Collaboration Assurance Integration

Before You Begin

- Review Role Mapping for Prime Collaboration Assurance to understand how your VOSS-4-UC roles map to Prime Collaboration Assurance roles.
- In Prime Collaboration Assurance, enable SFTP. SFTP is not enabled by default.
- Ensure that the smuser account is available in the Prime Collaboration Assurance, and you can log in. The default SFTP credential in PCA is smuser/smuse.

Use this workflow to integrate VOSS-4-UC with Prime Collaboration Assurance.

Procedure

1. Configure Prime Collaboration Assurance.
2. Set up Prime Collaboration Assurance to monitor the Unified Computing System.
3. Add the Service Provider space and Application space under Address space information when adding Cisco Unity Connection and Cisco IM and Presence server to VOSS-4-UC. Prime Collaboration Assurance uses the server's Service provider space to monitor the applications. See *Set Up IM and Presence Service Servers*

4. Add Cisco IM and Presence Service subnode information to VOSS-4-UC if you have multiple instances of Cisco IM and Presence Service deployed.
5. Ensure that your Unified Communications applications have all the needed credentials. At a minimum, you require credentials for Administration, platform, SNMP, JTAPI, and HTTP.

   Note:

   Depending on what you are monitoring, other credentials may be needed. For more information about the required protocols, support, and credentials to set up devices for Prime Collaboration Assurance monitoring, see:

   http://docwiki.cisco.com/wiki/Setting_up_Devices_for_Prime_Collaboration_Assurance.
6. Synchronize your customer information with VOSS-4-UC. See *Set Up Cisco Unified Communications Manager Servers* for more information.
7. (Optional) Ensure that the Session Border Controller has the required credentials in Hosted Collaboration Mediation-Fulfillment.
8. Ensure that the CPE (analog gateway or LBO deployed at CPE) has the required credentials in VOSS-4-UC under Devices.
9. Enter the SNMP commands manually on the Local Break Out (LBO) gateway or analog gateway. This task is required to manage the LBO gateway and analog gateway in Prime Collaboration Assurance.

   Note:

   IOS default command builder does not generate SNMP commands. The administrator must manually enter the SNMP commands.
10. Add Prime Collaboration Assurance to VOSS-4-UC (**Device Management > Prime Collab > Servers**). (Administration and SFTP credentials are required.)
11. Onboard the customer to Prime Collaboration Assurance using the Cisco Unified Communications Manager administrative interface. In HCMF, the CHPA pushes SNMP, Syslog, and Billing server configuration information to your VOSS-4-UC automatically. Add Syslog and SNMP configurations manually for Cisco Unity Connection and IM and Presence Service before onboarding.

    Note:

    Configure these credentials in Unified CM nodes to ensure a successful CHPA configuration:

    - Administration credentials for Unified CM
    - Platform credentials for Unified CM
    - SNMP and HTTP credentials for Unified CM
    - SFTP for Prime Collaboration Assurance

    Note:

    This configuration is pushed to Unified CM:

    - The SNMP community string
    - CDR (SFTP of the Prime Collaboration Assurance server)
    - Syslog configuration

    Note:

    JTAPI credentials are optional credentials used for TelePresence session monitoring. They are used to retrieve session status information from TelePresence devices. Create a JTAPI user in the Unified Communications Manager with the required permission to receive JTAPI events on endpoints. The

credentials must be manually configured in Unified CM. Note also that Prime Collaboration Assurance manages multiple call processor clusters and as a result you must ensure that the cluster IDs are unique.

12. Synchronize Active Directory users with VOSS-4-UC.

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

13. To confirm if the Cisco HCM-F (if installed) push and subsequent Device Discovery were successful, verify that the devices are managed in Prime Collaboration Assurance. Review the Current Inventory table at **Operate > Device Work Center** (Prime Collaboration Assurance 10.5.1) or **Device Inventory > Inventory Management** (Prime Collaboration Assurance 11.5 or later). Devices appear in **Inventory Management** with the Managed status. For details on the Prime Collaboration Assurance Inventory table, see the **Manage Inventory** section of Cisco Prime Collaboration Assurance Guide Advanced, available at:

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

    Note:

    In Cisco HCM-F (if installed), you may receive a **Credential-related error message**, but there can be other reasons for this error, such as a firewall issue. We recommend that you use Prime Collaboration Assurance to verify that devices are managed. If a device is not going into the managed state successfully, refer to the **Troubleshooting** section of the **Discover Devices** chapter in Cisco Prime Collaboration Assurance Guide Advanced for troubleshooting tips.

    A list of the devices supported by Prime Collaboration Assurance is available at:

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

14. Check the Prime Collaboration Assurance dashboard.

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

15. Monitor components and devices with Prime Collaboration Assurance.

6.10. Microsoft Devices

6.10.1. Microsoft Devices Introduction

VOSS-4-UC can be used to manage multiple applications within Microsoft's Unified Communications stack including Active Directory, Skype for Business Server, Exchange Server, Skype for Business Online, Exchange Online, and Office 365.

Windows PowerShell is utilized for this purpose. Because PowerShell is native to Microsoft Windows, VOSS-4-UC requires access to at least one Windows computer that will, in turn, execute remote PowerShell cmdlets on VOSS-4-UC's behalf. In this document we will refer to these computers as "VOSS-4-UC PowerShell Proxies", or simply "PS Proxies". If you are using VOSS-4-UC to manage multiple customer domains, you need at least one PS Proxy for each customer domain under management.

VOSS-4-UC will create, via a PS Proxy, a separate PowerShell session for each of the Microsoft applications being managed for a specific customer domain. All of the PowerShell sessions for a particular customer domain may be hosted by the same PS Proxy, or you can configure a separate PS Proxy for each session.

The PS Proxies hosting these PowerShell sessions may be dedicated for this purpose exclusively, but this is not required.

Refer to Appendix: Microsoft Configuration for the software and security requirements and configuration for each of the PowerShell sessions created by VOSS-4-UC.

Sign into VOSS-4-UC as an administrator at a hierarchy level at or above where you will be adding the Microsoft devices. You can add Microsoft devices at the customer level, the provider level, or at any intermediate node above customer. Open the **Device Management** menu.

6.11. Active Directory Server

6.11.1. Active Directory Server Configuration Parameters

Refer to the Provision VOSS-4-UC section in Appendix: Microsoft Configuration for detailed steps and examples.

An example page is shown in *Active Directory Server Configuration Page*.

The configuration parameters are described in the table below.

Active Directory Server Configuration Parameters

Parameter	Description
Version	Currently, the only supported value is `1.0`.
Host Name	IP address or FQDN of the PowerShell Proxy that will be used to create the Active Directory PowerShell session.
Username / Password	Sign-in credentials for the Remote Management Service Account[1]
Domain Name / Domain Username / Domain Password	Sign-in credentials for the Active Directory Management Account[2]
Active Directory Filter	Active Directory search filter. This is the "-Filter" argument to the PowerShell cmdlet *Get-AdUser*. It is a required parameter; to search without filtering, simply specify the single character "*" (without the quotes). For information about advanced filtering, see this article.
Active Directory Search Base	The Active Directory path to search under - typically the distinguished name of the top-level organizational unit containing the user and contact objects to be managed by VOSS-4-UC. This is an optional parameter. The default value is domain's default naming context.

6.12. Skype for Business Server

[1] See *Remote Management Service Account*
[2] For Domain Name / Domain Username / Domain Password, see the Active Directory entry in *Minimum Privileges by UC Application*.

6.12.1. Skype for Business Server Configuration Parameters

Refer to the Provision VOSS-4-UC section in Appendix: Microsoft Configuration for detailed steps and examples.

An example page is shown in *Skype for Business Server Configuration Page*.

The configuration parameters are described in the table below.

Skype for Business Server Configuration Parameters

Parameter	Description
Version	Currently, the only supported value is `6.0`.
Host Name	IP address or FQDN of the PowerShell Proxy that will be used to create the Skype for Business Server PowerShell session.
Username / Password	Sign-in credentials for the Remote Management Service Account[1]
Domain Name / Domain Username / Domain Password	Sign-in credentials for the Skype for Business Server Management Account[2]
Online Username / Password	Credentials for the Skype for Business Server Management Account. Use the username as it appears in the Office 365 Admin Center. The password will be the same as the one you use in the row above.

6.13. Exchange Server

6.13.1. Exchange Server Configuration Parameters

Refer to the Provision VOSS-4-UC section in Appendix: Microsoft Configuration for detailed steps and examples.

An example page is shown in *Exchange Server Configuration Page*.

The configuration parameters are described in the table below.

Exchange Server Configuration Parameters

[1] See *Remote Management Service Account*.
[2] For Domain Name / Domain Username / Domain Password, see the Active Directory entry in *Minimum Privileges by UC Application*.

Parameter	Description
Version	Currently, the only supported value is `1.0`.
Host Name	IP address or FQDN of the PowerShell Proxy that will be used to create the Exchange Server PowerShell session.
Username / Password	Sign-in credentials for the Remote Management Service Account[1]
Domain Name / Domain Username / Domain Password	Sign-in credentials for the Active Directory Management Account[2]
Connection URI	A URI of the form *http://<Exchange Server FQDN>/PowerShell*, where `<Exchange Server FQDN>` is the FQDN of an on-premises Exchange Server hosting the Exchange Admin Center.
Online Username / Password	Credentials for the Active Directory Management Account. Use the username as it appears in the Office 365 Admin Center. The password will be the same as the one you use in the row above.

6.14. Microsoft Online (Office 365 Tenant)

6.14.1. Microsoft Online (Office 365 Tenant) Configuration Parameters

Refer to the Provision VOSS-4-UC section in Appendix: Microsoft Configuration for detailed steps and examples.

An example page is shown in *Microsoft Online (Office 365 Tenant) Configuration Page*.

The configuration parameters are described in the table below.

Microsoft Online (Office 365 Tenant) Configuration Parameters

Parameter	Description
Version	Currently, the only supported value is `1.0`.
Host Name	IP address or FQDN of the PowerShell Proxy that will be used to create the Microsoft Online PowerShell session.
Username / Password	Sign-in credentials for the Remote Management Service Account[1]
Domain Name / Domain Username / Domain Password	Sign-in credentials for the Microsoft Online Management Account[2]
Online Username / Password	Credentials for the Microsoft Online Management Account. Use the username as it appears in the Office 365 Admin Center. The password will be the same as the one you use in the row above.

[1] See *Remote Management Service Account*.
[2] For Domain Name / Domain Username / Domain Password, see the Active Directory entry in *Minimum Privileges by UC Application*.
[1] See *Remote Management Service Account*.
[2] For Domain Name / Domain Username / Domain Password, see the Active Directory entry in *Minimum Privileges by UC Application*.

6.15. Skype for Business Online

6.15.1. Skype for Business Online Configuration Parameters

Refer to the Provision VOSS-4-UC section in Appendix: Microsoft Configuration for detailed steps and examples.

An example page is shown in *Skype for Business Online Configuration Page*.

The configuration parameters are described in the table below.

Skype for Business Online Configuration Parameters

Parameter	Description
Version	Currently, the only supported value is `1.0`.
Host Name	IP address or FQDN of the PowerShell Proxy that will be used to create the Microsoft Online PowerShell session.
Username / Password	Sign-in credentials for the Remote Management Service Account[1]
Domain Name / Domain Username / Domain Password	Sign-in credentials for the Skype for Business Online Management Account[2]
Online Username / Password	Credentials for the Skype for Business Online Management Account. Use the username as it appears in the Office 365 Admin Center. The password will be the same as the one you use in the row above.

6.16. Exchange Online

6.16.1. Exchange Online Configuration Parameters

Refer to the Provision VOSS-4-UC section in Appendix: Microsoft Configuration for detailed steps and examples.

An example page is shown in *Exchange Online Configuration Page*.

The configuration parameters are described in the table below.

Exchange Online Configuration Parameters

[1] See *Remote Management Service Account*.
[2] For Domain Name / Domain Username / Domain Password, see the Active Directory entry in *Minimum Privileges by UC Application*.

Parameter	Description
Version	Currently, the only supported value is `1.0`.
Host Name	IP address or FQDN of the PowerShell Proxy that will be used to create the Exchange Online PowerShell session.
Username / Password	Sign-in credentials for the Remote Management Service Account[1]
Domain Name / Domain Username / Domain Password	Sign-in credentials for the Exchange Online Management Account[2]
Connection URI	All Exchange Online tenants use the same URI: `https://outlook.office365.com/powershell-liveid/`
Online Username / Password	Credentials for the Exchange Online Management Account. Use the username as it appears in the Office 365 Admin Center. The password will be the same as the one you use in the row above.

6.17. Clone a Device Model

6.17.1. 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:

[1] See *Remote Management Service Account*.
[2] For Domain Name / Domain Username / Domain Password, see the Active Directory entry in *Minimum Privileges by UC Application*.

- 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.
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.

6.18. Load Balancing

6.18.1. 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”.

6.18.2. 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.

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.

6.18.3. 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**.
   - 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**.

6.19. Network Device Lists

6.19.1. Network Device List

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

A Network Device List (NDL) is a list of network devices that are assigned to a Site. An NDL can contain one instance each of Cisco HCM-F, Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco WebEx. Only Cisco HCM-F is required.

NDLs can be defined only at the Customer hierarchy level. A customer can have multiple NDLs defined.

NDLs can be defined only by a Provider or Reseller administrator.

The HCM-F device is pre-populated in the NDL and should not be changed.

Shared UC Applications (that is, UC Applications that are defined above the Customer hierarchy level) can be included in an NDL. However, to use that NDL, the customer must be defined as allowing Shared UC Applications.

After an NDL is assigned to any Site, only the following modifications are supported:

- Network Device List Name can be changed.
- Network Device List Description can be changed.
- New devices can be added.

An NDL cannot be deleted if it is assigned to any Site.

Note:

- Unified Communications application clusters are not linked to the customer until the Network Device list is created.
- Only publisher nodes are shown in the drop-down list for Cisco Unified Communications Manager and Cisco Unity Connection.

6.19.2. Configure a Network Device List

1. Log in as provider or reseller administrator.
2. Click **Customer Management > Network Device Lists**.
3. Choose a customer on the hierarchy tree where the NDL is to be created.
4. Click **Add**.
5. Enter a name for the NDL, and optionally a desciption.
6. Click the + next to **Cisco Unified CM**.
7. Choose the Cisco Unified Communications Manager instance from the drop-down list.
8. Optionally, add **Cisco Unity Connection** and **Cisco WebEx** instances to the NDL.
9. Click **Save**.

6.19.3. Network Device List Selection Rules

If an administrator at a hierarchy has access to more than one Network Device List (NDL), the option to choose a specific hardware group or list may be needed in order to provision a set of devices.

The Rule Model Device Selection Type model provides a solution to this problem and instances of it are a set of rules for views and relations at a hierarchy level. A particular NDL can then be selected from a popup form before the Add form of these model types are shown. In this way, the administrator can then select the specific required NDL.

When an instance of the Rule Model Device Selection Type model is added, the target relation or view is specified and more than one set rules can be added for it - one for each relevant Hierarchy Node Type.

In addition, a Default GUI Rule that is applied to the Relation or View is reflected as the Default value for the Permitted Hierarchy Node Type.

In addition to this behavior, these rules apply:

- The NDL popup is only available for Relations and Views.
- Device form fields are filtered according to the device listed in the selected NDL.
- More than one type of device is supported for the selected NDL.
- Any Provisioning Workflow Network Device Filters (NDF) override a selected NDL device choice.
- Only the Add operation supported.
- For details on NDL popups, refer to the topic on Network Device List Selection Rules Advanced Configuration in the Advanced Configuration Guide.

6.19.4. Network Device Rules at a Site

The following rules apply to Network Device Lists (NDLs), network devices and device models at site hierarchies:

For a site which references a NDL, device models cannot exist at this site if these belong to a network device not referenced in the NDL.

Therefore:

1. A device model from a device cannot be added to it if it has a NDL referencing a different device.
2. A NDL cannot be added to it if it has device models that references a different network device than the one referenced in the NDL.

7 Data Sync

7.1. Data Sync Overview and Key Settings

The data of the various devices can be updated on VOSS-4-UC, or also directly on the device. Therefore, it is necessary to periodically synchronize cached VOSS-4-UC data with the data on devices.

Consider an example: when an instance of a Unified CM is added to the system, its data is imported and cached. However, when instances are added, updated or removed from the Unified CM, the cached data in VOSS-4-UC becomes out of sync with data on the device.

If data is deleted from Unified CM before it is deleted from VOSS-4-UC, the error “The specified resource could not be found” is displayed. This means the resource is out of sync and VOSS-4-UC may need to re-sync with Unified CM to delete or update it.

The Data Sync feature provides a means to dynamically synchronize cached VOSS-4-UC data with data on devices. The data sync instance is associated with the connection parameters of a device type in VOSS-4-UC.

Supported devices include:

- HCM-F (if installed)
- Cisco Unified CM
- Cisco Unity Connection
- LDAP
- WebEx

Individual Add, Update and Delete operations carried out by a data sync instance can be disabled on the user interface. If no operation is selected, the default behavior is maintained.

Refer to the Best Practices Guide chapter on Data Sync for additional considerations when managing your data syncs.

7.2. Default Cache Control Policy

A default Cache Control Policy is applied to manage the caching behavior of the system, in other words, it controls how data is read.

The defaults are set as follows:

- Cache Policy for Reads: read from cache then device
- Read Before Write: On Update

- Read After Write: On Add
- Read After Write: On Update
- Model specific overrrides:
  - Model Type: `device/notification_service/*`
    - Cache Policy for Reads: Cache

The following concepts apply:

- Cache only: Unless overridden within the request, instance reads via the API always return the cached version of data. There is no need for the client to query the uncached instance data.
- Cache then device: The API will return the cached data, the GUI will indicate that the data shown is cached and will automatically make an API call requesting non-cached data. It is up to external clients to query the data requesting non-cached data. If this option is selected, data is loaded into the system in two steps:

  1. Load cached data
  2. Load device data

  The 'cached' visual indicator is displayed until the second step is complete.

  The device data overrides the previously displayed data unless the user has made an input:

  a. The fields changed by the user will reflect the user's input and not the device data.

  b. Arrays are blocked for the duration of the device data loading (while the 'cached' flag is displayed) and the user can not add or remove elements until the device data loading completes.

  Data is validated constantly as displayed values change, and validation status always reflects the very latest state.
- Manual: Unless overridden within the request, instance reads via the API always return the cached version of data. An external client using the API needs to provide a button to allow the user to manually retrieve non-cached data.
- No cache: Unless overridden within the request, instance reads via the API always return the uncached version of data that is queried from the device. In this mode the GUI will not show any data until it is retrieved from the device.

For Relation model types, the relation's cache control policy will filter down to the joined device models. For example:

- If the cache control policy of a Relation is Cache then Device, any GET operations that do not specify the cached parameter will return a cached result. It then becomes the client's responsibility to make another request with `cached=false`.
- If the cache control policy of a Relation is Cache only or Manual, then any GET requests that do not specify the cached parameter, return cached data for all joined models.
- If the cache control policy on read is No cache, the Relation will always fetch the latest device data.

7.3. Key Settings for Data Sync

A number of key settings that are available for data sync:

- Model Type lists - define which entities to pull in a given sync (for example, only pull in `device/cucm/User` records from Cisco Unified CM).

- Model Instance filters - limit a sync to a subset of entities in a sync (for example, pull in users with a primary extension starting with 1). This setting requires a system level administrator to expose it on the GUI.
- Actions - select which actions (Add/Update/Delete) are active for a sync. Update tends to be the most effort to run, because for most systems this involves a GET API call for each record and comparing to our data. Add/Del can be determined from the initial list API calls. If you are really only need the Add and/or Del action, then disabling the Update action will likely save considerable time on the sync.
- Quick Import - use the list API responses to update the VOSS-4-UC cache and will not do individual GET calls for each entity for the update. This works well where the list response contains all the values for the entity or only key settings need to be updated. The removal of all the individual GETs means the sync occurs much faster, because VOSS-4-UC is not waiting for the API responses when there are a many entities to update. This is useful if the list and GET responses are needed or if you only need the summary data from the list view.

Note: The Quick Import option is not recommended in most cases, but should only be used for the sync of `device/cuc/ImportUser`. However, *initially* there is an exception to the performance improvement of a quick import sync with `device/cuc/User`:

When quick import is turned on on a sync which has previously run without it, dependent, non-Import User model types use the LIST response data to compare with the resource data which was originally saved using the GET response data. The data sync detects a change and a resource save is initiated for each instance. In the case of `device/cuc/User`, this means that dependent import API calls are made, which result in a long sync time.

Once it has completed, however, *subsequent* quick import syncs should show an improvement over non-quick import syncs, but when changing back to a non-quick import sync, the same effect would likely be observed.

7.4. Data Sync Types

Data synchronization is available with the following functionality:

- Merge data by pulling data that is on the device but not in the cache, to the cache and vice versa
- Pull all data from the device
- Pull only the schema from the device (used for LDAP)
- Pull data from the Change Notification Feature local data collection
- Purge data from the cache
- Push data in the cache to the device

A quick import option is available to fetch only summary data that is contained in a list operation response and not the data for all instances/fields.

For all the syncs in general, the VOSS-4-UC system builds up the lists of entities from both VOSS-4-UC and the device (for example Unified CM) for comparison. The field that is used for this comparison is the key for the device entity, which is typically the unique identifier for the record in the device we that are syncing with. For example, for Unified CM, the identifier is the pkid which is the internal Unified CM database id.

In the case of subscribers, a sync will build up the list of `device/cucm/Users` in VOSS-4-UC and then request from the Unified CM the lists of users it currently has for the comparison. The differences in the lists are then handled according to each sync type.

Details of the sync types are listed below:

- Pull from Device - The VOSS-4-UC resource is updated where the same key is present in both lists. In this case, the device data is the master and the VOSS-4-UC system model data is updated with the device data.
  - For example, if new data is added to the Unified CM so that the VOSS-4-UC system data state for a Unified CM `device/cucm/User` does not show instances that are shown on the Unified CM, pull data synchronization synchronizes the system data with the Unified CM data. For example, a user's Department may be updated on the Unified CM, but this update will only show on the system after Pull from Device synchronization. If a user resource is created in Unified CM but not in VOSS-4-UC, this will add the `device/cucm/User` instance into VOSS-4-UC *at the level the pull sync was run from*, for example at the customer level.
  - In the case where you delete a VOSS-4-UC resource from the device so that the key is in the VOSS-4-UC list but not in the 'device' list, a pull sync will remove the resource in VOSS-4-UC. For example, if the resource is a user in VOSS-4-UC but not in Unified CM, the pull sync will remove the `device/cucm/User` record in VOSS-4-UC.

  If you are pulling device data, for example LDAP users from an LDAP device, the results returned to VOSS-4-UC are dependent on the LDAP server configuration. For example, if the returned results exceed the LDAP server configured maximum and if the server does not support paging, then an appropriate error message is returned.
- Push to Device - The VOSS-4-UC system data state is the master and devices are synchronized with it.
  - Where you delete device data from VOSS-4-UC so that the key is in the 'device' list but it is not in the VOSS-4-UC list, for example deleting a user in VOSS-4-UC, this will remove the user from Unified CM to match the user not existing in VOSS.
  - If new device data is added to the VOSS-4-UC system data so that the resource shows instances that are not shown on the device, push data synchronization synchronizes the device data with the VOSS-4-UC system data. For example, adding a `device/cucm/User` instance to VOSS-4-UC and running a Push to Device sync will add the user record to Unified CM.

  Keys found in both lists are ignored, for example no updates are made for existing records in either direction. So in the `device/cucm/User` example, if the same user exists in both the VOSS-4-UC and Unified CM system, then no update occurs in either direction. In other words, detailed settings may still not match after a Push to Device sync.
- Merge with Device - This is a combination of pull and push data synchronization and takes place in both directions.

  Merge data synchronization synchronizes data between the system and the Unified CM data without overwriting or deleting any data.
  - If you create a resource where the key is in the 'device' list but not in the VOSS-4-UC list (for example, the entity is in Unified CM but not in VOSS-4-UC), then the VOSS-4-UC resource is created. For example, adding a user in Unified CM will create the `device/cucm/User` record in VOSS-4-UC after the merge sync.
  - If you add to a device so that the key is in the VOSS-4-UC list but not the 'device' list (for example, the entity is in VOSS-4-UC but not in Unified CM), then the device resource is created. For example, creating a `device/cucm/User` record in VOSS-4-UC will create the user in Unified CM.

  Keys found in both lists are ignored, for example no updates will be made for existing records in either direction. So in the `device/cucm/User` example, if the same user exists in both the VOSS-4-UC and Unified CM system, then no update occurs in either direction. In other words, detailed settings may still not match after a Merge with Device sync.

- Change Notification Sync - A pull sync of changes stored in the local collection that is updated by the Change Notification Collector service.

  For more details on CNF, refer to the relevant CNF topics in the Data Sync chapter of the Core Feature Guide.

- Purge Local Resources - All resources or instances of device information that exist in the system will be deleted. However, the entities in the device will not be deleted. This option is typically used when cleaning up the system.

Note: Bear in mind that with the above keys list sync logic, in the case of a reversion of the Unified CM to restores/inactive partitions, the relevant pkids might be different in the end state than they were at the last time VOSS-4-UC was in sync with Unified CM before the restore - especially if there was a lot of testing in between.

What this means practically is that there could for example be a user with the same username in both VOSS-4-UC and Unified CM, but if that user's pkid in Unified CM is now different to the one that VOSS-4-UC holds from previous syncs or interactions, then the users will be seen as different even though the usernames are the same.

7.5. Synchronous and Asynchronous Data Sync

A Data Sync is by default set to be asynchronous, in other words other tasks can be carried out while the sync is in progress. However, it can be set to be synchronous so that a workflow step can for example wait for the sync process to complete.

Asynchronous imports initiated by a Data Sync are standalone transactions, in other words they aren't child transactions of the Data Sync execute transaction. Synchronous imports initiated by a Data Sync are children of the Data Sync execute transaction.

7.6. Full Sync

A full pull sync, when runs, empties the changes from the data collection as they don't need to be processed by the Change Notification Sync. Use the disabled operations and the model type list of the full sync to filter the changes to remove. If a model instance filter is included, no changes are removed.

7.7. Enable a Scheduled Data Sync

By default, when a Cisco Unified Communications Manager or Cisco Unity Connection device is set up in VOSS-4-UC, a full data sync instance is created to perform the initial sync of all data from the device. A Change Notification Sync type also gets created in the Data Sync page. In addition, a Schedule is created to execute that data sync every 14 days, but is disabled by default. We recommend running the full data sync manually only when necessary. However, if a regularly scheduled sync is desired, the schedule can be enabled as follows:

7.7.1. Procedure

1. Log in as provider administrator.
2. Choose **Administration Tools > Scheduling**.
3. Choose the schedule instance that matches this naming convention:

   HcsSync-<ip_address>-<device_name>-SCHED. For example:

   HcsSync-192.0.2.24-CUCM01-SCHED
4. Select the **Active** check box.
5. Click the **Multiple Executions** tab, and update the interval, if desired.
6. Click **Save**.

The full data sync executes immediately, and executes again according to the schedule.

7.8. Manually Run the Default Data Sync

You can always manually run the default data sync when there have been updates to Cisco Unified Communications Manager or Cisco Unity Connection devices that need to be synced into VOSS-4-UC.

Note: Manual run of the change notification sync is not supported.

7.8.1. Procedure

1. Log in as provider or reseller administrator.
2. Choose **Device Management > Advanced > Perform Publisher Actions**.
3. From the **Action** drop-down, choose **Import**.
4. From the **App Type** drop-down, choose **CUCM Device** or **CUC Device**.
5. From the Available Clusters list, choose the device and click **Select**.
6. Click **Save**.

7.9. Controlling a Data Sync with a Model Type List

Using a Model Type List (MTL), you can control the types of data that are synced into VOSS-4-UC from Cisco Unified Communications Manager or Cisco Unity Connection devices. Controlling the types of data that are synced can greatly improve sync performance. The MTL is a list of device models associated with the device type, for example, Phone and Line device models that are associated with the Unified CM device.

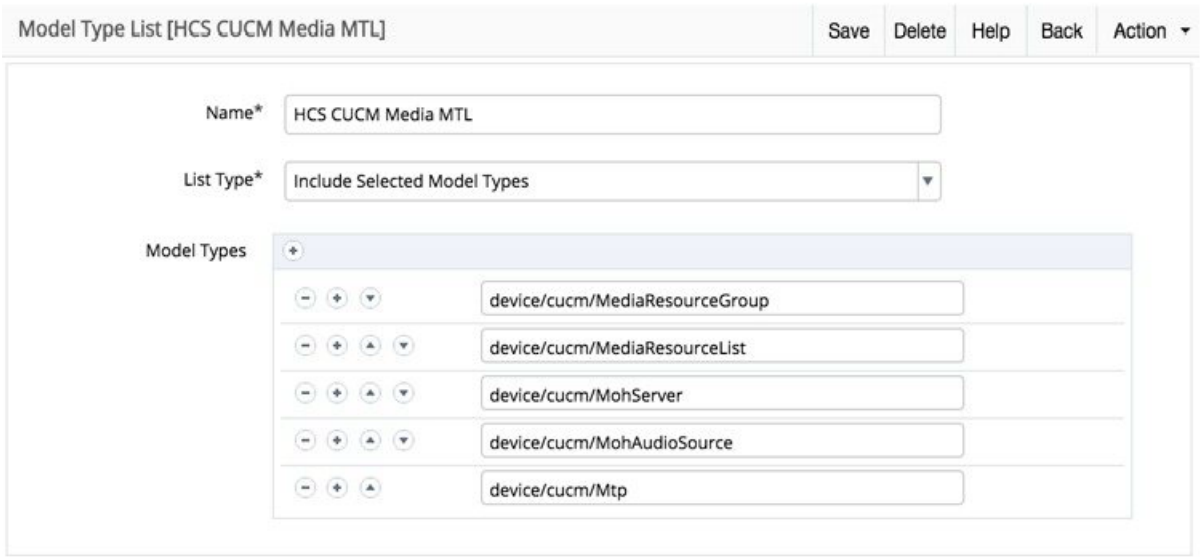
These are the possible types of Model Type Lists:

- Include Selected Model Types - This list represents the device models to explicitly include in the data sync.

- Exclude Selected Model Types - This list represents the device models to explicitly exclude from the data sync.
- Ordered List - This list represents the device models to explicitly include in the data sync in the order they must be synced.

A data sync created with an empty Model Type List attribute results in the subsequent import(s) synchronizing all device models for the corresponding device.

Here's an example of an include MTL:



A data sync using this MTL will sync all Media Resource Group, Media Resource Lists, Music on Hold servers and audio sources, and Media Termination Points. No other data will be synced from Unified CM.

It is recommended to define MTLs for sets of data that are being modified on the device directly, particularly Unified CM because this is where the bulk of the configuration data for each customer resides. By defining MTLs that target specific data sets rather than doing a full sync, the performance of VOSS-4-UC can be maintained with better response times and quicker transaction execution. Some Unified CM device models to avoid unless needed are Users, Phones, and Lines, as there may be large numbers of these in the Unified CM and result in a lengthy data sync operation.

Data sync overhead can be further reduced if you want to sync only new and deleted instances of the device model and not updates to existing instances. This can be done by unchecking the Refresh Existing (Changed) Data check box on the Data Sync configuration page. This check box controls whether existing device model instances are updated in VOSS-4-UC in addition to importing new instances and removing deleted instances. If checked, all device model instances must be synced and examined. If unchecked, only new and deleted instances need to be imported and the data sync will run considerably faster.

7.10. Create a Targeted Model Type List

If you manage data on Cisco Unified Communications Manager (Unified CM) or Cisco Unity Connection directly on a regular basis, perhaps for configuration that is not orchestrated from VOSS-4-UC, such as media resources, it is recommended to create a Model Type List and Data Sync specifically targeting the data items you are managing. This ensures each data sync is highly optimized for the data being changed on Unified CM directly and minimizing the load on VOSS-4-UC. To create a targeted Model Type List:

7.10.1. Procedure

1. Log in as Provider level admin or higher.
2. Select **Administration Tools > Model Type List**.
3. Click **Add**.
4. Specify the name of the Model Type List.

   It is recommended to use a naming convention that makes it easy to identity the MTL in a list view, such as Unified CM Media Resources.
5. From the **List Type** drop-down, choose the list type:
   - Choose **Include Selected Model Types** if the list of device models you want to sync is relatively short.
   - Choose **Exclude Selected Model Types** if the list of device models you want to sync is relatively long. Exclude device models that tend to have lots of instances, like users, phones, and lines.
   - Choose **Ordered List** if the list of device models you want to sync is relatively short and the order in which they are synced matters.
6. Add Model Types to the list of device models that are to be included or excluded according to the List Type selected.

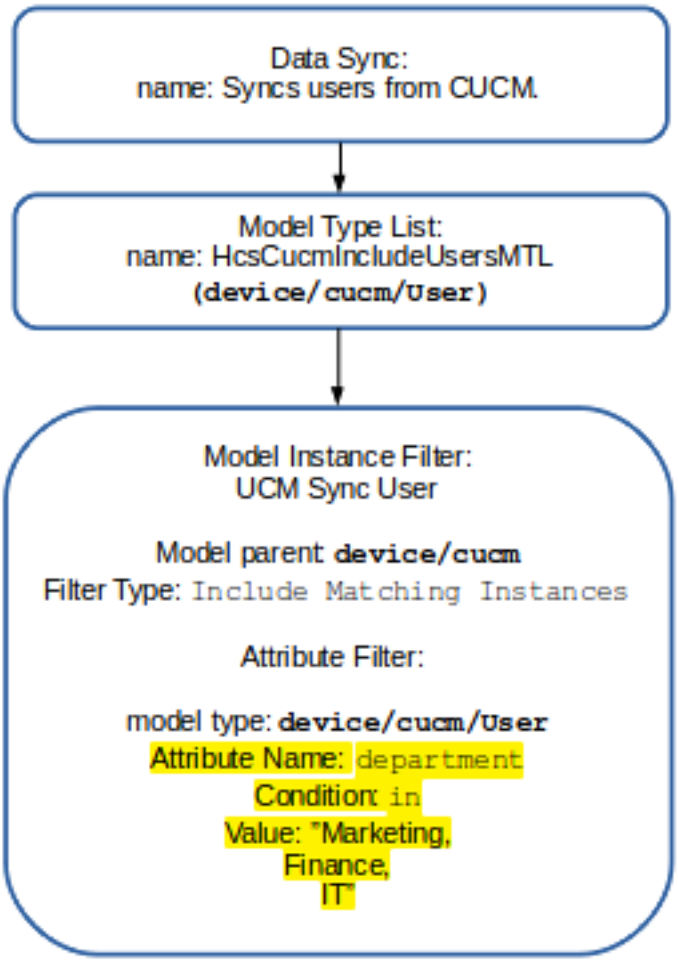
   See “View List of Device Models” below for information on how to see a list of available Unified CM and Cisco Unity Connection device models.
7. Click **Save**.

7.11. Model Instance Filter

The model instance filter (MIF) capability allows the administrator to provide criteria to define a subset of model instances to sync in. This causes the sync to only sync in those instances matching the criteria instead of all the instances.

A data sync can be set up with reference to:

- the device that is the sync target
- a set of data in the form of a model type list, that also defines the sync sequence of the models in this list
- model instance filters of the models in the list - to provide more specific filtering of specific instances of the models to sync



7.11.1. Add a Model Instance Filter

1. Log in as a Provider level administrator and choose **Administration Tools > Model Instance Filter** to display the list view of existing filters at the corresponding administrator hierarchy.
2. Choose **Add** to open the Model Instance Filter form. Provide a **Name** for the filter.
3. Choose the device or model type from the **Model Parent** drop-down. The filter will be applied to it.
4. Choose the type of filter - the inclusion or exclusion of attributes: **Include Matching Instances** or **Exclude Matching Instances**.
5. Add one or more filters in the **Model Filters** group:
   a. Choose the **Model Type** that belongs to the **Model Parent**.
   b. Add one or more attribute filters in the **Attribute Filters** group:
      - The **Attribute Name** should be selected after inspecting list request responses in the Transaction log - refer to the note below.
      - Choose its **Condition**.
      - Provide a **Value** to filter on.

   Filter criteria can be set up according to your purposes:

- Multiple **Model Type** entries are treated as an OR condition; creating a list of criteria. Any records matching any of the entries will result in a match. This is useful when defining criteria for different model types, for example, criteria for user records and different criteria for phone records. It is also useful for defining multiple criteria on the *same* model type and attribute, for example, multiple entries for `device/cucm/User` model type where the attribute of `userid` for example matches different macro-based conditions.
- Multiple **Attribute Filters** - attribute criteria for a model type are treated as a logical AND condition and entries need to match *all* the criteria in order to meet the condition. This is useful when creating criteria that match multiple different attributes of the model type, for example, match a user that has a matching `userid` as well as a matching `department`.

6. Click **Save**. The filter can be selected from the **Model Instance Filter** drop down when creating or modifying a Data Sync.

Note:

- If the filter is added at a hierarchy level *below* that of the the Data Sync, executing the Data Sync will fail, displaying a message "Model type list <ModelTypeList> not found at or above the current hierarchy.".
- In order to identify the **Attribute Name** of the model that can be used for a filter, inspect the transaction log for a list request of the model from the device.

  For example, in order to find the available Model Instance Filter attributes of `device/cucm/UserProfileProvision`, inspect the response from a list request from the device.

  From the RESPONSE snippet below, it can be determined that the attributes available for filtering are:

  – name
  – description
  – allowProvision
  – limitProvision

```
</ns0:listUserProfileProvision>
</soapenv:Body>
</soapenv:Envelope>

RESPONSE:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <ns:listUserProfileProvisionResponse xmlns:ns="http://www.cisco.com/AXL/API/11.5">
      <return>
        <userProfileProvision uuid="{96FA39CD-8A29-4B26-A3F5-0FF683326134}">
          <name>Standard (Factory Default) User Profile</name>
          <description>Standard (Factory Default) User Profile</description>
          <allowProvision>false</allowProvision>
          <limitProvision>10</limitProvision>
        </userProfileProvision>
```

7.11.2. Common Use of Model Instance Filters

While model instance filters can be used on any sync type, their common uses are:

- On add syncs - to retrieve a subset of records from the underlying device into VOSS-4-UC. For example, to limit the users pulled from LDAP, from UCM, and so on.

- On delete/purge sync - to target specific records for removal in a purge or delete sync. For example, to purge a subset of users from VOSS-4-UC that were inadvertently pulled in.

Note: Model Instance filters do not work with Cisco UCM Change Notification sync types. If a model instance filter is needed for a UCM element, this model type should be excluded from the change notification sync and a separate sync should be set up for this.

7.11.3. Macro Functions in Model Instance Filters

Macro functions can be used in the **Value** field to define matching criteria. This is particularly useful for "contains" matching, for example, using `fn.contains` or `fn.containsIgnoreCase`.

The value read in from the device API call can be referenced using the input context and the field name from the API call (for example, `input.telephoneNumber`).

For example:

- **Model Type**: `device/cucm/User`
- **Attribute Name**: `telephoneNumber`
- **Value**: `macro.ZA-number`

where `macro.ZA-number`:

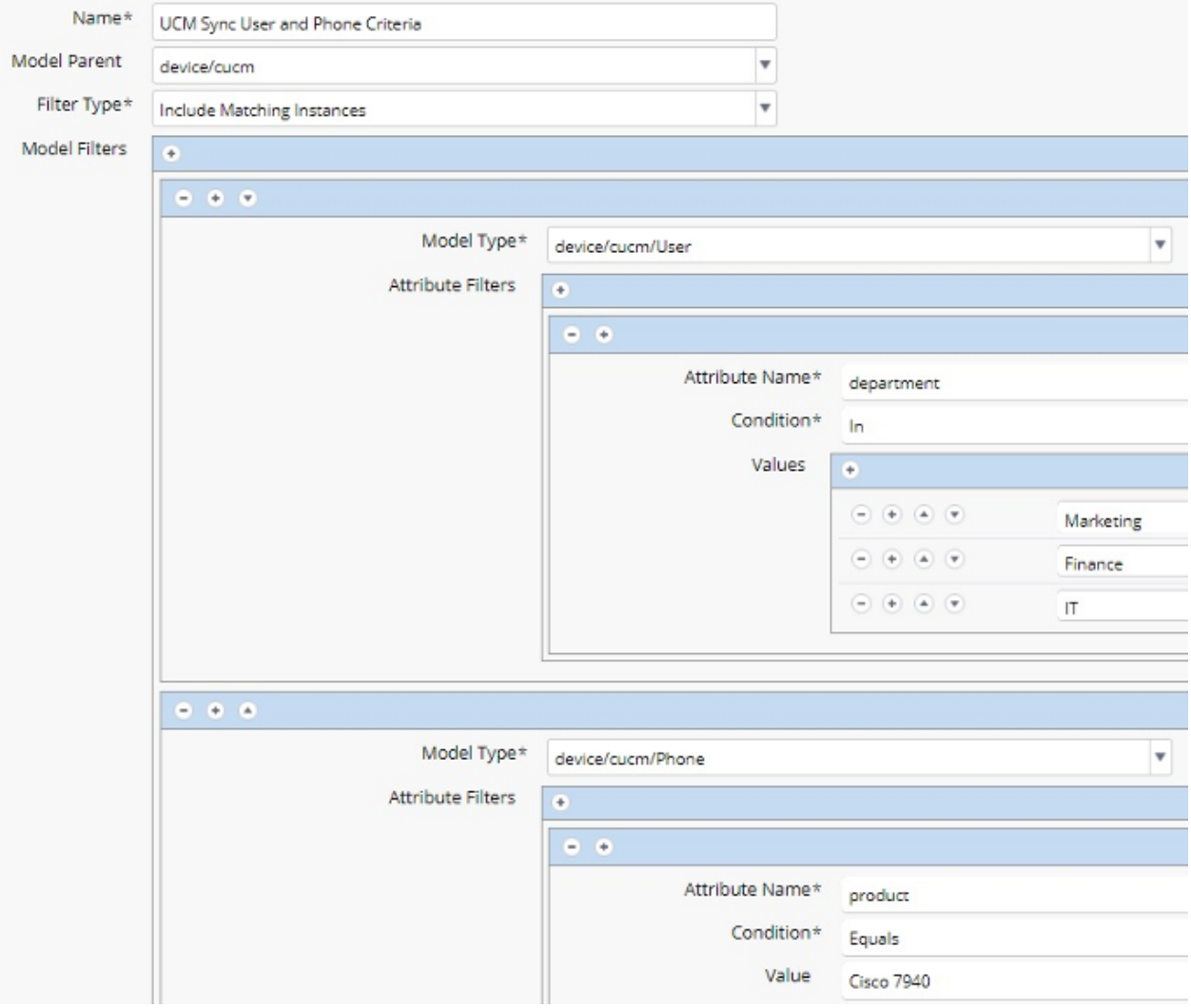
```
(( fn.containsIgnoreCase +27,input.telephoneNumber == True)) \
  <input.telephoneNumber> \
  <THIS SHOULD NOT MATCH>.
```

This condition will sync every user with a telephone number that includes `+27`. For any other user, the transaction detail log would show: "THIS SHOULD NOT MATCH".

Macros cannot be used in the **Value** field in conjunction with the "in" **Condition**.

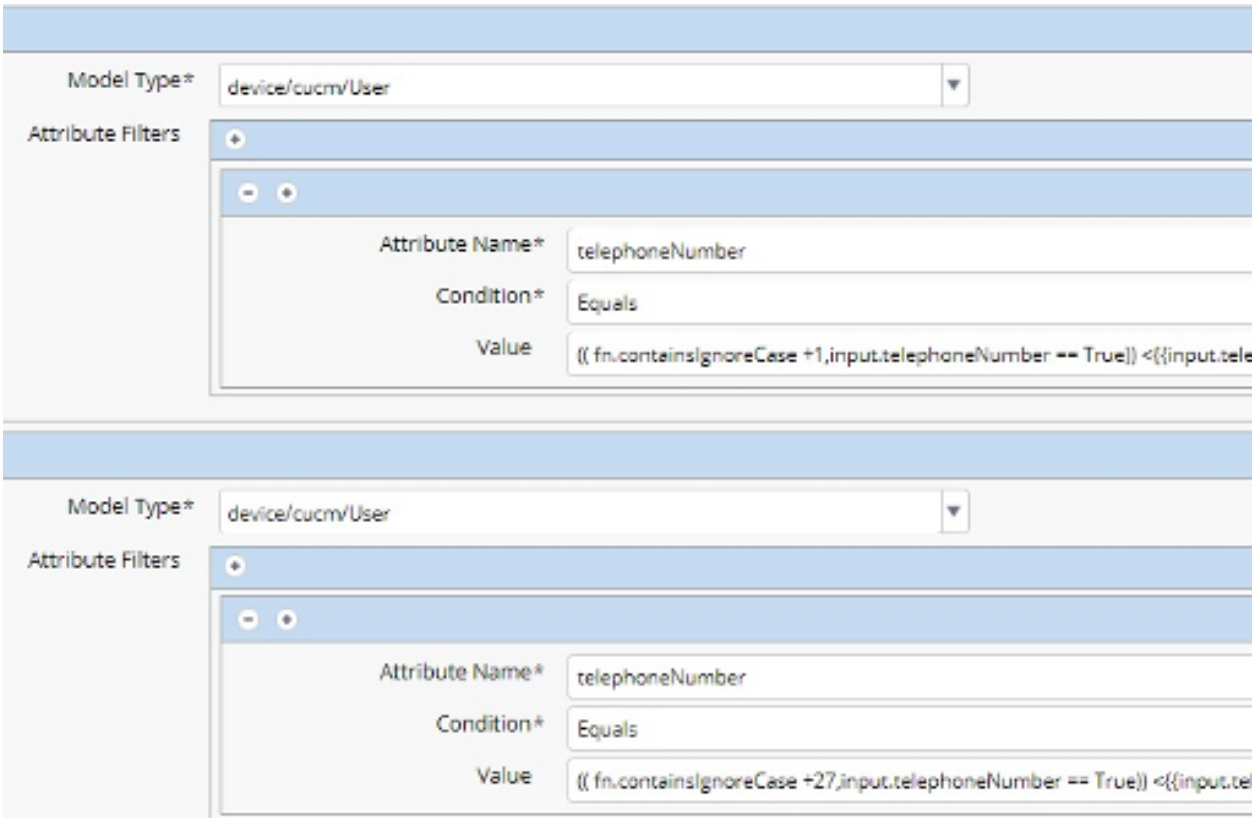
7.12. Model Instance Filter Examples

1. A MIF with multiple Model Filter entries to match criteria on different model types:



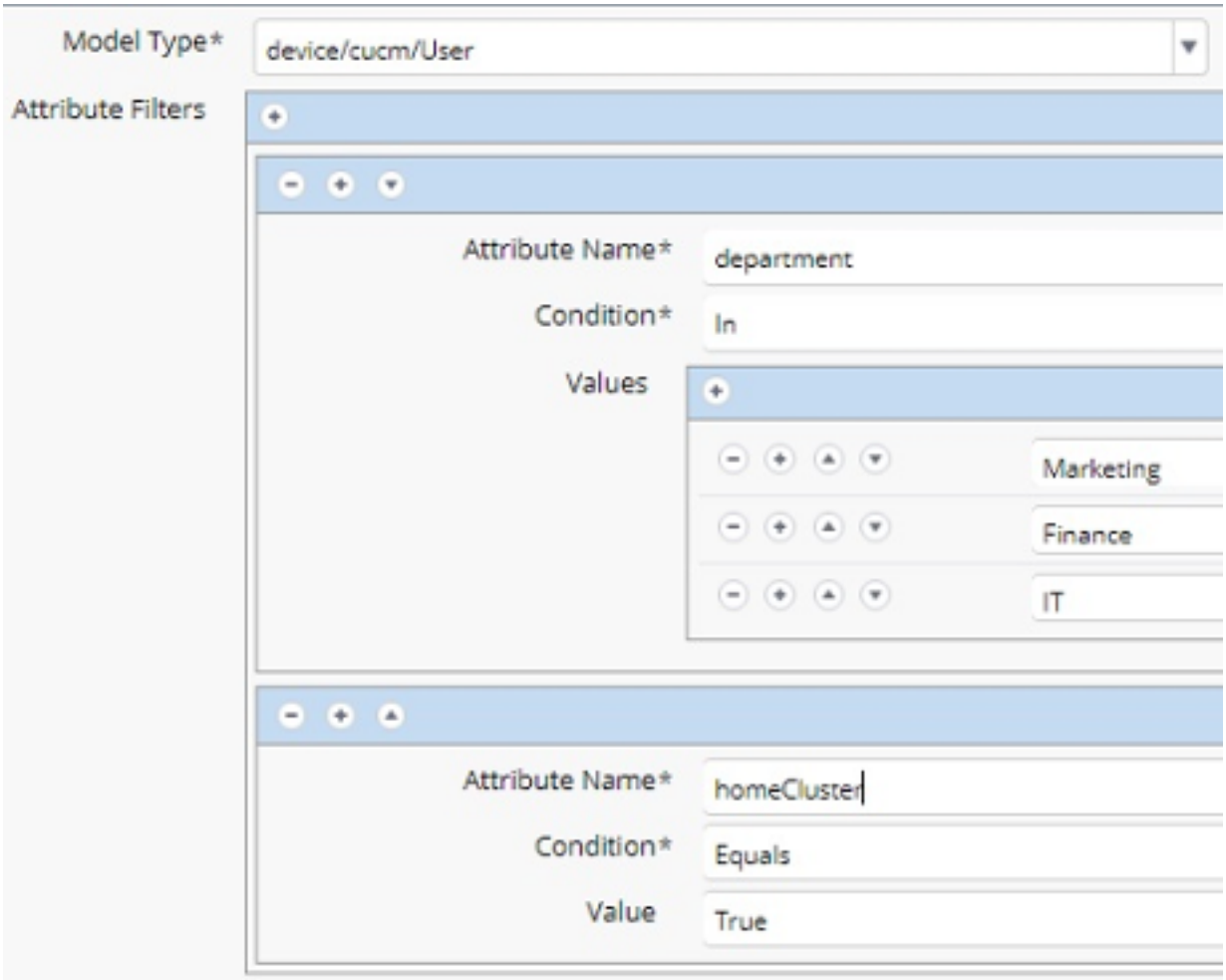
This will result in: looking at `device/cucm/User` records it will match users that have a department of Marketing, Finance, or IT (due to the IN condition). When looking at `device/cucm/Phones` it will match phones of the type “Cisco 7940”.

2. A MIF with multiple Model Filter entries with the same model type and macros to create a list of records to match



When looking at the `device/cucm/User` records it will match users that have a telephone number containing `+1` OR `+27`. The macro in the value field is cut short but it's using the macro in the notes above for reference. Due to the macros in use in the value, this had to be done as multiple model filter entries instead of a attribute filter using the IN condition.

3. A MIF with multiple attribute filters applied to the same model type



When looking at the `device/cucm/User` records it will match users that have a department matching Marketing, Finance, or IT, AND has the home cluster flag set to true.

7.13. View List of Device Models

Use this procedure to see the device models available to use in Model Type Lists for custom data syncs from Cisco Unified Communications Manager or Cisco Unity Connection.

7.13.1. Procedure

1. Log in as hcsadmin.
2. Click the ? on the menu bar to open Online Help.
3. Select Model API.
4. Select Device/Cuc or Device/Cucm. All the applicable device models are listed for the selected device.

7.13.2. What to Do Next

When including the device model in a Model Type List, use the format: device/<device_type>/<device_model>. For example, device/cucm/BillingServer.

7.14. Create a Custom Data Sync

Create a custom data sync to use a targeted Model Type List.

7.14.1. Procedure

1. Log in as hcsadmin.
2. Choose **Administration Tools > Data Sync**.
3. Click **Add**.
4. Enter the name of the Data Sync in the **Name** field.

   It is recommend to use a naming convention that makes it easy to identify the data syncs in the list view, such as C1Pull-CUCM01-DS where C1 is the customer name, Pull is the data sync type, CUCM01 is the name of the Cisco Unified Communications Manager, and DS stands for Data Sync. You could also include the type of data included in the sync, such as C1Pull-CUCM01-MediaResources-DS.
5. From the **Device Type** drop-down, choose the Device Type you are syncing from.
6. From the **Sync Type** drop-down, choose **Pull from Device**.
7. From the **Dependency Resolution** drop-down, choose **Default**.
8. Select the **Execute Asynchronously** and **Refresh Existing (Changed) Data** check boxes.

   Execute Asynchronously means that the sync request will return a reply before its complete when executed from the API. Refresh Existing (Changed) Data means that all instances of the device models specified in the Model Type List will be updated.
9. Select the **Force Refresh of Data** check box if a data update is required regardless of whether data has changed on the device. This option would for example be used if it is required that update workflows be run upon a data sync.
10. From the **Model Type List** drop-down, choose the targeted Model Type List you defined earlier.
11. Leave **Synchronization Order** and **Model Instance Filter** blank.
12. Click + next to **Device Filters** to add an entry to the list.
    a. From the **Attribute Name** drop-down, choose **host**.
    b. From the **Condition** drop-down, choose **Equals**.
    c. From the **Value** drop-down, choose the hostname/IP address of the device.

Note: Workflows can be added to, and executed by a custom data sync to perform specific data sync operations.

---

13. In the **Workflows** section, include workflows in the custom data sync if you want to perform specific data sync operations, otherwise leave the **Workflows** section empty. For example, if you want to move remote destinations from the Customer hierarchy level to the Site level, choose the **RD_Overbuild_PWF_wrapper** workflow from the **Workflow** drop-down.
14. Click **Save**.

7.14.2. What to Do Next

To run the custom data sync, click the data sync from the **Data Sync** list and click **Execute**.

7.15. Alert Field Descriptions

Field	Description
ID *	The unique ID of the alert.
Code *	The code of the alert.
Category *	The category of the alert.
Severity	The severity of the alert.
Message	The message describing the alert.
Count	The number of times this alert has occurred.
Latest Alert	The last time this alert occurred.

7.16. Change Notification Sync

7.16.1. Change Notification Feature Overview

The VOSS-4-UC interaction with the UCM Change notification sync has two primary components:

- Data Collector - collects the changes from the Cisco Unified CM and updates the VOSS cache on the configured frequency (defaults to every 300 seconds). This collector must be enabled to collect the changes, otherwise the sync will not process any changes.
- Change Notification Sync - this is a type of sync that processes the changes the collector puts into the VOSS cache. A scheduled sync should be set up and enabled so that the changes are processed within a reasonable period. The sync can also be run adhoc if required around the schedule.

The VOSS-4-UC data collector retrieves the change records from the Cisco Unified CM on the configured interval. For example, this could be every 300 seconds (5 minutes) which is the default. When a Change Notification Sync type is run, VOSS-4-UC processes the change records collected. VOSS-4-UC then processes the records accordingly:

- Add - will do a GET API call to retrieve the full record and add it to VOSS-4-UC.
- Update - will do a GET API call to retrieve the full record and update the record in VOSS-4-UC.
- Del - will remove the record from VOSS-4-UC.

The efficiency on these Update syncs is because there is no need to do a GET API call for every single record in the system - only for those that changed. In large UC application installations, this can make a big difference in Update sync times.

For example, with a data collector polling period of 300 seconds and a CNF sync scheduled for every 24 hours, the process would work as follows:

- Every 300 seconds (5 minutes) the polling collector would get all the current changes from Cisco Unified CM.
- This polling would repeat every 5 minutes - updating the VOSS-4-UC cache.
- After 24 hours, the CNF sync would run and process all the changes VOSS-4-UC stored over that 24hr period. The duration of this sync will depend on the number of changes to process, since each requires an AXL GET API request.

This type of sync, especially for updates, is far more efficient, because a GET AXL request for every object in the system is not required - only for those that changed in the time between syncs.

On a system with 10000 users for example, if 100 of the users were changed, then only 100 GET AXL request are needed. By contrast, a normal sync doing an update would require 10000 GET AXL requests to update the same 100 users.

The VOSS-4-UC data collection can store up to 200,000 changes from a single Cisco Unified CM Cluster. A warning is raised when 75% of the data collection storage capacity is reached. When the 200,000 changes capacity for a cluster is reached, a sync error occurs on the user interface (see *Errors and Troubleshooting Change Notification Processes*) To avoid the sync error, we recommend always having a scheduled CNF sync running on a regular basis based on your needs when Change Notification is enabled.

7.16.2. Setup to Enable or Disable CNF for a Cisco Unified CM Cluster

The following steps are a checklist to enable change notification for a Cisco Unified CM cluster in VOSS-4-UC.

1. Ensure the Service is enabled and configured in Cisco Unified CM. (*Cisco Unified CM Setup to use CNF*)
2. Enable Change Notification on the Cisco Unified CM cluster in VOSS-4-UC. (*VOSS-4-UC Change Notification Functionality*)
3. Review the detailed Change Notification settings for the cluster. (*VOSS-4-UC Change Notification Functionality*)
4. Review or create the required Data Sync instances for change notification for the cluster. Refer to the topics on Data Sync following *Data Sync Overview and Key Settings*.

   The number of syncs and their setup will depend on the needs for your system and the design.

   See the Best Practices Guide for guidance on sync logic and recommended setups. If further recommendations or guidance is needed, contact your VOSS account team or VOSS support.
5. Review or create required schedules for the Data sync(s) created above and activate the schedule(s). (*Enable a Scheduled Data Sync*)

   Follow the guidance for scheduling around syncs to ensure the load on the system is optimized. At least one sync schedule should be activated for the CNF setup to be complete.

Follow the steps in reverse in order to disable change notification for the cluster.

7.16.3. Detailed Cisco Unified CM CNF Functionality

The change notification capability supports all the objects that are available via AXL. In general, this means that everything VOSS-4-UC can manage in Cisco Unified CM will be available via change notification.

Data that VOSS-4-UC pulls from Cisco Unified CM that is *not* via AXL, includes:

- `device/cucm/PhoneType` - this is a combination of thinAXL so would not auto-update. This includes when you add or update phone types in Cisco Unified CM with COP files or via Cisco Unified CM upgrades. So a non-CNF sync is still required for this model.
- Phone Status and IP Address - this is pulled into the system when the phones are viewed in VOSS-4-UC (list view or individual phone). This is not via AXL so would not be updated via change notification or even a normal sync at this point.

In Cisco Unified CM, the change queue cache is stored in memory and is limited to 100,000 changes. The cache can fill quickly depending on the types of changes performed. For example, if an XSI (IP Phone) Service has been configured for 10,000 phones and the service is deleted, the cache will include one entry representing the deletion of the service plus 10,000 phone updates indicating the service was removed from each device. The polling period from the Cisco Unified CM is configurable and the timing should be considered based on how frequent configuration changes are being made in Cisco Unified CM. The default in VOSS-4-UC when polling is enabled is 300 seconds but it can be modified to be longer (up to 7200 seconds) as desired.

Cisco Unified CM Setup to use CNF

There are two settings in the Cisco Unified CM to check and update to ensure Change Notification is enabled and set up for the right queue size (accessed via service parameters: - **System > Service Parameters > Cisco Database Layer Monitor** then click the **Advanced** button):

Service Parameter Name	Setting
AXL Change Notification	This should be set to “On”
AXL Change Notification Queue Size	This has a default of 20000. For a typical system, it is suggested this is changed to the maximum of 100000 to reduce the chance of changes being missed under heavy provisioning tasks.

7.16.4. VOSS-4-UC Change Notification Functionality

This section provides more details on the functionality of the Change Notification Feature (CNF) components in VOSS-4-UC.

Change Notification Collector

The `data/DeviceChanges` model has an instance per UCM cluster and will provide the data collector status and pending changes in the cache for that cluster. An instance of the model will appear for all UCM clusters whether change notification is enabled or not. It gives you access to:

- **Base** tab
  - **Last Collection Time** - time the changes were last collected from the device

  - **Pending Change Notifications** - a view of pending changes collected for different types of models and by type of change (Add/Update/Delete). By default, this is `device/cucm/User`, `device/cucm/Line` and `device/cucm/Phone`. However, these models are adjustable on the **Settings** tab. If additional model types to the defaults above are added to the list, these are also shown. The remaining model types are all grouped in a single row called `Other`.

- **Settings** tab
  - **Polling Interval (seconds)** (300-7200 seconds with default 300) - the duration for collection of changes from the device
  - **Enable Change Collection** - enable or disable the change collector for that device.
  - **Ignored Operations** - you can select certain operations (Add/Mod/Del) to not be collected. Typically you want to collect all changes; however this option can be used to ignore some changes for specific scenarios if needed (for example, you will only handle updates via the CNF sync).
  - **Displayed Model Types** - here you can configure which models you want to see summary stats for on the **Base** tab. You can add, remove or change models to meet specific needs (for example, `deviceProfile` for extension mobility profiles, `remoteDestination` for SNR remote destinations, and so on).

The `data/DeviceChanges` model should be included in menu layouts for roles that need access to this level of detail for the CNF syncs.

Change Notification Sync Type

When a Change Notification Sync type is used in a data sync, there are a number of differences in the sync behavior in comparison with a normal pull sync:

- A GUI portal rule on the Data Sync interface will change some of the settings visible on the Data Sync GUI interface when the **Sync Type** is set to Change Notification Sync. This selection hides settings that are not relevant and exposes new settings for this type only.
- **Number of Changes to Process** - This input field becomes available from the Data Sync interface. Leaving the input box blank or typing in 0 will mean the sync will process all the pending changes collected - subject to the selected model type list and Disabled Operations set up on the sync. If you enter a number, the sync will process that number of changes only and leave any additional changes in the change collection for the next sync.

  Typically this value should be 0 or blank, unless there is a specific reason to limit the number of changes to process, for example when managing how long the sync may run.

All other visible settings are the same as with a normal pull sync, for example, device filters, workflows, and so on.

When a sync runs (either a normal pull sync or a change notification sync), it will clear out the change notification collection of any model types and changes processed for that cluster.

The model type lists and disabled operations define which models and types of actions are processed in either a pull or a change notification sync:

- The model type list (if one is assigned) assigned to the sync will determine which model type changes will be processed from the collected changes (for example, `device/cucm/User` for user entities only).
- The **Disabled Operations** tab defines if any of the types of changes are ignored. For example, selecting **Remove** will ignore delete changes.

Pull Sync and Change Notification Sync details:

- A pull sync does not utilize the change notification collection as a source of data. However, it will clear the collection for the models types it processes.
  - A *full* pull sync (a pull sync without a model type list) will clear the change collection as part of the sync process since it is pulling *all* the latest information from the UCM.
  - A pull sync with a model type list defined (for example one that contains `device/cucm/User`) will clear the change collection of any `device/cucm/User` changes, since it is syncing all the user information anyway. All other model types and changes will be left in the collection.
  - If a pull sync is run with **Disabled Operations** selected (for example, **Add** is selected) this will process the pending changes for Update and Delete actions for any matching models. However, *all* actions for the matching model will be cleared from the cache, *including Add actions*.
- A Change Notification Sync utilizes the change collection as its source of information and will clear that changes from the change collection for any model types it is processing.
  - A *full* Change notification sync (CNF sync without a model type list) will process *all* the pending changes and clear the change collection (unless limited by a value in the **Number of Changes to Process** setting on the sync. Then only that number of changes will be processed and cleared).
  - A change notification sync with a model type list defined (for example contains `device/cucm/User`) will process all the pending changes for the `device/cucm/User` model type and clear those from the change collection.
  - If a change notification sync is run with **Disabled Operations** (for example, **Add** is selected), it will process the Update and Delete changes for the matching models. However, *all* actions for the matching model(s) will be cleared from the cache, *including Add actions*.

This sync behavior means that you may wish to set up multiple syncs for a cluster to handle different types of sync and sync schedules to meet your needs. Ensure that you generally have all the model types covered in your scheduled syncs if CNF is enabled, otherwise some changes may never be cleared from the change collection, thereby taking up space.

For additional considerations and information around sync setup best practices, see the Best Practices Guide.

VOSS-4-UC Setup to enable Change Notification

Enabling the Change Notification capability is completed on a per UCM Cluster basis. This can be done on the UCM Server configuration page for a publisher via the publisher tab and selecting the **Enable Change Notification Sync** checkbox. When selected and saved, the system will:

- Enable the data collector for that cluster
- Create a CNF sync type for the cluster
- Create a schedule for the CNF sync. The schedule will be disabled by default.
- These settings should all be reviewed, adjusted, or additional instances created to meet your needs. See further information in:
  - The Best Practices Guide
  - The System Monitoring Configuration section in the Advanced Configuration Guide on sync best practices for different scenarios and other considerations.
- A full sync with the UCM Cluster should be executed just before or after enabling Change Notification for the cluster. This can be part of changing the setting for an existing cluster or adding a new publisher. Currently, both actions will invoke a full sync of the cluster. However, if the sync is not completed during the add/modify of the publisher, then one should be initiated.

When CNF is disabled on the Publisher configuration page (or if the cluster is removed from the system), the following will occur:

- The auto-generated schedule that was added during enabling will be removed. Any additional custom scheduled added will not be removed automatically and should be removed before disabling the change notification for the cluster to avoid unnecessary syncs running.
- The auto-generated CNF sync type that was added during enabling will be removed. Any additional custom CNF sync types for the cluster added will not be removed automatically and should be removed before disabling the change notification for the cluster to avoid unnecessary syncs being set up.
- The data collector for the cluster will be disabled.

Note: If the collector is only disabled via the `data/DeviceChanges` model, then the schedules and sync will remain. This is the best approach if you need to temporarily disable the CNF sync (for example, for a maintenance window).

7.16.5. Errors and Troubleshooting Change Notification Processes

A number of scenarios may result in error conditions in the change notification process. The VOSS-4-UC system is enabled to display alerts automatically in this case, so that it is not necessary to configure the change notification feature (CNF) alerts manually.

Administrators can view the alerts at the hierarchy level they log in at and all the levels below that hierarchy. For example, if an alert is raised at the customer level (sys.hcs.provider.reseller.c1), then the provider, reseller, and customer administrators can see that alert, but not the site administrators. All the administrators have read and delete permissions to the alerts.

When a change notification feature alert is raised, the Notifications indicator on the VOSS-4-UC Admin GUI shows the alert. Clicking the Notifications button shows a pop-up and a message that alerts have been raised. By clicking on the message, users are directed to the list of alert messages which can also be accessed via the menu under **Administration Tools > Alerts**.

CNF alerts have the following distinct properties:

- ID: A generated identifier of the target device of the collector For Unified CM, the ID shows the host name, port, and hierarchy.
- Code: An error or warning code associated with the alert.
- Alert category: The category of the alert - Device Change Notification Collector
- Severity: VOSS-4-UC displays severity codes and messages as follows (“{}” indicate device or number placeholders in the messages). Each alert has some properties, for example, severity (Error, Warning or Info), the number of times that the same alert has been raised, and the time stamp of the last alert instance.
- Message: Displays error message description and the statement to fix the error.
- Count: Displays the number of times the alert has occurred for a specific device.
- Latest Alert: Displays the last time this alert occurred.

Note: Administrators can also filter alerts by any of the alert fields.

VOSS-4-UC displays change notification feature alerts for the following error scenarios:

- Warning:
  - 45000: Unprocessed changes at 75% of limit for device {}. Please configure and run the necessary data syncs.
- Error:
  - 40000: Device change notifications are not supported for device {}.
  - 40001: Device change notification data for device {} has been lost. Tracking data has been repaired and collector process will continue. Some changes may have been lost, please run a full sync on the device.
  - 40002: Device change notification tracking data for device {} has become corrupted. Tracking data has been repaired and collector process will continue. Some changes may have been lost, please run a full sync on the device.
  - 40003: Device change notification tracking DB write for device {} failed. The collector process will continue to attempt DB writes. Please investigate the database write failure.
  - 40004: Device change notification data DB write for device {} failed. The collector process will continue to attempt DB writes. Please investigate the database write failure.
  - 40005: Unable to repair device change notification tracking data for device {}.
  - 40006: Too many unprocessed changes recorded for device {}. No new changes will be recorded until at least {} changes are processed. Please configure and run the necessary data syncs.
  - 40008: Could not update pending changes data for device {}. {}.

The administrator reads, inspects, acts on (for example, run a full sync on the device), and then manages alerts of the Change Notification collection service. The administrator can delete the alert from the list only when the issue that raised the alert has been resolved.

Note: If the Administrators forget to remove the change notification feature alert after resolving it, the alert will still be shown when they log in to VOSS-4-UC. We strongly recommend removing the alert after resolving it.

Change Cache Full on Cisco Unified CM

If the Cisco Unified CM maximum number of stored change records is exceeded (see detailed Cisco Unified CM functionality section for more details on the limit and configuration) then the Cisco Unified CM will drop the oldest changes that have not been collected. This can happen if the polling time in VOSS-4-UC is set up to be too long or the Cisco Unified CM is experiencing a very high level of changes (see the detailed VOSS-4-UC functionality section for more details on polling configuration). When this situation occurs, VOSS-4-UC will get an error on polling and will try to recover. This activity is logged as an Alert in the system and provides the outcome - recovery was successful (alert code 40001 or 40002) or recovery was not successful (alert code 40005).

In the event the recovery was successful, you may want to review and consider a full sync as some changes would have been lost (the oldest changes in the Cisco Unified CM cache).

In the event the recovery was not successful, then a full sync is required to update and to get change notification functioning again. The full sync is needed as changes would have been missed from the Cisco Unified CM and we need to be at a clean sync in order to start processes changes again.

In this situation, application info log messages are logged as well - “Repaired change notification tracking data for device {}” or “Unable to repair change notification tracking data for device {}”

VOSS-4-UC Change Collection full for a Cisco Unified CM cluster

If the VOSS-4-UC change collection for a given Cisco Unified CM cluster exceeds the maximum changes - 200,000 - then an alert with code 40006 is raised. This alert means that no further changes are collected from the Cisco Unified CM until some of the pending changes are processed. This can be carried out by an administrator executing a sync for that Cisco Unified CM cluster to clear some of the changes. If the next scheduled sync is not too far ahead in time, then waiting for the next scheduled sync to run may be acceptable.

Other errors

The other error codes listed for the alerts are more internal in nature and should result in a VOSS support ticket being raised for further investigation.

8 Customer Configuration

8.1. CUCM Group Selection

Provider level administrators can manage the Default CUCM Group setting in a customer's Site Defaults:

- The least utilized Group can be calculated, in other words the group with the least number of phones can automatically be determined.

  In this case, the administrator can set the Default CUCM Group in the customer's Site Defaults to automatically be the least utilized group so that CUCM Groups are optimally assigned whenever a site is created.

- The current device utilization of customer CUCM Groups can be inspected. Device utilization is calculated by inspection of the Device Pools that belong to a CUCM Group of a CUCM cluster and the number of Phones in these Device Pools.

  The administrator can therefore inspect the CUCM Group counts and then choose a Default CUCM Group to be the Default CUCM Group in the customer's Site Defaults.

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

8.2. Select a CUCM Group

1. Log in as a Provider administrator and select **Customer Management > Advanced > CUCM Group Selection**.
2. The list of existing CUCM Group Selection configurations at the Provider hierarchy are listed.

   Click **Add** to create a configuration. A hierarchy pop-up will show to choose the customer hierarchy at which the configuration should apply.
3. Choose a Name for the configuration. The default name is the hierarchy name.
4. Choose an Algorithm to apply to the CUCM Group Selection:
   - If Use Default is selected, the Site Defaults doc is updated if necessary so that the Default CUCM Group is applied.

     Note: The CUCM Group called Default is always used when adding a Site unless the "Least utilized" algorithm has been selected. Default will also be the fallback CUCM Group in the event that all CUCM Groups have been excluded from the selection.
   - If Least utilized CUCM Group is selected from the Algorithm drop-down, options are available to include and exclude specific CUCM groups from the algorithm.

- If no groups are included or excluded, *all* groups available at the customer hierarchy are considered by the algorithm.
- If groups are added to the CUCM Groups to Include, only these groups are considered by the algorithm.
- If groups are added to the CUCM Groups to Exclude, these groups are not considered by the algorithm, *unless* they have also been added to the Groups to Include.

The table below summarizes the options and outcomes:

Group Selection	Algorithm	Include List	Exclude List	Result	Comment
No	Use Default	N/A	N/A	Default	Falls back to Default always
Yes	Use Default	None	None	Default	•
Yes	Least utilized	None	None	Least utilized	•
Yes	Least utilized	Yes	None	Least utilized	From the groups in the included list.
Yes	Least utilized	None	Yes	Least utilized	Least utilized from all groups except in the exclude list.
Yes	Least utilized	Yes	Yes	Least utilized	From the groups in the included list. Note that the exclude list will be ignored in this case.

5. Click **Save** to save the configuration for the customer hierarchy. When a new site is created, the Default CUCM Group in the Site Defaults Doc is updated to reflect the configuration, so that any sites that are now created under this customer hierarchy will apply the calculated CUCM Group.

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

8.3. CUCM Group Counts

1. Log in as a Provider administrator and choose **Customer Management > Advanced > CUCM Group Counts**.
2. From the **CUCM** drop-down, choose a CUCM instance to show the CUCM Group counts for.
3. The **CUCM Group counts** field shows all CUCM groups and the count of devices in the format: *<group_name>*[*<count>*].

   If a CUCM Group has no device pool, in other words it has no devices, the group shows as *<group_name>[0 no device pools]*.

The administrator can use the CUCM Group Count data to inspect CUCM Group utilization at a customer, or to choose a Default CUCM Group that will be assigned to a customer's Site Defaults Doc.

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

8.4. Extension Mobility Cross Cluster (EMCC) Configuration

Extension Mobility Cross Cluster (EMCC) extends VOSS-4-UC's current extension mobility functionality to allow the user to log in to a device, from within a connected cluster, anywhere in the world. This enables the user to retain the settings, services and lines he/she is familiar with at their home location.

VOSS-4-UC automates most of the EMCC provisioning to enable this feature to work on all dial plans across multiple Cisco Unified Communications Manager (Unified CM) clusters that are managed by the same platform instance. A small number of manual configurations remain, specifically around network security, which is outlined in a separate section. VOSS-4-UC only automates provisioning of the home cluster in cases where the Unified CM clusters are managed by separate platforms, that is, cross-cluster configuration across multiple platforms is not supported.

8.4.1. EMCC Use Case

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

- A user from the HOME cluster goes to the VISITING cluster and logs onto a phone. The two clusters can be in different countries/territories.
- The user cannot be authenticated in the VISITING cluster, but since the cluster is EMCC enabled, and the phone is subscribed to the EMCC service, the cluster searches for the user in defined EMCC remote clusters.
- Once the user (also subscribed to the EMCC service) is authenticated, the phone is unregistered from the VISITING cluster, and re-registered to the HOME cluster.
- The geolocation of the phone is sent to the HOME cluster. This enables the HOME cluster to associate the relevant roaming device pool to the user's phone using the geolocation filter.
- The phone behaves and dials exactly the same as if the user was logged in at the HOME cluster, and all his/her settings and preferences are preserved.
- Calls to the HOME cluster emergency numbers as well as the VISITING cluster emergency numbers break out at the VISITING cluster (physical location).
- Various other elements such as trunks, EMCC countries, and so on, must be configured on both the HOME-and VISITING clusters to ensure the feature functions.

Note: Refer to the "Cisco Unified Communications Manager Features and Services Guide" for more information about the EMCC feature.

8.4.2. Prerequisites for Configuring EMCC using VOSS-4-UC

Before you can configure Extension Mobility Cross Cluster (EMCC) using VOSS-4-UC, make sure that the following parameters have already been configured on each required EMCC cluster (Unified CM) located at the relevant Customers:

- EMCC Feature Configuration such as Default TFTP Server for EMCC Login Device, EMCC Geolocation Filter

8.5. EMCC Group Management

An Extension Mobility Cross Cluster (EMCC) group is a collection of clusters and countries that essentially forms an 'EMCC Cloud', which determines the specific clusters between which a user can roam.

Note: A cluster can only be included in one group.

EMCC groups typically cater for situations where all the clusters are in different countries, and are managed by the same platform instance. To support multiple clusters in the same country, you need to refine the geolocations and geolocation filters to uniquely identify the clusters in the default provisioning of country. This is supported by using the home cluster setup for each of the clusters in the group.

The EMCC Group screen allows a provider administrator to add or remove clusters and countries to or from an EMCC group, or to modify/delete an existing EMCC Group.

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

See also:

- *Add an EMCC Group*
- *Modify an EMCC Group*

8.6. Add an EMCC Group

When adding an EMCC Group, the cluster the user is on when taking this action is automatically selected/included in the new group.

8.6.1. Before You Begin

Make sure the required route patterns have been created (see *Add EMCC Route Pattern*).

8.6.2. Procedure

1. Log in as provider administrator or higher.

2. Choose **Customer Management > EMCC > EMCC Group**.
3. Click **Add**.
4. Choose the required customer from the **Hierarchy** drop-down list. The **EMCC Group** screen is displayed.
5. Enter the mandatory EMCC Group Name in the **Name** field.
6. Choose the required CUCM Clusters and Countries to include in the EMCC Group by selecting single or multiple entries in the **Available** areas of the screen, and then clicking **Select** to move them to the **Selected** area of the screen. Use the Remove, Move Up and Move Down buttons as required to assist in creating the EMCC Group. An EMCC Group **must contain** a minimum of two clusters.
7. Make sure that the required CUCM Clusters and Countries are listed in the CUCM Clusters and Countries areas of the screen respectively.
8. Click **Save** to add the EMCC group to VOSS-4-UC.

   Upon creation of the EMCC Group, the following elements are provisioned per country and EMCC route pattern:

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

8.7. Modify an EMCC Group

1. Log in as provider administrator or higher.
2. Choose **Customer Management > EMCC > EMCC Group**.
3. Click on the EMCC Group that you want to modify. The selected **EMCC Group** screen is displayed.
4. Add or remove the CUCM Clusters and Countries within the EMCC Group by selecting single or multiple entries in the **Available** or **Selected** areas of the screen, and then clicking **Select** or **Remove** to include or exclude them from the group as required. Use the Move Up and Move Down buttons as required to assist in creating the EMCC Group.
5. Click **Save** to save the modified EMCC group to the VOSS-4-UC database.

8.8. EMCC Route Patterns

See:

8.9. Add EMCC Route Pattern

1. Log in as provider administrator or higher.
2. Make sure that the hierarchy path is set to the correct customer node.
3. Choose **Customer Management > EMCC > EMCC Route Patterns**.
4. Click **Add** to add an EMCC Route Pattern. The **EMCC Route Patterns** screen is displayed.
5. Enter the following fields as required:
   a. **Country**. Choose the relevant ISO country code from the drop-down list.
   b. **Pattern**. Enter the route pattern, including numbers and wild cards. Do **not** use spaces in your route pattern.
   c. **Called Party Transformation Mask**. Enter a transformation mask value. Valid entries include digits 0 to 9, the wild card character X. Note that if this field is left blank, no calling party transformation takes place.
6. Click **Save** when complete to add the EMCC Route Pattern.

8.10. Modify EMCC Route Pattern

1. Log in as provider administrator or higher.
2. Make sure that the hierarchy path is set to the correct customer node.
3. Choose **Customer Management > EMCC > EMCC Route Patterns**.
4. Click the EMCC Route Pattern that you want to modify.
5. Update the following fields as required:
   a. **Country**. Choose the relevant ISO country code from the drop-down list.
   b. **Pattern**. Enter the route pattern, including numbers and wild cards. Do **not** use spaces in your route pattern.
   c. **Called Party Transformation Mask**. Enter a transformation mask value. Valid entries include digits 0 to 9, the wild card character X. Note that if this field is left blank, no calling party transformation takes place.
6. Click **Save** when complete to save the changes to the EMCC Route Pattern.

Note: To delete an EMCC Route Pattern, click on the pattern to delete on the **EMCC Route Patterns** list view, and then click **Delete** on the button bar.

8.11. EMCC Templates

Use EMCC templates to define the common EMCC attributes to add a group of new EMCC. Prior to creating the template, make sure EMCC settings have already been configured in Cisco Unified Communications Manager Administration.

See also:

- *Configuration Templates*

8.12. Clone and Add EMCC Template

1. Log in as provider administrator or higher.
2. Make sure that the hierarchy path is set to the correct customer or location node.
3. Choose **Customer Management > EMCC Templates**.
4. Click on the EMCC Template from which you want to create a new EMCC Template.
5. Click **Action > Clone**. The selected EMCC Template is cloned. See also *Workflow for Creating Configuration Templates* for more information.
6. Enter a new **Name** for the EMCC Template. This is mandatory field.
7. Edit existing fileds, and add new fields as required. See also *Configuration Template Field Reference*.
8. Click **Save** to add the EMCC Template.

8.13. Modify EMCC Template

1. Log in as provider administrator or higher.
2. Make sure that the hierarchy path is set to the correct customer or location node.
3. Choose **Customer Management > EMCC Templates**.
4. Click on the EMCC Template that you want to edit. See also *Workflow for Creating Configuration Templates* for more information.
5. Edit and add the required fields, making sure that all mandatory fields are complete. See also *Configuration Template Field Reference*.
6. Click **Save** to save the modified EMCC Template.

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

---

9 Site Management

9.1. Modify Site Defaults

Site defaults provide the default values for many tasks undertaken while onboarding, and are not limited to the Subscriber Management tasks. When a site is created, a site defaults instance is created on that site with the same name as the site. Many of the attributes in this data model contain default values when this instance is created.[1]

The Site Defaults Doc is particularly useful when managing multi-site, multi-country customers. It allows a Provider Administrator or higher to set geo-specific information at a site level to allow multi-national sites to stay in sync. Geo-specific information includes CUCM user-locale and network-locale defaults as well as the CUC timezone and language defaults.

1. Log in as provider, reseller, or customer administrator.
2. Choose **Site Management > Defaults**.
3. Click the site that you want to modify defaults for.
4. From the **General Defaults** tab, click the following fields to modify their default values as required:

[1] For Provider deployments, when a Cisco HCS site dial plan is created, the site defaults on that site are updated. The updated defaults are dial plan-related attributes that are affected by the site dial plan that was deployed. If these specific site defaults attributes already had values before the site dial plan was deployed, they are overwritten. When the site dial plan is removed, these same attributes are reset (set to empty string) in the site defaults.

Option	Default Value
Name	Site name This field is mandatory. It should be the same name as the site. Only one instance of site defaults exists for a site.
Default CUCM Device Pool	Cu{CustomerId}Si{SiteId}-DevicePool
Default CUCM Location	Cu{CustomerId}Si{SiteId}-Location
Default CUCM Region	Cu{CustomerId}Si{SiteId}-Region
Default CUCM Date/Time Group	CMLocal[2]
Default User Locale	The user locale identifies a set of detailed information to support users at the specific location, including language and font. Choose the required user locale from the drop-down list, which contains all user locales available on the CUCM at the selected location.
Default Network Locale	The network locale contains a definition of the tones and cadences that the phones and gateways use at the specific location. Choose the required network locale from the drop-down list, which contains all network locales available on the CUCM at the selected location.
Default User Profile (for User Self Provisioning)	Choose from the drop-down list.
Default CUCM Hunt Pilot Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM Call Pickup Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM Call Park Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM MeetMe Partition	Cu{CustomerId}Si{SiteId}-Feature-PT
Default CUCM Group	Default value: Default

5. From the **Device Defaults** tab, click the following fields to modify their default values as required. These default values are applied to the configuration template associated with adding a subscriber (SubcriberPhonePrePopulate).

[2] For Provider deployments, choose from the drop-down list.

Option	Default Value
Default CUCM Phone Product	Cisco 9971
Default CUCM Phone Protocol	SIP
Default CUCM Phone Button Template	Standard 9971 SIP
Default CUCM Phone Security Profile	Cisco 9971 - Standard SIP Non-Secure Profile
Default CUCM Phone Softkey Template	Standard User
Default CUCM Phone SIP Profile	Standard SIP Profile
Default CUCM Phone Presence Group	Standard Presence Group
Default CUCM Phone Common Profile	Standard Common Phone Profile
Default CUCM Phone Line E164 Mask	Enter a E164 mask value that will be applied as a default when devices have not been configured with static values.
Default CUCM Device CSS	Cu{CustomerId}Si{SiteId}-{countryIsoCode}- DP-Emer-CSS
Default CUCM User Subscribe CSS	Internal-CSS
Default CUCM Phone Subscribe CSS	Cu{CustomerId}Si{SiteId}-InternalOnly-CSS
Default CUCM Device Profile Product	Cisco 9971
Default CUCM Device Profile Protocol	SIP
Default CUCM Device Profile Button Template	Standard 9971 SIP

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

6. From the **Line Defaults** tab, click the following fields to modify their default values as required. These default values are applied to the configuration template associated with adding a line (line-cft).

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

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

7. From the **User Defaults** tab, click the following fields to modify their default values as required:

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

8. From the **CUC Defaults** tab, click the following fields to modify their default values as required:

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

See *Cisco Unity Connection Localization* for more details if required.

9. From the **HotDial Defaults** tab, click the following fields to modify their default values as required:

Option	Default Value
Default PLAR CSS	None
Default HotDial TimeZone	None

10. For information on the **Overbuild Defaults** tab (visible to provider and reseller administrators), see *Overbuild Site Defaults: Overview*.
11. Click **Save** to save the modified site defaults.

9.2. 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)	
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	

Continued on next page

Table 1 -- continued from previous page

Tasks	HCS Admin	Provider / Reseller Admin	Customer Admin	Site Admin
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.

9.3. Shared Lines

9.3.1. 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.

9.3.2. 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 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.

9.3.3. 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:

     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

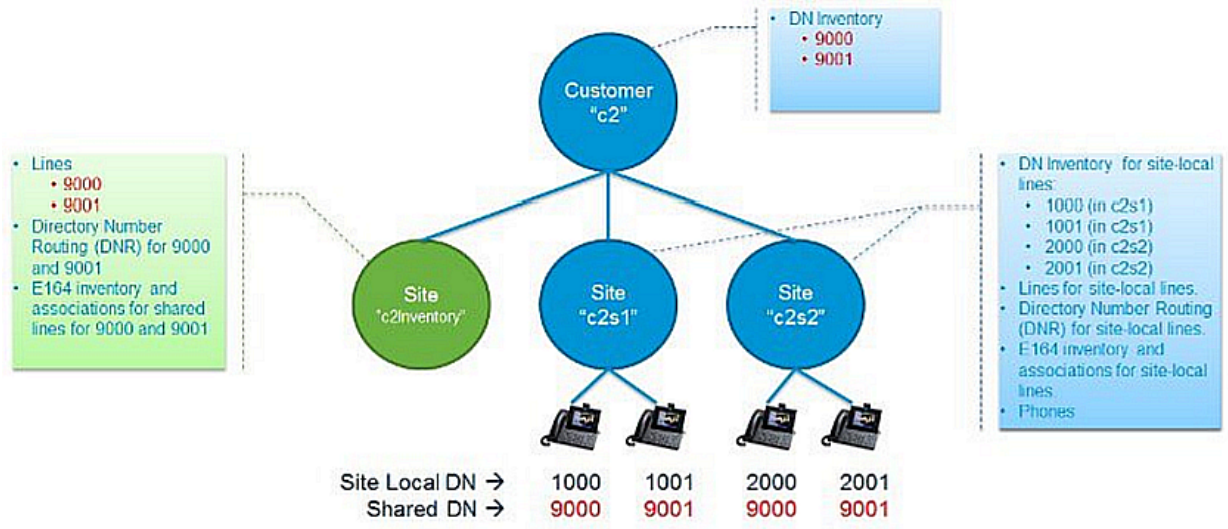
   - **DN inventory** - for lines to be used only at this site. Note that these DNs can be shared by multiple phones within the site.
   - **Subscribers** - configured from **Subscriber Management > Subscribers**, or **Subscriber Management > Quick Add Subscriber**.

- **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.

9.3.4. 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 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.



9.3.5. 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.

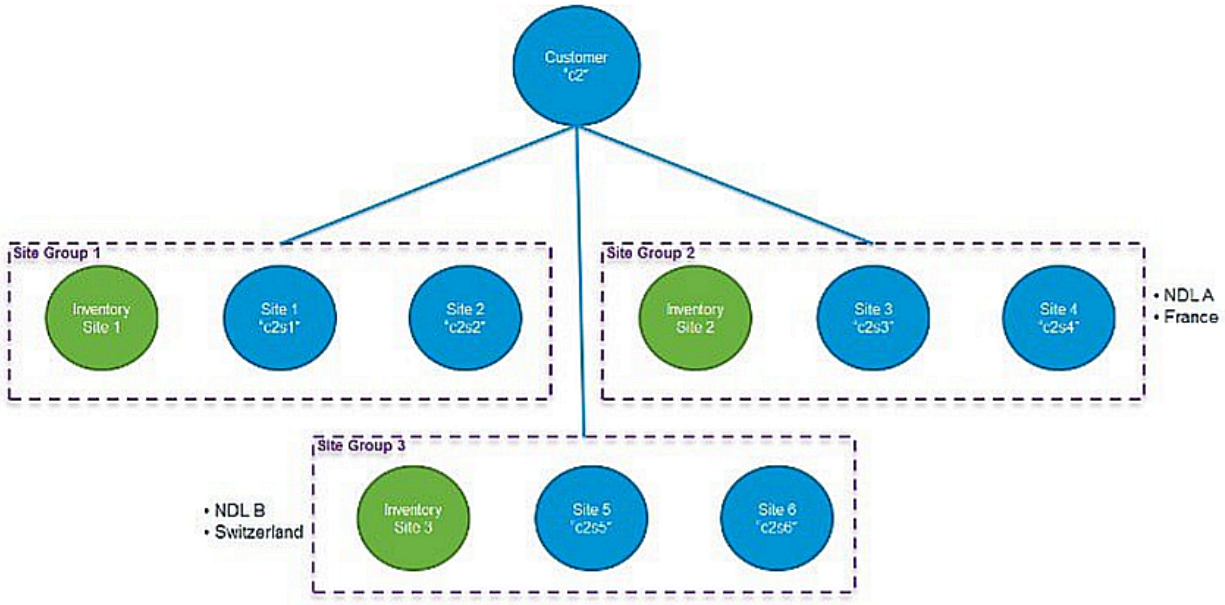
All sites in a site group must conform to the following rules:

- 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 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.

9.3.6. Inventory Site Diagram

The following diagram shows a customer with three Site Groups.



9.3.7. 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.

9.3.8. 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.

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 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**

9.3.9. 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.

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.

9.3.10. 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.

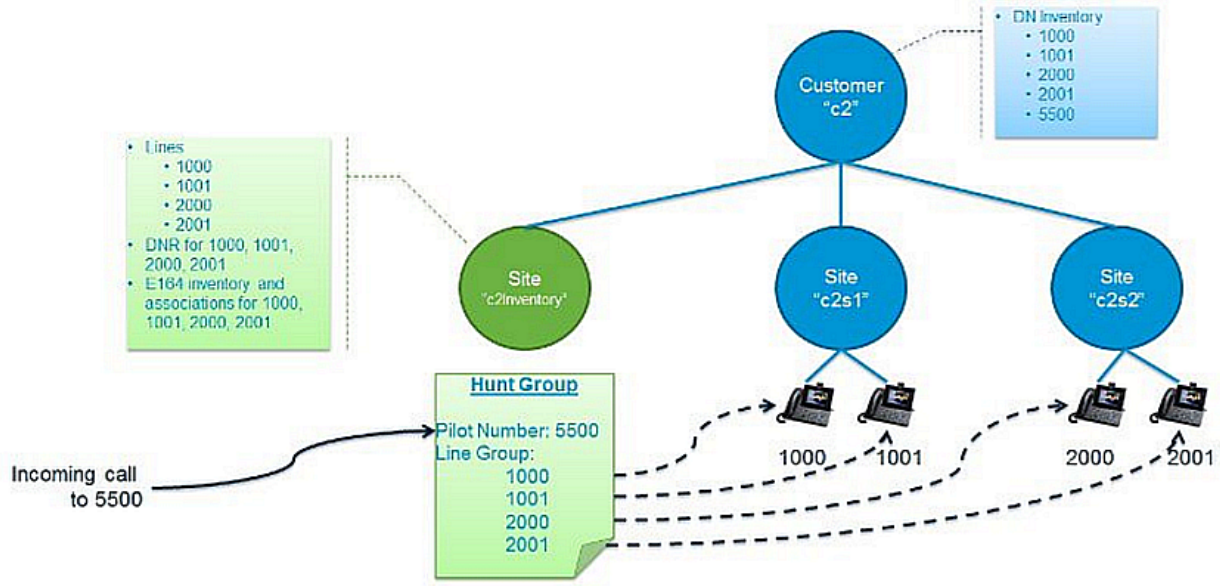
9.3.11. Hunt Groups and Call Pickup Groups for Shared Line Across Sites

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.

9.3.12. 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.



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).

9.3.13. 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.

9.3.14. 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.

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

9.3.15. 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.

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.

9.3.16. 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.

- 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.

10 Set Up Northbound Notification

10.1. Northbound Notification

The VOSS-4-UC Northbound Notification (NBN) provides a mechanism to notify an Operations Support System (OSS) or Business Support System (BSS) when user data in VOSS-4-UC is created, updated, or deleted. The Northbound Notifications can be customized to specify which events trigger notification and the destination of notifications.

The supported model types are:

data/NormalizedUser Essential user information. Changes occur either from LDAP sync or manually in VOSS-4-UC.

relation/Subscriber Subscriber information, such as assigned devices and services. Only changes made in VOSS-4-UC via Subscriber Management generate notifications. Changes to subscribers made in VOSS-4-UC do not generate notifications.

All NBN events are post-execution so the notification is sent immediately after the data is changed in VOSS-4-UC.

Note: Failing changes to user data result in a pair of notifications, one for the attempted change and an opposite one for the rollback of the change. For example, a failing user add generates a create notification and a delete notification.

To suspend notifications for a given model type and operation, mark the event as 'inactive' and notifications will neither be sent nor stored while the event is inactive. Once the event is marked as 'active', subsequent notifications will be sent.

10.2. Notification Format

The Northbound Notifications are sent to a destination as HTTP or HTTPS POST requests. The message body is a JSON map that contains the notification data. The JSON map is in this format:

Key	Datatype	Operation
model_type	String	All
operation	String	All
pkid	String	All
hierarchy	String	All
new_data	Map	Create/Update
previous_data	Map	Update/Delete

The keys in the new_data and old_data maps are the attribute names for the given model type.

10.2.1. Example

See this example of a notification's message body triggered by updating a user:

```
{
   'model_type': 'data/NormalizedUser',
   'operation': 'update',
   'pkid': '5445310900698a11d83164e3',
   'hierarchy': '543c57ea00698a11d8305815',
   'new_data': {
      'username': 'jdoe',
      'mail': ['jdoe@provider.com'],
      'givenName': ['Jane'],
      'sn': ['Doe'],
      'l': ['RTP']
   },
   'previous_data': {
      'username': 'jdoe',
      'mail': ['jdoe@provider.com'],
      'givenName': ['Jane'],
      'sn': ['Doe'],
      'l': ['New York']
   }
}
```

10.3. NBN Transaction Processing

Once an NBN event is triggered, it is handled in a new transaction independent of the original transaction that triggered the event. These transactions can also be queried through the transaction log. The result of the NBN transaction will be successful if a positive HTTP or HTTPS response code is received from the OSS/BSS. If no response is received (timeout) or a negative response code is received, the transaction will show as failed.

10.4. Northbound Notification Workflow

Perform the following procedures to configure northbound notification.

10.4.1. Procedure

1. Configure Northbound Notification Destination to specify the destination for northbound notifications.
2. Configure Northbound Notification Event to specify an event to trigger the northbound notification.
3. Configure Northbound Notification Event Attributes to specify the list of attributes to be received in a notification for a specific event.

   Note:

   Steps 2 and 3 can be performed in either order, but after the list attributes are defined in Step 3 you will need to edit the event (Step 2) to add or update the Attribute Selector field.

10.5. Configure Northbound Notification Destination

Use this procedure to set the destination for Northbound Notifications of VOSS-4-UC events. Only one NBN destination can be configured.

Note: You cannot delete a destination until it is removed or disassociated from all events.

10.5.1. Procedure

1. Log in as provider administrator.
2. Choose **Administration Tools > Northbound Notifications > Destination**.
3. Click **Add**.
4. Provide the following information for the destination:

Field	Description
Hostname/IP Address	Hostname or IP address of the OSS/BSS http server. This field is mandatory.
Port	The destination port. This field is mandatory.
Username	If the OSS/BSS http server has authentication enabled, specify the username to use.
Password	The password for the above username.
Secure	Use HTTPS send method for secure transport of the notification. Default = Selected. Clear the check box to use HTTP instead.

5. Click **Save**.

10.6. Configure Northbound Notification Event Attributes

You can use attribute selectors to define the attributes to be received in a notification for a particular event. Notifications contain only the specified fields and are not sent if none of the fields are chosen.

Note: You cannot delete an attribute selector until it is removed or disassociated from all events.

Important: It is possible to create an attribute selector through the API with 'invalid' attributes as there is no API validation on the list of attributes. We recommend using the GUI or API to retrieve the list of attributes prior to creating an attribute list through the API. Refer to the API Reference Guide. If an invalid attribute is added to an attribute filter, the transaction will succeed but notifications will not contain the chosen field.

10.6.1. Procedure

1. Log in as provider administrator.
2. Choose **Administration Tools > Northbound Notifications > Attributes**.
3. Click **Add**.
4. Enter a unique name.
5. Choose a model type: either data/NormalizedUser or relation/Subscriber.
6. Highlight one or more attributes and perform the following:
   - Click **Select** to add an attribute to the list of chosen attributes. You can also select multiple attributes at a time by highlighting them and clicking **Select**. The attributes move from the **Available** box to the **Selected** box.
   - Click **Remove** to remove an attribute from the list of chosen attributes. You can also remove multiple attributes at a time by highlighting them and clicking **Remove**. The attributes move from the **Selected** box to the **Available** box.

   Example: For the data/NormalizedUser model, you could select Username, First Name, Last Name, Phone Number, and Mail. Notifications are then sent when an event occurs that includes one or more of these attributes.
7. Click **Save**.

10.6.2. What to Do Next

Apply the event attributes to an event by adding or updating the event and choosing the desired attribute selector.

10.7. Configure Northbound Notification Event

You must set the Northbound Notification Destination before you can configure events.

Use this procedure to specify an event to trigger Northbound Notifications.

1. Log in as provider administrator.
2. Choose **Administration Tools > Northbound Notifications > Events**.
3. Click **Add**.
4. Provide the following information for the triggering event:

Field	Description
Name	Event name. Must be unique. This field is mandatory.
Description	A description of the event
Active	Select to turn on notification.
Model Type	Choose either data/NormalizedUser or relation/Subscriber as the model type of the data that triggers the event. This field is mandatory.
Operation	Choose from the operations applicable to the selected model type. This field is mandatory.
Attribute Selector	Set an attribute selector to restrict (filter) the list of attributes sent in notifications for this event. This field is optional. To remove an existing attribute selector, backspace and delete it from the Attribute Selector field. If you do not specify an attribute selector, all possible attributes are sent in notifications for this event.
Destination	The provider's NBN destination. This field is read-only.

5. Click **Save**.

11 LDAP Management

11.1. LDAP Integration

LDAP servers can be integrated with VOSS-4-UC for these two purposes:

- User synchronization - sync users from LDAP into VOSS-4-UC and use LDAP to authenticate users.
- User authentication only - use LDAP to authenticate users in VOSS-4-UC (either added locally or synced from Cisco Unified CM)

User synchronization is available for Active Directory (AD) and OpenLDAP.

User authentication only is not available for OpenLDAP.

Note:

- To use LDAP for authentication only, you must have VOSS-4-UC 10.6(3) or later.
- Since LDAP servers support case insensitive search base DNs, VOSS-4-UC supports this case insensitivity. For example, on an LDAP server, the following search base DNs are equal:
  - CN=Users,DC=example,DC=com
  - cn=Users,dc=example,dc=com

11.1.1. Multiple LDAP OUs Per Hierarchy

Large corporations and institutions with multiple domains or agencies may require more than one LDAP Organizational Unit (OU) to be configured at a hierarchy.

VOSS-4-UC allows for multiple LDAP OUs at a hierarchy by providing for a *unique combination* of the following LDAP server properties at the hierarchy:

- IP address
- Port
- search base DN

Multiple search base DNs can therefore be configured at the *same hierarchy* for different organizations within the same company, so that administrators and self-service users can successfully authenticate. For example:

LDAP server setup:

IP	Port	Search base DN	Hierarchy
1.2.3.4	389	ou=SharedOUA,dc=voss-solutions,dc=com	Provider.Customer
1.2.3.4	389	ou=SharedOUB,dc=voss-solutions,dc=com	Provider.Customer

Users:

- userA: ou=SharedOUA,dc=voss-solutions,dc=com
- userB: ou=SharedOUB,dc=voss-solutions,dc=com

11.2. Set up an LDAP Server

Use this procedure to set up an LDAP server for integration with VOSS-4-UC.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy node to the desired node where you want the users synchronized.
3. Choose **LDAP Management > LDAP Server**.
4. Click **Add**.
5. Complete, at minimum, the mandatory LDAP Server fields (see below).
6. Click **Save** to save the LDAP server.

11.2.1. LDAP Server Fields

Fields	Description
Description	Defaults to the current hierarchy level.
Host Name *	Hostname or IP address of the LDAP server. This field is required.
Port	Port number for LDAP traffic. Defaults to 389.
User DN *	The User Distinguished Name of an administrative user who has access rights to the Base DN on the LDAP server. This field is required. Examples: • Administrator@stb.com • OU=LDAP0,DC=stb,DC=com
Admin Password *	Admin password associated with the user. This field is required.
Search Base DN *	Base Distinguished Name for LDAP search. This should be a container or directory on the LDAP server where the LDAP users exist, such as an Organization Unit or OU. As an example, to search within an Organizational Unit called CUS01 under a domain called GCLAB.COM, the Search Base DN would be OU=CUS01,DC=GCLAB,DC=COM. This field is required.
Search Filter	An RFC 2254 conformant string used to restrict the results returned by list operations on the LDAP server.
Server Type *	Choose between **Microsoft Active Directory** or **OpenLDAP**. For AD LDS (ADAM), choose **Microsoft Active Directory**.
AD Sync Mode *	Defaults to Direct.
CUCM LDAP Directory Name	The name of the LDAP Directory configured on CUCM that we want this user to be considered synced from. The LDAP Directory must be configured on CUCM already. This is an optional parameter but the following should be considered: For top down sync scenario, Users will be added to CUCM as Local Users if this parameter is not set. For bottom up sync scenario, Users will not be able to log on to CUCDM if this parameter is not set.
Encryption Method	Choose between **No Encryption**, **Use SSL Encryption (ldaps://)**, or **Use StartTLS Extension**.
Server Root Certificate	If **Trust All** is Cleared, the LDAP server's SSL certificate is validated against this root certificate. If no **Server Root Certificate** is specified, validation is done against any existing trusted CA certificates. Use this option for custom root certificates in .pem format. See "SSO Certificate Management" for more information.
Trust All	Select this check box to disable certificate validation.
Primary Key Attribute	The attribute value used to uniquely identify and search for records on an LDAP server. For example, `uid` is the attribute when using a 389-Directory Server and `entryUUID` when using an OpenLDAP server. The attribute must be unique, should not change over time and should not be location specific. If no attribute is entered, `entryUUID` is used for an OpenLDAP server and `ObjectGUID` if the LDAP server is Microsoft Active Directory.

Search Filter examples:

- `(telephoneNumber=919*)`: all telephone numbers starting with 919
- `((&(OfficeLocations=RTP)(|(department=Engineering)(department=Marketing)))`: office is located in RTP and department is either Engineering or Marketing
- `(&(MemberOf=cn=Admin,ou=users,dc=foo,dc=com)(!(c=US)))`: all Admins except those in the U.S.

What to Do Next

Perform a test connection to ensure the LDAP server is configured correctly.

If the authentication credentials or search base DN are invalid, an error message pops up on the GUI, for example:

Error encountered while processing your request

caught exception: [Helper] validation failed; Invalid search base db.

11.3. Set up LDAP for User Synchronization

Follow these steps to set up an LDAP for user synchronization. This process synchronizes users from the configured LDAP directory into VOSS-4-UC. The users then appear at the hierarchy node at which the LDAP User Sync object exists. You can manage the users through User Management menu options (for example, move users to other hierarchies, or push to Cisco Unified Communications Manager).

Note: The LDAP Authentication Only check box is available only in VOSS-4-UC.

11.3.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node of the LDAP server you want to synchronize users from.
3. Choose **LDAP Management > LDAP User Sync**.
4. Click **Add**.
5. On the **Base** tab, provide the following information:

Field	Description
LDAP Server*	This read-only field displays the LDAP Server you are synchronizing users from.
LDAP Authentication Only	Important: Leave the check box clear to synchronize users from LDAP. Default is Clear. When cleared, users are synchronized from the configured LDAP directory and their passwords are authenticated against the configured LDAP directory. When selected, users are not synchronized from the configured LDAP directory, but their passwords are authenticated against the LDAP directory. When selected, you can manually add users from the GUI or API, bulk load them, or synchronize them from Cisco Unified CM.
User Model Type	The User Model Type identifies which LDAP object, defined in the configured LDAP server, is used to import and authenticate users. If the LDAP server is Microsoft Active Directory, the default is `device/ldap/user`. If the LDAP server is AD LDS (ADAM), this should be set to `device/ldap/userProxy`. If the LDAP server is OpenLDAP, the default is `device/ldap/inetOrgPerson`. To identify a non-default User Model Type to use, contact the LDAP server administrator.
LDAP Authentication Attribute	The attribute used for creating an LDAP user. This value will be used for LDAP authentication against LDAP when the **LDAP Authentication Only** check box is selected (see above field).
User Entitlement Profile	Choose the User Entitlement Profile that specifies the devices and services to which users synchronied users synchronized from the LDAP server are entitled. The chosen entitlement profile is assigned to each synchronized user. It is checked during user provisioning to ensure the user's configuration does not exceed the allowed services and devices specified in the entitlement profile.
User Role (default)*	The default role to assign to the synced user (if no other LDAP Custom Role Mappings are applicable for the synced user, then this fallback/default role will be applied). This field is mandatory.
User Move Mode	Indicates whether users are automatically moved to sites based on the filters and filter order defined in **User Management > Manage Filters**.
User Delete Mode	Indicates whether users are automatically deleted from VOSS-4-UC if they are deleted from the LDAP directory. If set to automatic, all subscriber resources associated with the user, such as a phone, are also deleted.
User Purge Mode	Indicates whether users are automatically deleted from VOSS-4-UC if they are purged from the LDAP device model. An administrator can remove the LDAP user from the device layer even if the user has not been removed from the LDAP directory.

6. Click the **Field Mappings** tab and modify the default mappings if required:
    - LDAP Username
        - For Microsoft Active Directory, this is typically the `sAMAccountName`.

  - For AD LDS (ADAM), the `sAMAccountName` attribute is not part of the default schema, but can be added if required. Confirm with the LDAP server administrator. Alternatively, use `uid`.
  - For OpenLDAP, this is typically the `uid`.
- Sn (Surname)

7. (Optional) Complete other field mappings as needed, for other operations such as pushing users to Cisco Unified Communications Manager or creating move filters.
8. Click **Save**.

An LDAP synchronization is scheduled, but is not activated by default. See *Synchronize Users from LDAP*.

Note: The following fields are *not* imported by VOSS-4-UC during LDAP synchronization:

```
photo
jpegPhoto
audio
thumbnailLogo
thumbnailPhoto
userCertificate
logonCount
adminCount
lastLogonTimestamp
whenCreated
uSNCreated
badPasswordTime
pwdLastSet
lastLogon
whenChanged
badPwdCount
accountExpires
uSNChanged
lastLogoff
dSCorePropagationData
```

11.4. Synchronize Users from LDAP

For VOSS-4-UC, you can synchronize users from LDAP by activating a scheduled synchronization, or by performing a manual synchronization.

Note: You cannot cancel a synchronization, and you cannot delete an LDAP server while a synchronization is in progress.

11.4.1. Procedure

1. To activate a scheduled LDAP synchronization:
   a. Browse to **LDAP Management > LDAP Schedule**.
   b. Click an LDAP Schedule.

c. Select the **Active** check box.

d. Click **Save**.

2. To perform a manual LDAP synchronization, see *Synchronize or Purge LDAP Users*.

VOSS-4-UC attempts to synchronize users from the LDAP server. It may take a few minutes for the users to show up in VOSS-4-UC.

11.4.2. What to Do Next

Browse to **User Management > Users** and verify that users were synchronized from LDAP.

11.5. Set up LDAP for Authentication Only

Use this procedure to set up LDAP to only authenticate users in VOSS-4-UC. Users may be added locally, or synced from Cisco Unified CM. Users who are LDAP synced in Cisco Unified CM and then synced into VOSS-4-UC will be LDAP authenticated by default. Users who are manually configured in Cisco Unified CM and then synced into VOSS-4-UC will not be LDAP authenticated by default. Users who are manually configured in VOSS-4-UC also will not be LDAP authenticated by default. The default behavior can be changed using the procedures described in View and Update LDAP Authentication Users.

Note: LDAP for Authentication Only is available at hierarchy nodes that have an LDAP server. Therefore, LDAP for Authentication Only is not available for users created at the site level.

Important: When **LDAP Authentication Only** is used (check box selected), then the **CUCM LDAP Directory Name** for the LDAP server must be filled in.

When more than one LDAP server sync is created and this is not filled in, no LDAP users will be created and a warning message will be seen in the transaction log.

11.5.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where you have set up the LDAP server you want to use to authenticate users.
3. Choose **LDAP Management > LDAP User Sync**.
4. Click **Add**.
5. On the **Base** tab, provide this information:

Field	Description
LDAP Server	Choose the LDAP Server you are authenticating users at.
LDAP Authentication Only	Important: Select this check box to use the LDAP server only to authenticate users. Default = Cleared. When cleared, users are synced from the configured LDAP directory and their passwords are authenticated against the configured LDAP directory. When selected: • The **CUCM LDAP Directory Name** for the LDAP server must be filled in. When more than one LDAP server sync is created and this is not filled in, no LDAP users will be created and a warning message will be seen in the transaction log. • Users are not synced from the configured LDAP directory, but their passwords are authenticated against the LDAP directory. • You can manually add users from the GUI or API, bulk load them, or sync them from Unified CM.
User Model Type	This read-only field identifies which LDAP object, defined in the configured LDAP server, is used to authenticate users.
LDAP Authentication Attribute	Choose the LDAP Attribute to be used to authenticate users. This field is mandatory. Options are: • sAMAccountName - AD only, this is the default for AD. • uid - OpenLDAP only, this is the default for OpenLDAP. • mail • employeeNumber • telephoneNumber • userPrincipalName - AD only. These are the same values Unified CM users for LDAP Attribute for User ID. Caveats (AD only) For the following types of users, do not select userPrincipalName, unless the userPrincipalName value was set as the Username when the user was created: • Users created using the VOSS-4-UC GUI • Users created using the VOSS-4-UC API • Users bulk loaded into VOSS-4-UC • Users manually created in Unified CM and synced into VOSS-4-UC For users synced from LDAP into Unified CM and then into VOSS-4-UC: Caveats (AD and OpenLDAP) For users synced from LDAP into Unified CM and then into VOSS-4-UC: • We strongly recommend selecting the same LDAP Authentication Attribute as Unified CM uses for LDAP Attribute for User ID. • If you sync users into Unified CM using attributes other than sAMAccountName/uid, do not choose sAMAccountName/uid. If you sync users from LDAP into Unified CM using employeeNumber, choose employeeNumber for the LDAP Authentication Attribute. However, to get the LDAP Authentication to work properly, one of these conditions must be met: • Before syncing users from Unified CM to VOSS-4-UC, set the Employee Number field on the CUCM Server FieldMapping tab to userid. • Define the LDAP for Authentication Only sync before syncing users from Unified CM into VOSS-4-UC

6. Click **Save**.

All users that have SyncToHierarchy set to the hierarchy of the LDAP server now use the LDAP server for authentication. The users are added to the LDAP Authentication Users list.

11.6. View and Update LDAP Authentication Users

All users that use LDAP for authentication are displayed here. This list includes users that use LDAP for authentication only, and users that have been synced from LDAP.

Note: To view and update LDAP Authentication Users, you must have VOSS-4-UC.

11.6.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **LDAP Management > LDAP Authentication Users**. For each user that uses LDAP for authentication the following information is displayed:

Field	Description
LDAP Username	Matches the value of the LDAP authentication attribute which is specified in the User Model Type field of the LDAP User Sync configuration.
Data Username	The username either created in VOSS-4-UC, or synced from Cisco Unified CM, or synced from LDAP.
LDAP Server	The LDAP server being used for authentication.

3. To disable LDAP authentication for a user, click the user, then click **Delete**. The user is removed from the LDAP Authentication Users list. Local authentication is used for the user to log in.
4. To update LDAP authentication for a user, click the user. Make the update, then click **Save**. You can update only the LDAP Username field. However, LDAP authentication fails if the corresponding change is not also done on LDAP.

11.7. Set up LDAP Custom Role Mappings

This feature is used to apply customized roles to LDAP Synced and moved users, and to overwrite the default roles that are applied to them following an LDAP User Sync or Move User operation.

Important: For LDAP User Sync

- When a user is synced in from an LDAP server, by default they are assigned the role configured in the 'User Role (default)' in the LDAP User Sync.
- If the user's **Active Directory Group** Membership matches a group configured in the Custom Role Mapping, and the hierarchy of the LDAP User Sync matches the **Target Role Context**, then the role specified in the Custom Role Mapping will take precedence over the 'User Role (default)'.

For Move User

- When a user is moved to a hierarchy manually using 'Move Users', by default they are assigned the role specified in the 'Set Default Role'.
- If the user's **Active Directory Group** matches a group configured in the Custom Role Mapping, and the user's destination hierarchy type matches the **Target Role Context**, then the role specified in the Custom Role Mapping will take precedence over the 'Set Default Role' chosen in 'Move Users'.
- When a user is moved to a hierarchy automatically using a filter, they are assigned the role specified in the filter in 'Set Default Role' by default.
- If the user's **Active Directory Group** Membership matches a group configured in the Custom Role Mapping, and the user's destination hierarchy type, specified in the filter matches the **Target Role Context**, then the role specified in the Custom Role Mapping will take precedence over the 'Set Default Role' set in the filter.

11.7.1. Procedure

1. Log in as provider or reseller administrator.
2. Set the hierarchy path to where the LDAP Custom Role Mapping must be added.
3. Choose **LDAP Management > LDAP Custom Role Mappings**.
4. Click **Add**.
5. Complete the following mandatory fields:

Field	Description
Active Directory Group*	A group in the Active Directory to which the user belongs. This is derived from the 'memberOf' from the LDAP Schema. This must be an exact match of the value defined in Active Directory, e.g. CN=Administrators,CN=Builtin,DC=test,DC=net.
Target Role Context*	This value defines the hierarchy for which the Custom Role Mapping will be applied. This must match the hierarchy type where the users are Synced, or their destination hierarchy when moved. For example, if the user is assigned a 'CustomerAdmin' role, and the LDAP User Sync is configured at Customer level then the **Target Role Context** must be set to Customer. If the user is assigned a 'SiteAdmin' role, and the user is being moved either manually or automatically using 'Filter to a Site', then the **Target Role Context** must be set to Site. Choose the hierarchy node type from the drop-down list.
Target Role*	The role which will be applied to the user if their **Active Directory Group** and **Target Role Context** are matched. This must be a valid role at the user's destination hierarchy. This can be defined at a specific role or defined as a macro, e.g. if the user is assigned a 'SiteAdmin' role then the role can be defined as the exact name of the role or defined as a macro, which allows re-use for any site name e.g. {{macro.SITENAME}}SiteAdmin.

6. Click **Save**.

11.8. Re-provision Synced LDAP Users

Use this procedure to re-provision users that were synchronized from an LDAP server, in particular, those users that have been updated on the LDAP server and for which these updates have not been propagated through VOSS-4-UC.

In particular, the re-sync will force an update of the selected users on all UC apps by executing an update Data Sync as well as its associated workflow.

11.8.1. Procedure

1. Log in as a customer administrator or higher and select **User Management > Sync & Purge > LDAP Re-Provision Users**.
2. Choose the LDAP Server on which the users need to be re-synced.
3. From the LDAP Users control, add one or more users to re-sync.
4. Click **Save** to start the re-sync action.

12 Single Sign On

12.1. SSO Certificate Management

Use this procedure to create a self-signed or third-party-signed system certificate to use when setting up Single Sign-On (SSO) on the web proxy node on VOSS-4-UC.

Note:

- Web server certificate management is carried out on the VOSS-4-UC command line. Refer to the CLI documentation for details.
- During customer onboarding, SSO certificate creation is customer specific.

Procedure

1. Log in as hcsadmin.
2. Choose **Single Sign On > Certificate Management**.
3. Click **Add**.
4. On the **Base** tab, enter a **Name** and **Description** for the certificate.
    - For a self-signed certificate, leave the **Generate Certificate Signing Request** check box clear.
    - For a third-party-signed certificate, select the **Generate Certificate Signing Request** check box.
5. For a self-signed certificate, control when the certificate is valid by changing the Valid From and Valid To fields. These are measured in seconds and default to 0 (now) and 315360000 (10 years), respectively.
6. (Optional) Change the **Key Length** from the default of 1024.
7. Click the **Certificate Information** tab, and complete all mandatory fields (see **Certificate Management** fields).
8. Click **Save**.
9. If you created a self-signed certificate you are done. If you requested a third-party-signed certificate, continue to the next step.
10. Click the certificate you just created.
11. Choose **Action > Export Certificate Request**.
12. Follow your organization's procedures to obtain the third-party signature for the certificate.
13. Click the certificate.
14. Choose **Action > Upload Signed Certificate**.

15. Browse to the signed certificate and click **OK**.

12.1.1. Certificate Management Fields

Field	Description
Common Name *	Enter the FQDN for your server.
Country Code *	A two-digit country code
State *	An appropriate country subdivision
City *	Your city
Organization *	Your organization
Organization Unit *	Your organization subunit

12.2. Configure Single Sign-On for VOSS-4-UC

Before You Begin

Create a self-signed or third-party-signed system certificate before you configure self-service SSO. For more information, see *SSO Certificate Management*.

The VOSS-4-UC server and the IdP (identify provider) server must be configured so that their clocks are synchronized.

Follow these steps to configure self-service Single Sign-On (SSO) for VOSS-4-UC. The configuration applies to the customers and customer administrators associated with the IdP.

Note: SSO support for administrative users is defined as follows:

- SSO is not supported for administrative users under **User Management > Local Admins** because their passwords are stored locally (and so are not available for SSO).
- SSO is supported for administrative users under **User Management > Users**, except for users with the Role set to SelfService.

Procedure

1. Log in to VOSS-4-UC as hcsadmin.
2. Choose **Single Sign On > SSO SP Settings**.
3. Click **Add**.

   Note: Configure only one instance of SSO SP Settings.
4. On the **Base** tab, from the mandatory **System Certificate** drop-down, choose the System Certificate to use. To allow the SSO SP Setting to expire, enter a number of hours in the **Validity (Hours)** field.

   Note:

   - Specifying an unsigned third-party-signed certificate will result in an error.
   - To renew an expired certificate, follow the steps: *Renew Single Sign-On Certificate for VOSS-4-UC*.

5. On the **SAML SP Settings** tab, enter the mandatory **FQDN of the Server**.

   Select the **Sign Authn Requests** and **Want Assertions Signed** check boxes as required by your security environment.

   Note that if a secure connection is required with the secure attribute set on the cookies, the URL values for bindings of End Points must be specified with `https`.

6. Click **Save**.
7. To view the location of the VOSS-4-UC SP metadata that you will upload to the IdP, choose **Single Sign On > SSO SP Metadata**. Point your browser to the URL shown here, and then save a copy of the SP metadata.
8. Upload the SP metadata to the IdP.

   Refer to your IdP documentation for details on configuring SSO on your IdP.

   Note:

   The IdP must release the UID and map it to an appropriate attribute. For example, an IdP that authenticates with Active Directory can map the uid SAML attribute to sAMAccountName in the Active Directory server.

9. Download the IdP metadata from the IdP server.

   Refer to your IdP documentation for details on downloading IdP metadata.

   Note:

   If an expired SSO certificate is being renewed and the IdP metadata has *not* changed, then the download, configure and upload of the IdP metadata is not required.

10. Log in as provider, reseller, or customer administrator, depending on your IdP configuration level.
11. Choose **Administration Tools > File Management** and upload the IdP metadata.
12. Choose **Single Sign On > SSO Identity Provider**.
13. Click **Add** to add the SSO Identity Provider configuration.

    Note: Only one instance of an SSO Identity Provider can be configured for a hierarchy node.

14. On the **SSO Identity Provider** screen, complete at minimum, the mandatory **SSO Identity Provider** fields (see **SSO Identity Provider** fields).
15. Click **Save** to save the SSO Identity Provider Configuration and enable SSO if selected.
16. Choose **Single Sign On > SSO User** to display enabled SSO users.

Use this URL for your SSO login:

`https://<FQDN of the Server>/sso/<login_URI>/login`

Upon login, the IdP will redirect you to this FQDN.

12.2.1. SSO Identity Provider Fields

Field	Description
Entity Id *	Entity ID of the IdP. This can be extracted from the IdP metadata file. This field is mandatory.
Login URI *	Login URI for the IdP. This is the URI that will be embedded in SSO Login URL. It can contain only alphanumeric characters and forward slashes. This field is mandatory.
Local Metadata File *	Choose the IdP metadata file. This field is mandatory and must be unique across the system.
SSO Enabled	Select the check box to enable SSO for users synced in or created at the current hierarchy level. Clear this check box to disable SSO for the users associated with the defined IdP.
Note	Reminder to upload the IdP metadata file
SSO Login URL	Read-only field displays the SSO Login URL to use.

12.3. Renew Single Sign-On Certificate for VOSS-4-UC

If a customer's Single Sign-on certificate expires, follow the steps below to renew the certificate for VOSS-4-UC:

1. Follow the steps to regenerate the certificate (either self-signed or CA signed) as described in *SSO Certificate Management*.
2. Follow the steps to regenerate and upload SP metadata to the IdP described in *Configure Single Sign-On for VOSS-4-UC*.

   Note:

   If an expired SSO certificate is being renewed and the IdP metadata has *not* changed, then the download, configure and upload of the IdP metadata is not required and these steps can be ignored.

12.4. SAML Elements in Assertions

The following list provides details for designers on the correct handling of Security Assertion Markup Language (SAML) elements in assertions:

1. When using the `SubjectConfirmation` element in a SAML assertion, the `NotOnOrAfter` condition shall be used.
2. When using the `Conditions` element in a SAML assertion, both the `NotBefore` and `NotOnOrAfter` elements or the `OneTimeUse` element shall be used.
3. If a `OneTimeUse` element is used in an assertion, there shall only be one used in the `Conditions` element portion of an assertion.

The VOSS-4-UC system will inspect SAML messages and raise error messages if the elements do not follow the rules for SAML assertions specified above.

The list below shows the respective error numbers and messages as they will show in the logs, as well as example error SAML snippets:

1. NOTONORAFTER_SUBJECTCONFIRMATION_ERROR (14010)

   “SubjectConfirmation is used but there is no NotOnOrAfter attribute”

```
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData/>
</saml2:SubjectConfirmation>
```

2. a) CONDITION_NOT_BOTH (14012)

   “NotBefore and NotOnOrAfter should be present when using either in Condition”

```
<saml2:Conditions NotOnOrAfter="2015-11-20T12:32:23.645Z">
    <saml2:AudienceRestriction>
        <saml2:Audience>http://functional.fedrampfail.plain/sso/metadata/</
↪saml2:Audience>
    </saml2:AudienceRestriction>
</saml2:Conditions>
```

2. b) CONDITION_ONETIMEUSE (14013)

   “OneTimeUse element should be present when neither NotBefore nor NotOnOrAfter attributes in Condition”

```
<saml2:Conditions>
    <saml2:AudienceRestriction>
        <saml2:Audience>http://functional.fedrampfail.plain/sso/metadata/</
↪saml2:Audience>
    </saml2:AudienceRestriction>
</saml2:Conditions>
```

3. CONDITION_MULTIPLE_ONETIMEUSE (14014)

   “Only one OneTimeUse element should be present in Condition”

```
<saml2:Conditions>
    <saml2:AudienceRestriction>
        <saml2:Audience>http://functional.fedrampfail.plain/sso/metadata/</
↪saml2:Audience>
    </saml2:AudienceRestriction>
    <saml2:OneTimeUse/>
    <saml2:OneTimeUse/>
</saml2:Conditions>
```

13 Entitlement Management

13.1. Entitlement

VOSS-4-UC Entitlement represents the set of rules surrounding the suite of services and devices (and their number) available for particular subscribers. For instance, one customer may specify that end users may only have voice service with a maximum of two devices, one being a flavor of IP set, and the other being an analog set. Another customer may configure their end users to have both voice and voicemail services, with a maximum of ten devices limited to SIP sets. Both of these are valid rule sets intended to govern their respective users' service or device set.

There are four principal VOSS-4-UC models from which the entitlement rule sets are built.

13.1.1. Device Types

Device types represent the suite of physical devices which may be grouped into device groups for subsequent entitlement purposes. These device types should mirror the supported product types available on the Cisco Unified Communications Manager.

The device type data model is prepopulated with a snapshot of current product types; however, the provider administrator can add, as well as update or remove, additional device types, if needed.

13.1.2. Device Groups

A device group is a subset of device types. Device groups are not necessarily discrete; that is, different device groups may share specific device types.

Provider administrators can add, delete, and update device groups. Reseller and customer administrators can only view device groups.

13.1.3. Entitlement Catalogs

An entitlement catalog specifies supported device groups and available services (broad categories of functionality) for a particular hierarchy. The services which are available to be selected in an entitlement catalog are as follows: Voice, Voicemail, Presence, Extension Mobility, Single Number Reach, WebEx, CMR, and Webex Teams. Entitlement catalogs also set the maximum allowed number of total devices and the maximum allowed number of devices in each device group within the catalog.

If entitlement is to be used, an entitlement catalog must exist at the Provider hierarchy node. No more than one entitlement catalog may exist at any given hierarchy node. The entitlement catalog at a particular

hierarchy node restricts the device groups, device counts, and services which are available to entitlement profiles at or below that node in the hierarchy. No entitlement profile may exceed the restrictions imposed by its associated entitlement catalog. Similarly, an entitlement catalog at a particular hierarchy imposes limitations on any subsequent entitlement catalogs beneath it in the hierarchy structure. No entitlement catalog created deeper in the hierarchy structure may exceed the restrictions specified in a higher entitlement catalog.

Provider administrators can add, update, and delete entitlement catalogs at their hierarchy level and below. Reseller and customer administrators can only view entitlement catalogs.

13.1.4. Entitlement Profiles

Entitlement profiles establish the set of services, device groups, and device limits to which an end user may subscribe. No entitlement profile may exceed the specifications dictated by the hierarchy-associated entitlement catalog. An entitlement profile may not exist at a particular hierarchy node unless an entitlement catalog exists at or above the entitlement profile's hierarchy node.

Unlike entitlement catalogs, there may be multiple entitlement profiles at a given hierarchy node. Each of these entitlement profiles must have a unique name within the hierarchy. Additionally, no device type may appear in more than one device group within a given entitlement profile.

Entitlement profiles can be assigned to users when users are synced from Cisco Unified Communications Manager or from LDAP, or when users are added or modified in VOSS-4-UC via Subscriber Management and User Management.

Provider administrators can add, update, and delete entitlement profiles at their hierarchy level and below. Reseller and customer administrators can only view entitlement profiles.

13.1.5. Entitlement Defaults

Entitlement defaults work differently depending on how a user is added to VOSS-4-UC:

- Bottom-up (UCM user sync)

  This is based on the entitlement profile setting on the UCM server (publisher) the user is being synced from. The default entitlement profile is not used in this path.

- Quick Add Subscriber

  This assigns the entitlement profile selected on the portal/loader by the administrator who adds the subscriber. When using QAS via the portal, it pre-populates the entitlement drop-down with the entitlement profile tagged as default.

- LDAP Top-down

  Entitlement is determined by the entitlement profile setting on the LDAP User sync that is syncing the user in. The default entitlement profile is not used in this path.

- User Management/Subscriber Management Add (GUI or loader)

  This uses the value provided via the portal/loader. The default entitlement profile is not used in this path.

Important: When a user has an empty value for their Entitlement:

- If the user's Entitlement value is blank, and none of the Entitlement Profiles in the User's hierarchy tree have the **Default Profile** check box selected (set to true), then no Entitlement Profile is applied and no Entitlement checking is done. This means all services and all phones are available to the User.
- If the user's Entitlement value is blank, and one of the Entitlement Profiles **does** have the **Default Profile** check box selected (set to true), in the User's hierarchy tree, then the User will inherit this Entitlement Profile.
- If the **Default Profile** check box is cleared (set to false) from one Entitlement Profile and added to another Entitlement Profile, then this new Entitlement Profile will become the default Profile applied to all Users in the hierarchy below whose Entitlement Profile is blank.

13.2. Entitlement Enforcement

- Device Groups

  A user to whom an entitlement profile is applied is limited to devices in the device groups assigned in the entitlement profile. Adding a Phone to a user in Subscriber Management fails if the added Phone is not in a device group assigned to the entitlement profile applied to the user.

- Device Limits

  A user to whom an entitlement profile is applied is subject to the following device limits set in the entitlement profile:

  – Total number of devices

  – Total number of devices in a device group

  Adding a Phone to a user in Subscriber Management fails if the total number of devices limit or the total number of devices in a device group limit is exceeded.

- Transaction Log

  The transaction log messages contain detailed information that can be used to determine what entitlement profile limitation caused an action to fail.

13.2.1. Service Levels

The following table shows the impact to a user when a service is disabled in the entitlement profile applied to the user.

Note: An entitlement profile can be explicitly assigned to a user, or implicitly applied if an entitlement profile is designated as the default entitlement profile in a hierarchy node at or above the user's hierarchy node.

Service disabled	Result
Voice	Adding a phone to a user in Subscriber Management fails. For an existing user with a phone with this profile (where voice is disabled), the update of the user from "Subscriber Management" fails, unless the existing phones for the user are dissociated.
Voicemail	Adding Voicemail to a user in Subscriber Management fails. For an existing user with Voicemail, updates in Subscriber Management fail after an entitlement profile with Voicemail disabled is applied to the user.
Presence	Enabling Cisco Unified Communications Manager IM and Presence Service for a user in Subscriber Management fails. For an existing user with Cisco Unified Communications Manager IM and Presence Service enabled, updates in Subscriber Management fail after an entitlement profile with Presence disabled is applied to the user.
Extension Mobility	Adding Extension Mobility to a user in Subscriber Management fails. For an existing user with Extension Mobility, updates in Subscriber Management fail after an entitlement profile with Extension Mobility disabled is applied to the user.
Single Number Reach	For a new user, adding Single Number Reach in Subscriber Management fails, and for an existing user with Enable Mobility checked, adding Single Number Reach fails after an entitlement profile with Single Number Reach disabled is applied to the user.
WebEx	Adding or assigning WebEx feature to the subscriber fails if this field is disabled. For an existing subscriber if you enable WebEx and an entitlement profile with "WebEx disabled" is applied, the update operation fails.
CMR	Adding or assigning CMR feature to the subscriber fails if this field is disabled. For an existing subscriber if you enable CMR and entitlement profile with CMR disabled is applied, the update operation fails.
Webex Teams	Webex Teams is not available for a new subscriber if this field is disabled. If Webex Teams is enabled for an existing subscriber, and an entitlement profile with Webex Teams disabled is applied, the update operation fails.

13.3. Entitlement Workflow

13.3.1. Procedure

1. (Optional) Define additional device types.
2. Create device groups to define sets of device types that users may be entitled to.
3. Create entitlement catalogs to define limits on devices and services that entitlement profiles may entitle users to.
4. Create entitlement profiles to define the devices and services users are entitled to.
5. Identify the entitlement profile for users synced from Cisco Unified Communications Manager.
6. Identify the entitlement profile for users synced from LDAP.
7. Assign entitlement profiles to existing users in VOSS-4-UC.

13.4. Add Device Type

VOSS-4-UC is prepopulated with a list of current product types. However, the provider administrator may add additional device types as needed.

13.4.1. Procedure

1. Log in as provider administrator.
2. Choose **Entitlement > Device Types**.
3. Click **Add**.
4. Enter the new device type.
5. Click **Save**.

The new device type is added to the list of available device types that can be assigned to a device group.

13.5. Create Device Group

Device groups are used to limit entitlement to a defined subset of available device types.

13.5.1. Procedure

1. Log in as provider administrator.
2. Choose **Entitlement > Device Groups**.
3. Click **Add**.
4. Enter a name and optional description for the device group.
5. Choose devices from the list of available device types and move them into the selected list by clicking **Select**.
6. Click **Save**.

The device group is created and can now be used in entitlement catalogs and entitlement profiles.

13.6. Create an Entitlement Catalog

Entitlement catalogs limit the capabilities of entitlement profiles defined at hierarchy nodes at the same level or below where the entitlement catalog is defined.

Entitlement catalogs can be defined at the provider, reseller, or customer hierarchy level. Only one entitlement catalog may be defined at a given hierarchy node.

13.6.1. Procedure

See procedure below for clarity if required:

1. Log in as provider administrator.
2. Set the hierarchy path to the location where you want to create the entitlement catalog.
3. Choose **Entitlement > Catalogs**.
4. Click **Add**.
5. Enter a name and optional description for the entitlement catalog.
6. Select the services check boxes to include in the entitlement catalog. The available services are Voice, Voicemail, Presence, Extension Mobility, Single Number Reach, WebEx, CMR, and Webex Teams.
7. Specify the maximum number of devices allowable for the entitlement catalog.

   The maximum number cannot exceed the total of the maximums for all the device groups included in the entitlement catalog.
8. Click'+' next to **Device Groups**, and from the **Device Group** drop-down, choose a Device Group to include in the entitlement catalog.
9. Specify the maximum number of devices allowed for the selected device group.

   The maximum number for any device group cannot exceed the maximum number of devices for the catalog.
10. Click + to add more device groups to the entitlement catalog.
11. Click **Save**.

The entitlement catalog is created. Entitlement profiles can now be created at or below the level of the entitlement catalog (see: *Create an Entitlement Profile*).

13.7. Create an Entitlement Profile

Before You Begin

Define an Entitlement Catalog at or above the hierarchy node where you create an Entitlement Profile (see *Create an Entitlement Catalog*).

The Entitlement Catalog restricts the service and devices that can be entitled in the Entitlement Profile. An Entitlement Profile can further restrict services and devices a user is entitled to. However, it cannot expand the services and devices beyond the restrictions defined in the Entitlement Catalog.

Entitlement Profiles are used to define the services and devices a user is entitled to. An Entitlement Profile can be assigned to a user in these situations:

- When you sync the user into VOSS-4-UC from LDAP.
- When you sync the user into VOSS-4-UC from Cisco Unified Communications Manager.
- When you create or modify the user in VOSS-4-UC using Subscriber Management or User Management.

Note: The Maximum Number of Devices and Maximum Number of Devices in a Group are limitations for each individual user, not for all users in the system.

Procedure

See procedure below for clarity if required:

1. Log in as provider administrator.
2. Set the hierarchy path to the location where you want to create the Entitlement Profile.
3. Choose **Entitlement > Profiles**.
4. Click **Add**.
5. On the **Profiles** screen, complete at minimum, the mandatory **Entitlement Profiles** fields.
6. Click + next to **Device Groups** to add more device groups to the Entitlement Profile if required.
7. Click **Save**.

The Entitlement Profile is defined and can be assigned to users.

13.7.1. Entitlement Profiles Fields

- *Contact Center Management*

Field	Description
Name *	Entitlement Profile name. This field is mandatory.
Description	An optional description of the entitlement Profile
Default Profile	Select this check box to make this Entitlement Profile the default for the hierarchy node. Any previously designated User Entitlement Profile automatically has this check box cleared.
Voice	Select this check box to entitle voice services.
Voicemail	Select this check box to entitle voicemail services.
Presence	Select this check box to entitle presence services.
Extension Mobility	Select this check box to entitle Extension Mobility services.
Single Number Reach	Select this check box to entitle Single Number Reach service.
WebEx	Select this check box to add the WebEx service to the profile.
CMR	Select this check box to add Collaboration Meeting Rooms (CMR) service to the profile. Select WebEx service to select CMR.
Webex Teams	Select this check box to add the Webex Teams service to the profile.
Contact Center	Select this check box to add the Contact Center service to the profile.
Maximum Number of Devices *	Specify the maximum number of devices allowable for the Entitlement Profile. This field is mandatory. The maximum number cannot exceed the total of the maximums for the entire device group included in the Entitlement Profile.
Device Group *	Choose a Device Group to include in the Entitlement Profile. This field is mandatory.
Maximum Number of Devices in Group *	For the selected device group, specify the maximum number of devices allowed. This field is mandatory. The maximum number for any device group cannot exceed the maximum number of devices for the profile.

14 User Management

14.1. Users and Subscribers

14.1.1. User Management and Subscriber Management

In VOSS-4-UC there are two types of users, each with different properties and purposes, but closely related:

- VOSS-4-UC Users (found in **User Management > Users**)
- Subscribers (found in **Subscriber Management > Subscribers**)

It is important to understand how the two types of users operate and how they relate to each other. Both types of users have an impact during user provisioning operations such as LDAP sync, Cisco Unified Communications Manager (Cisco Unified CM) sync, or user bulk loading. The major distinction between the two types of users is that VOSS-4-UC Users exist only on VOSS-4-UC, while Subscribers exist on the UC applications (Cisco Unified Communications Manager, Cisco Unity Connection, and WebEx).

The primary purpose of VOSS-4-UC Users is to provide a way for you to stage users into VOSS-4-UC before you determine which site, and which UC applications to assign to the users. Once a VOSS-4-UC User is sent to a Cisco Unified CM, a corresponding Subscriber comes into existence.

A typical flow of user provisioning is to sync users from LDAP into VOSS-4-UC, move the users to one or more sites, and push the users to UC applications. When the user is synced from LDAP to VOSS-4-UC, a VOSS-4-UC User is created (but not a subscriber). The VOSS-4-UC User is then moved to a site (**User Management > Move Users**). The subscriber can be created with either the advanced subscriber (**Subscriber Management > Subscribers**) or the quick add subscriber (**Subscriber Management > Quick Add Subscriber**). This is known as the “top-down” approach to user provisioning that progresses from LDAP to VOSS-4-UC User to Subscriber. The VOSS-4-UC User provides a way for you to manage the user before the user is assigned to a specific site and sent the Cisco Unified CM.

You do not need to send all VOSS-4-UC Users to a Cisco Unified CM and have a corresponding Subscriber created; this is a decision by the administrator based on criteria associated with each user. We recommend that you filter out any users from LDAP that are not eligible for UC services. It is possible that some ineligible users cannot be filtered due to missing attributes and thus get synced into VOSS-4-UC. These users remain as VOSS-4-UC Users and do not have a corresponding Subscriber created.

VOSS-4-UC Users provide more capabilities other than the ability to stage users in VOSS-4-UC prior to sending to Cisco Unified CM:

- LDAP sync—The workflows to manage syncing users from LDAP
- LDAP authentication—Enabling and disabling LDAP authentication
- SSO—Enabling and disabling SSO authentication

- Provisioning status—Tracking where the user came from (LDAP, Cisco Unified CM, manual configuration) and which hierarchy the user was originally added to
- Moving users—Moving users between hierarchy nodes

All Subscribers have a corresponding VOSS-4-UC User. This allows the user to sign in to VOSS-4-UC using either local authentication, LDAP authentication, or SSO authentication, and to track the provisioning status. You can also create a Subscriber directly, either through the GUI, through bulk load, or using Cisco Unified CM sync. A VOSS-4-UC User instance is created automatically. Therefore, as an administrator, you don't have to explicitly add a VOSS-4-UC User as a separate step, if staging is not needed, as is the case when configuring Subscribers directly on a site using bulk loading.

Subscribers provide all of the UC application provisioning logic by distributing the user configuration to each of the UC applications: Cisco Unified Communications Manager, Cisco Unity Connection, and WebEx. Subscribers combine most of the data associated with a user into one logical entity:

- Cisco Unified CM users
- Phones
- Lines
- Extension Mobility profiles
- Remote destinations
- Voicemail
- WebEx users

Each subscriber comes into existence when the Cisco Unified CM End User is created, and disappears when the Cisco Unified CM End User is deleted. Unlike VOSS-4-UC Users, there is no local data in VOSS-4-UC that defines the Subscriber. It is all based on data in the UC applications themselves. In the **Subscriber Management > Subscribers** list view, any user that has a Cisco Unified CM End User instance appears in the list, regardless of whether there is any other data associated with the user (for example, phone, line, and so on).

If the Cisco Unified CM End User is deleted, either on Cisco Unified CM directly, or from VOSS-4-UC, the Subscriber disappears. The Subscriber disappears even if there are phones, lines, or profiles that remain that were previously associated with that user. This is why you see the phrase "comes into existence", because the Subscriber is simply a representation of data in the UC applications. When the UC application data is created (in particular, the Cisco Unified CM End User), the Subscriber appears in the list view and can be viewed. When the UC application data is deleted (in particular, the Cisco Unified CM End User), the Subscriber disappears.

Note: Any changes on the Cisco Unified CM, such as adding or deleting end users, appear in VOSS-4-UC only after a sync has been performed. Refer to the "Data Sync" section of the Guide for more information on data syncing.

Because Subscribers are simply a representation of the data in the UC applications, you make changes either in VOSS-4-UC or in the UC applications directly. As an administrator, you make changes in the Advanced Subscriber GUI page (**Subscriber Management > Subscribers**) and that updates the data on the UC applications immediately. Alternatively, you can make changes directly in the UC applications. The next time you view a particular subscriber in VOSS-4-UC Manager, the changes appear. Thus, the UC applications provide accurate information about the user configuration and you can use whichever interface is most effective.

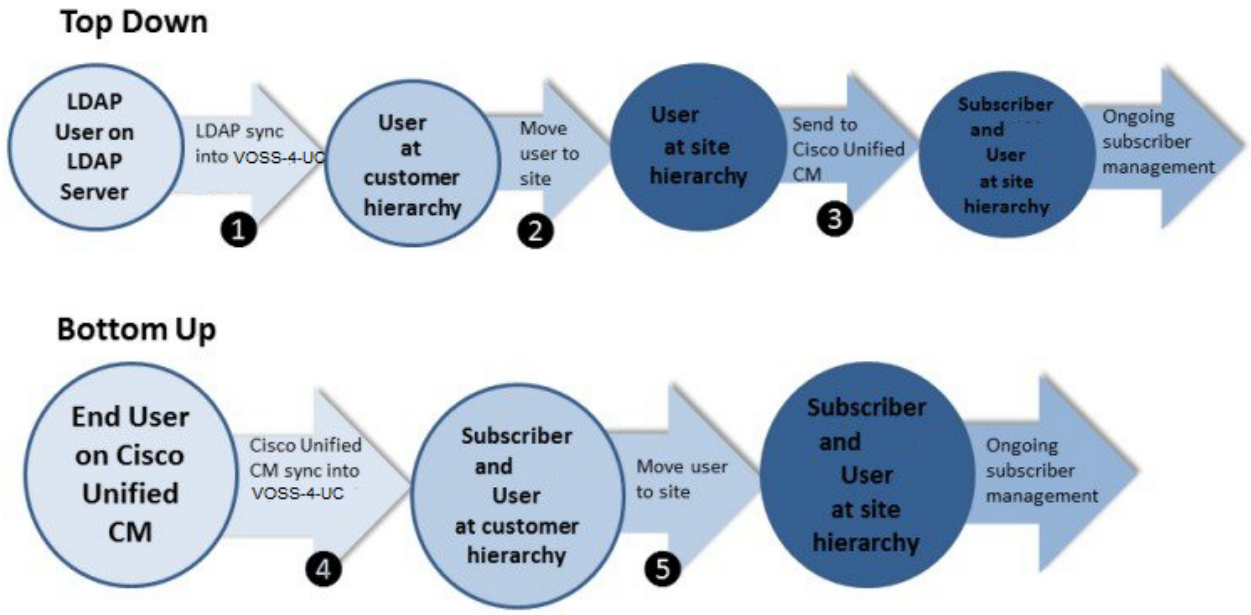
In summary, the difference between VOSS-4-UC Users and Subscribers is primarily the distinction between VOSS-4-UC data and UC application data. VOSS-4-UC Users encapsulate all of the VOSS-4-UC local data

associated with the user, and Subscribers encapsulate all of the UC application data associated with the user. A VOSS-4-UC User can be created independent of a Subscriber, but a Subscriber always has an associated VOSS-4-UC User.

Refer to the “User Management” section and “Subscriber Management” sections of this document for more details about each type of user.

14.1.2. User Management and Subscriber Management Use Cases

This following are two typical user provisioning use cases:



Use the following menus in VOSS-4-UC to perform the operations shown in the preceding figure:

1. **User Management Sync & Purge LDAP Users**
2. **User Management Move Users**
3. Performed by any of the following:
   - **User Management > Manage Users**
   - **Subscriber Management > Subscribers**
   - **Subscriber Management > Quick Add Subscriber**
4. **User Management > Sync & Purge > CUCM Users**, **Lines**, **Phones**
5. **User Management > Move Users**

In each diagram, the user starts on an external server, either an LDAP server (for example, Open LDAP or Active Directory), or on Cisco Unified CM. When the user is synced into VOSS-4-UC, either a VOSS-4-UC User is created, or both a VOSS-4-UC User and Subscriber are created. For each step, the diagram also shows the hierarchy node where the user exists. The result in both cases is that both a Subscriber and a VOSS-4-UC User exist. From that point, the user is primarily managed from Subscriber Management.

14.2. End-User Provisioning Workflow

14.2.1. Prerequisites

End-user provisioning with VOSS-4-UC depends on the completion of the following customer onboarding tasks:

- Devices defined (Cisco Unified Communications Manager, UC applications, WebEx)
- Network Device Lists (NDLs) created
- Single Sign On enabled, if necessary
- LDAP integration enabled, if necessary
- Any customer equipment to be monitored defined
- Customer sites defined with associated NDLs
- Customer and site dial plans configured
- Directory Number Inventory configured
- Voice Mail service defined and associated with a customer

See also *Example Fulfillment Procedures*.

14.2.2. Sample End-user Provisioning Workflow

The following is a sample end-user provisioning workflow. Not all steps apply for all customers. Some steps can be performed in alternate order.

1. Synchronize users from the LDAP server:
   - Set up LDAP for User Synchronization
   - Synchronize Users from LDAP
2. If LDAP synchronization is not used and users are provisioned on Cisco Unified Communications Manager (Unified CM), you can synchronize users from Unified CM. For more information, see *Synchronize Users, Lines, and Phones from Cisco Unified CM*.
3. In addition to synchronizing users, you can manually create users. For more information, see *Create and Update a User*.
4. (Optional) You can explicitly assign a credential policy to a user. For more information, see *Assign a Credential Policy to a User*.
5. Move users to sites using any of the following methods:
   a. Define move filters. For more information, see *Define a Filter*.
   b. Enable automatic user moves for synchronization. For more information, see Automatically Move Users Synchronized from Cisco Unified CM.
   c. Manually move users. For more information, see *Move Users*.
6. Push manually created and LDAP-synchronized users to Unified CM. For more information, see *Manual User Push to Cisco Unified CM*.

7. Manage subscribers (see under *Add Subscribers*):
    a. Configure a Phone with a Line.
    b. Associate a Phone to a Subscriber.
    c. (Optional) Change the Class of Service for the Subscriber from the Class of Service set in the Site Defaults. For more information, see *Configure Class of Service*.
8. (Optional) Associate voice mail to a subscriber (see under *Add Subscribers*):
    a. Associate the Voice Mail Service to a Subscriber.
    b. Associate a Voice Mail Profile to a Line.
    c. Enable Call Forward to Voice Mail.
    d. Reset a Phone.
9. (Optional) Associate the Extension Mobility Service to a subscriber (see under: *Add Subscribers*):
    a. Add Login/Logout Service on Unified CM.
    b. Import UC Services and Service Profiles.
    c. Subscribe the Login/Logout Service to a Phone.
    d. Associate the Extension Mobility Service to a Subscriber.
10. (Optional) Configure conferencing. For more information (see *Conferencing: Overview* and *Add Subscribers*).
11. Configure Single Number Reach for a Subscriber (see under: *Add Subscribers*).
12. Associate a Service Profile to a Subscriber and Enable IM and Presence.

14.3. General User Management Tasks

14.3.1. User Management Overview

Users are added to VOSS-4-UC from these potential sources:

- Synchronized from LDAP
- Synchronized from Cisco Unified Communications Manager
- Bulk loader template
- Manually created

Typically, users are associated with a site. You can create move filters to automatically assign users to sites when they are synchronized from LDAP or Unified CM. Bulk loaded and manually created users can be moved using filters or by individually selecting users.

There are two categories of users, local administrators and end users. The local administrators can be assigned to any of the hierarchy nodes (provider, customer, site). End users can only be assigned at the site level.

If an Identity Provider server is deployed at a hierarchy node above the site, you can configure VOSS-4-UC to provide Single Sign-On support for users created or synchronized at that hierarchy node.

Conflicts between users synchronized from different sources are handled according to the strategy described in *Managing Duplicate Usernames*. For information about user password management, depending on the source of the user, see Password Management.

Users associated with a site can be pushed to the Unified CM that appears in the Network Device List assigned to that site. Once pushed to Unified CM, users become subscribers that can be provisioned with various collaboration services.

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

14.3.2. Create and Update a User

Use this procedure to manually create a user.

Procedure

1. Log in as the administrator at the hierarchy node where you want to create the user.
2. Choose **User Management > Users**.
3. Click **Add**.
4. At a minimum, complete the following fields:

Fields	Description
Username	Sign-in username. This field is mandatory.
Entitlement Profile	Choose the entitlement profile that specifies which devices and services the user is entitled to.
Role	Choose the user's role. This field is mandatory.
Language	Choose the user's language. Note: If no language is selected, the language is inherited from the nearest hierarchy node (at or above the user) that has a default language configured. If no default language is configured anywhere in the hierarchy at or above the user, the user's language is English. Note: If a language is manually set for a user, that language remains unchanged even if the user is moved to a new place in the hierarchy. However, if the language is inherited, then the user's language changes when the user is moved to a hierarchy node that has a different default language.
Surname	User's family name. This field is mandatory.
Email Address	User email address.

5. Click **Save**. The user is created.

Note:

- If SSO is enabled for the hierarchy node where the user is added, the corresponding SSO user is created.

- IdPs are not configured at the site hierarchy node. Therefore, you can enable SSO for a user created at the site level only by performing these steps. Choose **Single Sign On > SSO User**, click **Add**, and choose the IdP that can authenticate the user.

Updating

If the user password is *updated*, user passwords on Unified CM, Unity and WebEx are also updated if these have been provisioned for the user.

Note: Since different UC apps can have different password strictness rules, the update transaction will only succeed if the strictness rules of *all* the UC apps have been met. Otherwise, the update transaction will roll back.

Administrators should therefore choose a password that meets the requirements of all the UC apps.

14.3.3. View Users

Use this procedure to view users at or below any hierarchy node.

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the desired hierarchy node.
3. Choose **User Management > Users**.

   A list of users that exist at or below the selected hierarchy node is displayed. Most fields are self-explanatory, except for the following:

Field	Description
User Type	The following values are possible: **VOSS-4-UC Only** Indicates that the user has been manually created in VOSS-4-UC and has not been synced from LDAP or from Cisco Unified CM. **CUCM Local** Indicates that the user exists on both VOSS-4-UC and Cisco Unified CM, and is not synced from LDAP. The user may have been created first on VOSS-4-UC (top-down) or created on Cisco Unified CM and synced into VOSS-4-UC (bottom-up). **CUCM-LDAP Synced** Indicates the user exists on both VOSS-4-UC and Cisco Unified CM, and has been synced from LDAP into Cisco Unified CM. **VOSS-4-UC-LDAP Synced** Indicates the user has been synced from LDAP into VOSS-4-UC. The user may or may not exist in Cisco Unified CM. **Unknown** Indicates that a model used to determine the User Type cannot be found. See the transaction log for details. **blank** Indicates that the user existed prior to the addition of the User Type field. You can run a user audit to update the value. See below.
Hierarchy	The current hierarchy level of the user. The value reflects any user moves that have occurred. To view the original hierarchy node of a user, see below.

4. Click any user to see additional information about the user.

See also:

- *Audit*
- *Check User Provisioning Status*

14.3.4. Manage Local Administrators and Operators

Default local VOSS-4-UC administrators are created when provider, reseller, customer, and site hierarchy nodes are established. Use this procedure to modify or create more local administrators or operators. Also use this procedure to create administrators for intermediate nodes.

An administrator for a particular hierarchy level can create or modify the administrators and operators at that hierarchy level and any level below. For example, a Customer XYZ administrator can create other Customer XYZ administrators and site administrators for Customer XYZ.

Procedure

1. Log in as an administrator.
2. To create or modify an administrator or operator at a level below your current level, set the hierarchy path at the top of the window. If you have signed in as provider administrator, and want to create a customer administrator, set the hierarchy path to the customer for which you want to create the administrator.
3. Choose **User Management > Local Admins**.

4. At a minimum, complete these fields:

Fields	Description
Username	Sign-in username. This field is mandatory.
Email Address	User email address.
Role	Choose the administrator's role. This field is mandatory. • For a provider, reseller, customer, or site administrator or operator, the available roles are limited to those applicable to the hierarchy level. • For an intermediate node administrator or operator, the available roles are limited to those associated with the nearest non-intermediate node above the intermediate node in the hierarchy.
Password	Set the password. This field is mandatory.
Language	Choose the administrator's language. Note: If no language is chosen, the language is inherited from the nearest hierarchy node (at or above the administrator) that has a default language configured. If no default language is configured anywhere in the hierarchy at or above the administrator, the administrator's language is English.

5. To modify an existing administrator or operator, click the administrator or operator.
   a. Modify the appropriate settings for the administrator or operator.
   b. Click **Save**.

14.3.5. Define a Filter

You can define a filter to easily select multiple users to move according to one or more user attributes.

If you specify multiple attributes, a user matches the filter only if the user matches all of the attributes in the filter. For example, a filter with State=Missouri and City=Kansas City, does not match a user in Kansas City, Kansas.

Procedure

1. Choose **User Management > Manage Filters > Define Filters**.
2. Click **Add**.
3. Click the **Base**, **Extended**, or **Custom** tab to locate the user attribute or attributes you want to filter on. Provide the following information:

Field	Description
Name	Enter a name for the filter. This field is mandatory.
Move To Hierarchy	Choose the target hierarchy node. This field is mandatory.
Move To Role	Choose the role to be assigned to the user after the move. The available roles depend on the target hierarchy node selected. This field is mandatory.
Condition	Choose a condition for at least one of the available filters.
Value	Specify the value to evaluate for the condition. Set this field for at least one of the available filters.

Example: Set the City Filter to Condition=isexactly and Value=Toronto to move users in Toronto to the target hierarchy node and give them the target user role.

4. Click **Save**.

The filter is available to be used to manually move users by choosing **User Management > Move Users**. Filters are automatically applied during LDAP and Cisco Unified Communications Manager user synchronization, if the User Move mode is set to automatic.

14.3.6. Methods for Pushing Users to Cisco Unified CM

When you manage users in VOSS-4-UC, you perform several steps to process the new users introduced into the system from the following sources:

- Synchronization from the LDAP directory
- Synchronization from Cisco Unified Communications Manager
- Manual configuration in VOSS-4-UC

One step is to push the user to the Unified CM assigned to the customer and site where the user was added. You can push the user to Unified CM from VOSS-4-UC in two ways:

- Automatic Push - Enabled or disabled using the **Auto Push to CUCM** check box from **Site Management > Sites**
- Manual Push - Performed from **User Management > Manage Users**

There are various options available in VOSS-4-UC for configuring users with phones, lines, and features. Depending on the option you choose, you can automatically push users to Unified CM.

To determine whether to automatically push users to Unified CM, consider the following guidelines:

- When users are synchronized into VOSS-4-UC from an LDAP server, or the users are configured locally on VOSS-4-UC, and then the **Subscriber Management > Subscribers** menu is used to provision phones, lines, and features for those users, we recommend an automatic user push to Unified CM. It does not matter whether you perform the Subscribers configuration through the GUI, bulk loaders, or API. We recommend automatic user push to Unified CM in all cases.
- When users are configured locally on Unified CM and synchronized into VOSS-4-UC, the users are already on Unified CM, so automatic push to Unified CM is not required.

14.3.7. Automatic User Push to Cisco Unified CM

You can enable Automatic User Push to Cisco Unified Communications Manager by selecting the **Auto Push Users to CUCM** check box on the **Site Management > Sites > Site Details** page. Automatic User Push is cleared (disabled) by default.

Users are automatically pushed to a Unified CM in the following situations:

- When users are moved to a site hierarchy level (either by filters, username, or usernames):
  - If a Network Device List (NDL) is configured on that site and contains a Unified CM, the users are pushed to the Unified CM.
  - If an NDL is configured on that site with no Unified CM, nothing happens.
  - If an NDL is not configured on that site, nothing happens.
- When an NDL is added to a site after the site was created:

  - If the NDL is configured with a Unified CM, the users at the associated site are pushed.
  - If the NDL is not configured with a Unified CM, nothing happens.
- When a Unified CM is added to an NDL:

  If the NDL is associated with a site, the users on that site are pushed to the new Unified CM.
- When a new user is created at the site level:
  - If an NDL is configured on that site and contains a Unified CM, the user is pushed to the Unified CM.
  - If an NDL is configured on that site with no Unified CM, nothing happens.
  - If an NDL is not configured on that site, nothing happens.

14.3.8. Manual User Push to Cisco Unified CM

You can manually push users to Cisco Unified Communications Manager (Unified CM) from hierarchy nodes between customer and site, inclusive.

Note: The following limitations exist when pushing users to Unified CM:

- A user may be pushed to only one Cisco Unified Communications Manager.
- Users with the SelfService role may be pushed only from a site.

For users that have been synchronized from LDAP, you can use **Subscriber Management > Quick Add Subscriber** to push the users to Unified CM, instead of this procedure.

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the hierarchy node where the users are located.
3. Choose **User Management > Manage Users**.
4. Choose **Add or update users to CUCM** from the **Action** drop-down.
5. From the **Network Device List** drop-down, choose a Network Device that contains the target Unified CM server.
6. Click **Users +**, and from the drop-down choose the user to move, repeat until all users are selected. Alternatively, select the **Move All Users** check box.
7. Click **Save** to move the selected users to Unified CM.
8. Verify that the users are in Unified CM:
   a. Choose **User Management > Provisioning Status**.
   b. Verify that the users are assigned to the Unified CM server.
9. Verify that users are available as subscribers. After the users are pushed to Unified CM, they appear as subscribers to be assigned phones, lines, and features.
   a. Choose **Subscriber Management > Subscriber**.
   b. Verify all the pushed users are listed.

c. Click one of the users to display the Subscriber page.

What to Do Next

After users are pushed to Unified CM, you can manage them with subscriber templates.

14.3.9. Automatically Move Users Synchronized from Cisco Unified CM

Use this procedure to automatically move users that were synchronized from Cisco Unified Communications Manager, using previously defined move filters.

Procedure

1. Choose **Device Management > CUCM > Servers**.
2. Click the Cisco Unified Communications Manager server to modify.
3. Click the **Publisher** tab.
4. From the **User Move Mode** drop-down, choose **Automatic**.
5. Click **Save**.

The users are automatically moved based on the previously defined move filters.+

14.3.10. Move Users

You can move users between any hierarchy nodes at or below the hierarchy node where the users were originally created or synced in. A common practice is to move users synced in at a customer hierarchy node to various customer sites.

Note: The following restrictions exist when moving users that have been pushed to Cisco Unified Communications Manager:

- Cisco Unified Communications Manager users can be moved only down the hierarchy.
- An NDL containing the same Cisco Unified Communications Manager that the users were pushed to must be referenced at or below the target hierarchy node.

Important: The following restrictions apply when you move users between sites:

- You cannot move users between customers.
- You can move users only between sites that reference the same NDL.
- You can move users only between sites that have the same type of site dial plan.
- You can move users only between sites that have the same country.

You can choose the users to be moved in the following three ways:

- **Move users by filters** - To choose the users depending on one or more user attributes, for example City or Street

- **Move users by usernames** - To choose multiple users by their usernames
- **Move user by username** - To move an individual user

Note:

- When moving a user for SLC dialplan the lines associated to the agent line and the shared line show warnings in the form of logs.
- The Users at Site level cannot be moved.

When you move users, choose a **Move To Role** from the drop-down for the users that is appropriate for the target hierarchy node.

14.3.11. Moving Users from Customer to Site

Use this procedure to move users from Customer to Site.

When you move users, choose a default role for the users that is appropriate for the target hierarchy node.

1. Log in at the appropriate hierarchy level.
2. Choose **User Management > Move Users**, or **Overbuild > Move Users**.
3. In the **Action** drop-down, choose the move method.
    - If you choose **Move users by filters**:
        a. From the **Move From Hierarchy** drop-down, choose the hierarchy node from which you are moving the user.

        A note appears stating that only users at the hierarchy you chose will be moved.

        b. From the **Available** list, choose one or more Move Filters and click **Select** to move them to the **Selected** list. You can choose filters in a different order to change the order in which they are applied.

        c. Click **Save** to move the filtered users.
    - If you choose **Move users by usernames**:
        a. From the **Move From Hierarchy** drop-down, choose the hierarchy node from which you are moving the users. The **Move To Hierarchy** drop-down appears.

        b. From the **Move To Hierarchy** drop-down, choose the target hierarchy node. The **Move To Role** drop-down appears.

        c. From the **Set Default Role** drop-down, choose the default role for the moved users. This default role will be assigned to the moved users unless valid LDAP Custom Role Mappings have been configured, which take precedence over the default role (see: *Set up LDAP Custom Role Mappings*).

        d. Click **Users +**, and from the drop-down, choose the user to move, repeat for each user you want to move. Alternatively select the **Move All Users** check box to select all the users.

        e. Click **Save** to move the users.
    - If you choose **Move user by username**:
        a. From the **User** drop-down, choose the user to move. The **Move From Hierarchy** drop-down appears displaying the existing hierarchy.

b. From the **Move To Hierarchy** drop-down, choose the target hierarchy node. The **Set Default Role** drop-down appears.

c. From the **Set Default Role** drop-down, choose the default role to assign to the moved user. This default role will be assigned to the moved users unless valid LDAP Custom Role Mappings have been configured, which take precedence over the default role (see: *Set up LDAP Custom Role Mappings*).

d. Click **Save** to move the user.

4. Choose **User Management > Users** to verify that the users are moved to the target hierarchy.

14.3.12. Moving Users from Site to Site

As an administrator, you can move users from one site to another with their assigned devices and services intact. Certain conditions must be met for a site-to-site move to succeed. These conditions differ slightly for users in non-SLC dial plans and users in SLC plans.

Non-SLC Dial Plans

When moving a user with their devices and services between sites with a non-SLC dial plan configured, VOSS-4-UC checks the following conditions:

- The sites are not configured with an SLC dial plan.
- Both sites use the same NDL.
- Both sites are in the same country.
- The SyncTo hierarchy is a parent of both sites.
- The target site data/SiteDefaultsDoc contains the needed default settings (that is, they are not empty nor null).
- The role is valid at the move-to site.

Models and Relations Moved

When a user is moved from one site to another, the following models and relations move with them:

- `relation/HcsUserREL`
- `relation/Voicemail`
- `relation/Subscriber`
- `relation/SparkUser`
- `relation/LineRelation`
- `relation/HcsCucmCcTagREL`
- `data/InternalNumberInventory`

Fields Updated by Destination Site's Defaults

Various fields from the destination site's defaults update the models that are moved, such as (but not limited to):

- Voicemail Pilot Numbers
- Unified CM Device Pool
- Unified CM Location

- Unified CM Region, and others

For the `device/cucm/Line` model, these fields are updated:

- Calling Search Space Name
- Route Partition Name
- Share Line Appearance Css Name

Within `relation/Subscriber`, three models are updated:

- Device Profile
- Remote Destination Profile
- Phones

Each of these models contains a Lines field, which in turn can contain individual lines. In a site-to-site move, the E164 Mask and Route Partition Name fields are updated for each line contained in these models.

In addition, the move updates some fields within these individual models:

- Remote Destination Profile
  - Device Pool Name
  - Route Partition Name within the Line Associations
- Phones
  - Device Pool Name
  - Location Name

Updating these values is also necessary if you want to use the Overbuild feature with your existing Unified CM data in the future.

The following models trigger a warning message when you attempt to move them from one site to another. While VOSS-4-UC does not prevent you from moving these models, it displays a message to notify you of the possible implications of moving them:

- E.164 associations
- Call pickup groups
- Hunt lists

Note: If you use an API for a version prior to VOSS-4-UC 11.5.1, the Move Users function has the previous behavior. Devices and services do not move with a user.

For the procedure to move users between sites, see *Move Users*.

Moving Users Between Non-SLC Sites with a DNR Configured

For moves between non-SLC sites with directory number routing (DNR) configured at *either* site, a warning appears stating that any lines associated to the user being moved may not work correctly unless you take one of the recommended actions provided. See the Advanced Configuration Guide to perform the first recommended action.

SLC Dial Plans

When you move a user between sites with an SLC dial plan configured, the required conditions are the same as with non-SLC plans. The only difference is that no error is triggered when the system check detects an SLC dial plan configuration for the customer.

Note: When user are moved from a dial plan site to a non-dial plan site the users are set to a default CSS.

Models and Relations Moved

When you move a user from one SLC site to another, the models and relations moved are the same as with non-SLC dial plans, with these exceptions:

- When moving relation/Subscriber -> Lines:
  - Lines are disassociated from all phones and the relation.
  - Removing the line from **Subscriber Management > Phones** should remove the primary line from the relation.

These models are **not** handled when moving SLC dial plans, because the line does not move:

- Internal Number Inventory (INI)
- E.164 Association
- E164 Inventory
- Call Pickup Group
- Hunt List

The following models trigger a warning message when you attempt to move them from one site to another. While VOSS-4-UC does not prevent you from moving these models, it displays a message to notify you of the possible implications of moving them:

- Agent line associations
- Lines associated to a subscriber's phones, device profile, or RDP
- Voicemail

14.3.13. Site-to-Site User Move Transaction Log Errors

Transaction log errors occur with a site-to-site user move, if the following conditions are not met:

- Each site is not in the same country.
- Sites must have the same types of dial plans (SLC vs. Non-SLC).
- The target site data/SiteDefaultsDoc contains the needed default settings (that is, they are not empty or null).
- Move is not outside the sync_to_hn.
- Role is valid at move to site.
- UC applications resources are set to false.

Review the transaction log for error messages and actions to resolve the errors.

14.3.14. Check User Provisioning Status

Procedure

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

2. Choose **User Management > Provisioning Status**.
3. This information is displayed for each user that is visible to the administrator:

Field	Description
Username	User's username.
CUCM Server	Cisco Unified Communications Manager to which the user is synced.
LDAP Server	LDAP from which the user is synced.
Synced To	Hierarchy level where the user was originally synced to or created at.
Hierarchy	User's current hierarchy node.

You can sort the table by clicking on the field headings. You can search any field where a magnifying glass appears when the cursor is on the field heading.

14.3.15. Synchronize or Purge LDAP Users

Use this procedure to synchronize or delete (purge) users that were synchronized from an LDAP server.

Procedure

1. Set the hierarchy path to the hierarchy node where the LDAP server is.
2. Choose **User Management > Sync & Purge > LDAP Users**.
3. Complete the following fields:

Field	Description
Remove Log Messages	Select the check box if you want to remove user management logs before synchronizing or purging.
Remove Log Direction	Choose **Local** to remove logs at the hierarchy of the LDAP server. Choose **Down** to remove logs at and below the hierarchy of the LDAP server. This field appears only if the **Remove Log Messages** check box is selected.
LDAP Server *	Choose the Organization Unit of the LDAP Server from which you need to sync or purge the users. This is mandatory field.
LDAP Action *	Choose synchronize or purge. This field is mandatory.

4. Click **Save** to start the action you selected.

14.3.16. Synchronize Users, Lines, and Phones from Cisco Unified CM

Use this procedure to synchronize users, lines, and phones from Cisco Unified Communications Manager (Unified CM).

Note: Synchronizing lines and phones is meant only for self-provisioning and is not intended for a full migration scenario. Only Jabber and desk phones are supported for synchronizing from Unified CM. Single Number Reach and Extension Mobility are not supported in terms of adding to Unified CM first and then synchronizing into VOSS-4-UC.

Use MIF filter to detect the unsynchronized users, and purge them from the affected site. After the users are purged, import the Unified CM once again.

Procedure

1. Set the hierarchy path to the hierarchy node where the Unified CM server is.
2. Choose **User Management > Sync & Purge > CUCM Users, Lines, and Phones**.
3. Complete the following fields.

Field	Description
Remove Log Messages	Select this check box if you want to remove user management logs before synchronizing.
Remove Log Direction	Choose **Local** to remove logs at the hierarchy of the selected Unified CM. Select **Down** to remove logs at and below the hierarchy of the selected Unified CM. This field appears only if the **Remove Log Messages** check box is selected.
Action	Choose synchronize. This field is mandatory.
Cisco Unified CM	Choose the Unified CM server. Data is synchronized from the selected Unified CM. This field is mandatory.

4. Click **Save** to start synchronizing.

14.3.17. Purge a Cisco Unified CM User from VOSS-4-UC Only

If the same user is synced from multiple Unified CMs, it will result in a duplicate user on VOSS-4-UC.

Use this procedure to purge a single Unified CM user from the VOSS-4-UC database only, while leaving it on the associated Unified CM.

Procedure

1. Log in as provider administrator or higher.
2. Set the hierarchy path to the hierarchy node where the Unified CM server is.
3. Choose **User Management > Sync & Purge > Local-Purge CUCM User**.
4. Complete the following fields.

Field	Description
Cisco Unified CM	Choose the Cisco Unified CM from which the user was synced.
User Name	From the **User Name** drop-down list, choose the user you want to delete from VOSS-4-UC.

5. Click **Save** to purge the selected user from VOSS-4-UC. Note that the user will remain on the associated Unified CM.

14.3.18. Convert User Type CUCM-LDAP to CUCM Local

This tool is used to convert a CUCM-LDAP user account to a CUCM Local User. If the user exists on CUCxn Server then the user is also converted to a Local User, that is, the user on CUCxn is set to “Do not Integrate with LDAP Directory”.

Converting a user from CUCM-LDAP to CUCM Local is typically required when the user has been deleted from the LDAP Server, the Unified CM has synced with the LDAP Server, and the user has been set to “Inactive”. In this scenario, the user would be deleted when the Garbage Collection process runs on the Unified CM.

Converting the user to a CUCM Local user prevents the user from being automatically deleted.

- Only users with CUCM-LDAP type are shown by default in the **User to Convert** drop-down.
- If the **Show Inactive LDAP Users Only** check box is selected, the list of users is filtered to only show the “CUCM-LDAP” users with a status of “Inactive”, i.e. status value = 2.

  An Inactive User on CUCM is a user that was deleted from the LDAP Server, and CUCM synced with the LDAP server after the deletion took place. Inactive Users will be deleted from CUCM when the Garbage Collector next runs on CUCM.
- Password. The password entered here will be used to set the password for the user on CUCM and CUCxn.

Informational fields show:

- Current User Hierarchy
- LDAP Directory Name
- Current User Status:
  - Active (1): the user is still in LDAP since the last sync
  - Inactive (2): the user is not in LDAP since the last sync

14.3.19. LDAP Sync Actions

LDAP Sync Action enables you to perform bulk syncing for users from multiple Organization Units (OU) of any LDAP server.

Note: It also allows you to select the required OUs of a single LDAP server, and perform the users sync only from the selected OUs.

---

1. Log in as a provider, reseller, or customer administrator.
2. Choose **Device Management > Advanced > LDAP Sync Actions**.
3. Choose the required sync action from **Action** drop-down list.
   - Choose **Import** for bulk syncing of users from multiple Organization Units.
   - Choose **EnableScheduleSync** to enable syncing for already LDAP scheduled job.
   - Choose **DisableScheduleSync** to disable syncing for already LDAP scheduled job.
4. Choose the required LDAP Server from the **Available** area, and click **Select**. The selected LDAP Server appears in the **Selected** area.

5. Click **Save**.
6. Click **Move Up** or **Move Down** to alter the order of user syncing action for LDAP Server.

14.3.20. Managing Duplicate Usernames

Users are created in a synchronization with LDAP or Cisco Unified CM, or they are created manually in the VOSS-4-UC. All users are created according to these duplicate username guidelines:

- The username of a user cannot be updated if another user in the current hierarchy has the same username. This restriction includes above, below, or at the same level in the current hierarchy.
- A user cannot be added if another user that is above, or was originally above before being moved, in the current hierarchy has the same username.
- A user cannot be manually added if another user that is at the same level or below in the current hierarchy has the same username.
- You cannot convert a user to a Subscriber / Unified CM user if another user at the same level or below the Unified CM in the current hierarchy has the same username.
- A user may or may not be synchronized from LDAP or Unified CM if another user at the same level or below in the current hierarchy has the same username. This condition depends on the source of the existing user as shown in these tables:

Note: The restriction on unique usernames in a hierarchy also applies to administrator users.

Users Created in an LDAP Synchronization

Original source of the existing user	Action
LDAP	Simple user update, if the user is coming from the same LDAP server
Cisco Unified CM	Update user, update provisioning status with LDAP server and SyncTo info
Manually created	Update user, update provisioning status with LDAP server and SyncTo info

Users Created in a Cisco Unified CM Synchronization

Original source of the existing user	Action
LDAP	User is not synchronized
Cisco Unified CM	Simple user update, if the user is coming from the same Cisco Unified CM server
Manually created	Update user, update provisioning status and SyncTo info with Unified CM server

The table below refers to Subscribers created in VOSS-4-UC using:

- User Management > Manage Users
- Subscriber Management > Subscribers
- Subscriber Management > Quick Add Subscriber
- Auto Push feature on Site

Quick Add Subscriber and Subscriber Management create Subscribers and users, while Manage Users and the Auto Push feature convert existing users into Subscribers.

Users Created in VOSS-4-UC and Pushed to Cisco Unified CM

Original source of the existing user	Action
LDAP	Update user, update provisioning status with Unified CM server (keep SyncTo info the same)
Cisco Unified CM	No action or updates are necessary
Manually created	Update user, update provisioning status with Unified CM server and update SyncTo to the Cisco Unified CM hierarchy if the current SyncTo is below it

Note:

- If a user cannot be created or updated during an LDAP or Unified CM synchronization, a log is created in User Management > Log Messages and the synchronization succeeds. If a user cannot be created or updated manually, an error message is generated.
- If the duplicate user check fails, the transaction fails, and the user is not converted to a Subscriber.
- If a user's SyncTo value is updated, SSO User updates can result. The SSO User's IDP is set to the IDP configured at the new SyncTo hierarchy node. If no IDP is configured at the new SyncTo hierarchy node, the SSO User is deleted, if it existed. If an IDP is configured at the new SyncTo hierarchy node, but no SSO User exists, an SSO User is created at the user's hierarchy node.
- An update is blocked if two duplicate users are from the same source but originate from different servers.

14.3.21. Audit

Use this procedure to audit user data for SyncTo, User Type, LDAP and CUCM Audit, and Subscriber at the selected hierarchy node. The following checks and corrections are performed:

1. Check for duplicate usernames. Warning messages are logged in **User Management > Log Messages**. For more information about duplicate usernames, see *Managing Duplicate Usernames*.
2. Check SyncTo settings. If the SyncTo setting is incorrect and the user is not a duplicate, the SyncTo setting is updated.
3. Check SSO User settings. If the SSO User setting is not correct based on the SyncTo setting and the user is not a duplicate, the SSO User is updated.
4. Check User Type settings. If the User Type is incorrect, it will be updated.

Provisioning Status (CUCM, LDAP and SyncTo)

Use this procedure to identify if the right SyncTo value is set for a given user, and to identify scenarios where the user provisioning status has invalid values.

1. Log in as a provider, reseller, or customer administrator.
2. Choose **Audit > Audit User Data**.
3. Choose a Hierarchy node.

   We recommended to run at Site hierarchy for a better performance.
4. In the **Provisioning Status (CUCM, LDAP and SyncTo)** area, from the **Options** drop-down, choose either Off, Report Only or Report & Fix.
5. Select the **Log to Transactions Only** check box to get audit data only in transaction logs not as Audit Report.
6. Click **Save**.

User Type

Use this procedure to identify if the right user type is set for a given user and fix if required.

1. Log in as a provider, reseller, or customer administrator.
2. Choose **Audit > Audit User Data**.
3. Choose a Hierarchy node.

   We recommended to run at Site hierarchy for a better performance.
4. In the **User Type** area, from the **Options** drop-down, choose either Off, Report Only or Report & Fix.
5. Select the **Log to Transactions Only** check box to get audit data only in transaction logs not as Audit Report.
6. Click **Save**.

Subscriber

Use this procedure to get report to identify scenarios where the subscriber is found with no corresponding user.

1. Log in as a provider, reseller, or customer administrator.
2. Choose **Audit > Audit User Data**
3. Choose a Hierarchy node.

   We recommended to run at Site hierarchy for a better performance.
4. In the **Subscriber** area, from the **Options** drop-down, choose either Off, Report Only or Report & Fix.
5. Select the **Log to Transactions Only** check box to get audit data only in transaction logs not as Audit Report.
6. Click **Save**.

Audit Report

If you have not selected the **Log to Transactions Only** check box, then the Audit Report gets created per user basis if there is any discrepancy.

You can view the reports under **Audit > Audit Report**.

You can also export the report to `.xls` and `.json` format.

Choose **Administration Tools > Transaction** to view the transaction log. Click the **Hcs Audit User Sync To View** transaction to open it. For example, the message indicates:

- The number of users found at or below the hierarchy node.
- The number of duplicate users detected.
- The number of SyncTo corrections made.
- The number of SSO User corrections made.

14.3.22. Assign a Credential Policy to a User

In general, a user inherits a credential policy from the nearest hierarchy node at or above the user's location that has a default credential policy set. However, you can explicitly assign a credential policy to a user.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **User Management > Users**.
3. Click the user that you want to assign a credential policy to.
4. Click the **Account Information** tab.
5. From the **Credential Policy** drop-down, choose a credential policy to assign.

   The menu contains all the credential policies available at or above the user's node in the hierarchy.
6. Click **Save**.

Note: If a user is signed in when the credential policy is changed, changes are not applied until the user signs out and signs in again.

14.3.23. Assign a Credential Policy to an Administrator

In general, an administrator will inherit a credential policy from the nearest hierarchy node at or above the administrator's location that has a default credential policy set. However, you can explicitly assign a credential policy to an administrator.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **User Management > Local Admins**.

3. Click the administrator that you want to assign a credential policy to.
4. Click the **Account Information** tab.
5. From the **Credential Policy** drop-down, choose a credential policy to assign.

   The menu contains all the credential policies available at or above the administrator's node in the hierarchy.
6. Click **Save**.

Note: If an administrator is already logged on when the credential policy is changed, changes do not take effect until the administrator logs out and logs on again.

14.3.24. Unlock a Locked Out User

If a user is locked out on account of a credential policy violation, an administrator responsible for the user can unlock the user's account.

Procedure

1. Log in as provider, reseller, or customer admin.
2. Choose **User Management > Users**.
3. Click the user whose account you want to unlock.
4. Click the **Account Information** tab.
5. Clear the **Locked** check box.
6. Click **Save**.

14.3.25. Unlock a Locked Out Administrator

If an administrator is locked out on account of a credential policy violation, an administrator at a hierarchy node above the locked out administrator can unlock the administrator's account.

Procedure

1. Log in as provider, reseller, or customer admin, depending on the location of the locked out administrator.
2. Choose **User Management > Local Admins**.
3. Click the administrator whose account you want to unlock.
4. Click the **Account Information** tab.
5. Clear the **Locked** check box.
6. Click **Save**.

14.3.26. Manually Disable User Account

Usually, a user account is disabled when the password has expired. However, an administrator can manually disable a user account at any time.

Note: Manually disabling a user is preferred to manually locking out a user as you can provide the reason for disabling.

Procedure

1. Log in as provider, reseller, or customer admin.
2. Choose **User Management > Users**.
3. Click the user whose account you want to disable.
4. Click the **Account Information** tab.
5. Select the **Disabled** check box.
6. Enter the reason the account is disabled in the **Reason for Disabled** field. This reason will be displayed to the user when the next login attempt fails.
7. Click **Save**.

14.3.27. Manually Disable Administrator Account

Usually, an administrator account is disabled when the password has expired. However, an administrator at a higher hierarchy level can manually disable an administrator account at any time.

Note: Manually disabling an administrator is preferred to manually locking out an administrator as you can provide the reason for disabling.

Procedure

1. Log in as provider, reseller, or customer admin.
2. Choose **User Management > Local Admins**.
3. Click the administrator whose account you want to disable.
4. Click the **Account Information** tab.
5. Select the **Disabled** check box.
6. Enter the reason the account is disabled in the **Reason for Disabled** field. This reason will be displayed to the administrator when the next login attempt fails.
7. Click **Save**.

14.4. Password Management

14.4.1. Password Management: Overview

The following sections describe the various ways passwords are set by default and can be configured between LDAP, Voss-4-UC and Cisco Unified Communications Manager.

14.4.2. Users Synchronized from LDAP to VOSS-4-UC

When users are synchronized top-down from LDAP into VOSS-4-UC, LDAP authentication is enabled by default in VOSS-4-UC for these users. When LDAP users are pushed to Unified CM and Cisco Unity Connection, authentication is either LDAP or local authentication, depending on how the applications are configured. If LDAP authentication is not configured in Unified CM or Cisco Unity Connection, the user is considered to be a local user in UC applications.

14.4.3. User Synchronized from LDAP to VOSS-4-UC (SSO Enabled)

Passwords are defined and enforced at the Identity Provider when the user is synchronized from LDAP to VOSS-4-UC with SSO enabled.

14.4.4. Users Synchronized from LDAP to Cisco Unified Communications Manager

When a user is synchronized from LDAP to Cisco Unified Communications Manager (Unified CM), the password is not synchronized like other user information that is pulled from LDAP. If LDAP Authentication is enabled, the password in the LDAP Server is used unless the password was changed locally in Unified CM, forcing the Unified CM password to be used. However, if LDAP Authentication is not enabled, the default password is whatever was configured in Unified CM as the default. If no default password is defined, then configure a password manually.

14.4.5. Users Synchronized to VOSS-4-UC

Passwords are not transferred when users are synchronized from Cisco Unified Communications Manager (Unified CM) to VOSS-4-UC. An administrator must configure the passwords before the accounts can be used.

The following Unified CM users are affected: users that were manually added to Unified CM and users that were synchronized from LDAP.

14.4.6. User Added Manually Through Subscriber Management

A user that is added through Subscriber Management has the same password that was configured in VOSS-4-UC when the subscriber was provisioned.

14.4.7. User Added Manually Through User Management

A user that is added through User Management has the local VOSS-4-UC password that was specified when the user was created. When this type of user is pushed to Cisco Unified Communications Manager (Unified CM), the password is not pushed. Instead the password can be configured in one of the following ways:

Create a Default Password with Unified CM

1. Log in to Unified CM as an administrator.
2. Choose **User Management > User Settings > Credential Policy Default**.
3. Choose the line item that has the Credential User to 'End User' and Credential Type to 'Password'.
4. Enter the default password in the confirmation box and click **Save**.

Note: Make sure that the user has the correct role defined.

Set the Password in the CUCM End User Page

1. Log in to Unified CM as an administrator.
2. Choose **User Management > End User**.
3. Filter for the user you wish to modify.
4. Change password fields for the specified user.

14.4.8. Force User Password Change

You can use a credential policy to force users to change their passwords on initial login. However, an administrator can manually force a user password change on the next login attempt.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **User Management > Users**.
3. Click the user whose password you want to be changed on the next login attempt.
4. Click the **Account Information** tab.
5. Select the **Change Password on Next Login** check box.
6. Click **Save**.

When the user next attempts to login, the user will be prompted to change the password. Once the password is changed the Change Password on Next Login check box is cleared.

14.4.9. Force Administrator Password Change

You can use a credential policy to force administrators to change their passwords on initial login. However, an administrator at a higher hierarchy level can manually force an administrator to change password on the next login attempt.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Choose **User Management > Local Admins**.
3. Click the administrator whose password you want to be changed on the next login attempt.
4. Click the **Account Information** tab.
5. Select the **Change Password on Next Login** check box.
6. Click **Save**.

When the administrator next attempts to login, the administrator will be prompted to change the password. Once the password is changed the Change Password on Next Login check box is cleared.

14.4.10. Manage Your Own Account Password

Logged in users or administrators can manage their own account passwords.

Note:

Users who are configured for Single Sign On or through LDAP do not manage their account passwords in VOSS-4-UC.

14.4.11. Change Your Own Password

Change your own password if required as follows:

1. Log in to VOSS-4-UC.
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the **Change Password** option from the drop-down menu. The **Change Password** screen is displayed.
4. Enter your existing password in the **Old Password** field.
5. Enter your new password in the **New Password** field. Refer to **Minimum Password Length** and **Enable Password Complexity Validation** fields under *Deploy a Customized Credential Policy* if required.
6. Confirm your new password by re-entering it in the **Repeat New Password** field.
7. Click **Change Password** in the button bar. Your password is changed.

14.4.12. Reset Your Password

You can only reset your password if you have already provided answers to the security questions created by your administrator. See “Configure Your Password Reset Questions” if required.

If you forget your password while attempting to log in to VOSS-4-UC:

1. Enter your username in the **Username** field on the Log in screen.
2. Click the **Forgot Password?** hyperlink located below the **Log in** button.
3. Enter your username again.
4. Click **Reset my password**.
5. Click in each security question field and type the correct answer.
6. Click in the **New password** field and type your new password. Refer to **Minimum Password Length** and **Enable Password Complexity Validation** fields under *Deploy a Customized Credential Policy* if required.
7. Click in the **Repeat password** field and re-type your new password.
8. Click **Reset my password**. Your password is changed.
9. Click the **Login** hyperlink if you want to attempt to log in again.

14.4.13. Configure Your Own Password Reset Questions

Use this procedure to configure your password reset questions:

Note: Configuring your own password reset questions is available only if the credential policy applied to your user account has Number of Questions Asked During Password Reset set to > 0.

Procedure

1. Log in to VOSS-4-UC.
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the **Password Reset Questions** option from the drop-down menu. The **Password Reset Questions** screen is displayed.
4. Type your password in the **Current Password** field.
5. Choose the required security question from the **Question** drop-down list.
6. Enter your answer to the above question in the **Answer** field. All answers should differ from each other.
7. Repeat steps 5 and 6 until you have configured the required amount of security questions (as determined by your administrator).
8. Click the **Update Security Questions** button in the button bar when complete. Your security questions and answers are updated.

14.5. Role Management

14.5.1. Support for Privacy and Security Notices

VOSS-4-UC allows for the configuration of appropriate login security warnings as well as links to cookie and privacy policies for best practice and compliance with regulatory requirements such as General Data Protection Regulation (GDPR).

Support is available on the login screen as well as menus of both the administrator interface and the Self-service application.

- Pop-up login banner

  A pop-up banner can be configured for the purpose of security notices or user agreements on the login page after users enter their credentials and when they click the **Login** button on either the administrator interface or Self-service application. Clicking either the **Agree** or **Cancel** buttons remove this pop-up banner.

  For details on configuration, refer to *Login Banner*.

- Privacy and Cookie Policy notices

  When drafting cookie policy notices, VOSS-4-UC provides reference content - see: *VOSS-4-UC Cookie Policy*

  - Login screens: As a part of Theme management, Privacy and Cookie Policy notices can be added on the login interface of both the administrator and Self-service login screens.

    For configuration details , refer to : *Set the Login Page Theme*.

    The style of the banner can also be customized. Refer to “Theme Banner Customization” in the “Advanced Configuration Guide”.

  - Menu items: High level system administrators above the Provider level hierarchy can manage privacy policy references that are available on administrator and Self-service user menus.

    For details, refer to *Privacy Policy Menu Items* and *Manage Privacy Policy Menu Items*.

14.5.2. Role Based Access

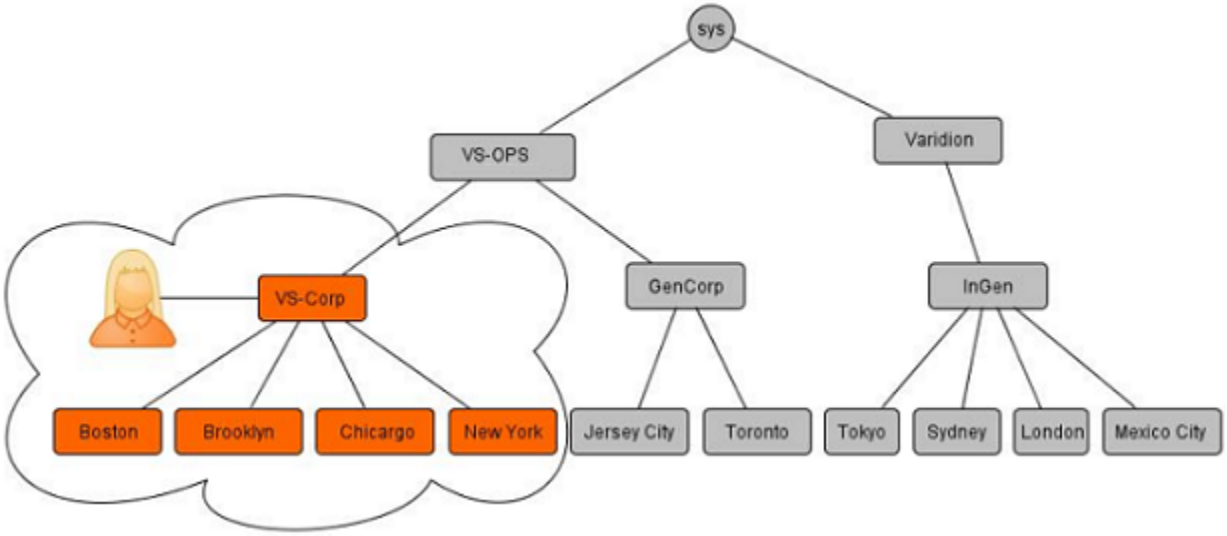
The system implements role-based access control by means of the following components:

- Hierarchy
- User Role

All users that are added to the the system are added at a hierarchy level. Such a user then only has visibility of, and access to, system resources that are available to users at that hierarchy level.

On the interface, this means that the user has no visibility of nodes outside of the sub-tree starting at the parent hierarchy. The user may change to a level of the hierarchy below the the parent hierarchy.

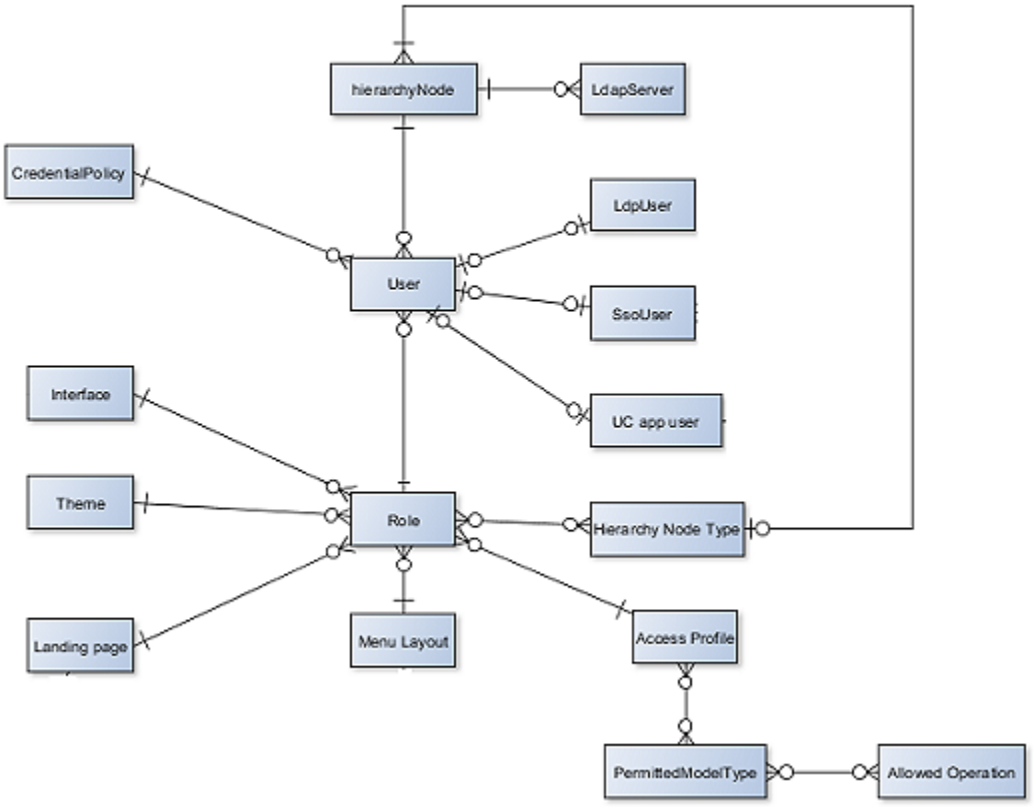
The following diagram shows that a user at VS-Corp has no visibility of GenCorp and InGen.



From the context of the hierarchy level that a user was created at, role-based access is implemented. When users are added to the system at a hierarchy level, a User Role can be assigned to them.

The User Role is a combination of:

- The rules that apply to the role. In particular, the hierarchy types that apply to the role. This means that the role is only available to a user at a hierarchy level that belongs to a hierarchy type associated with the role. For example, a Site Administrator role may have a rule that associates it with Site and Building hierarchy types, but not Customer hierarchy types. In this way a Site Administrator role cannot be associated with a user created at a Customer hierarchy level. A hierarchy rule is therefore enforced by the role.
- System permissions to resources from that hierarchy.
- Access Profiles associated with a User Role that determine access specific operations supported by different models and/or on miscellaneous permissions.
- The visibility of resource attributes.
- The look and feel of the interface.
- Default values of resource attributes.



14.5.3. User Roles

A User Role in the system combines the look and feel of the system interface with a number of default permissions and values. Refer to the diagram in *Role Based Access*. A specific User Role is a combination of:

- Landing Page - The appearance of and links on the first page after login.
- Menu Layout - The menu layout associated with a user role not only determines the menu that is available, but where relevant includes the Configuration Templates and the Field Display Policies that apply to the resource that is linked to from the menu.
- Theme - The appearance of the user interface can be associated with a role.
- Access Profile - Permissions for resources are defined in Access Profiles. An Access Profile can be associated with a User Role.
- Interface - Determines which application interface the role definition applies to. Administration and Self-Care are the two interfaces supported by roles today.

When a user is created or updated, a User Role can be selected for the user. This user will have the landing page, menu, theme and interface specified by the User Role. For example, the Configuration Template defaults and settings as well as Field Display Policy views of the menu associated with the role apply.

A User Role can be assigned to more than one user. The user hierarchy and role serve as components of role-based access control in the system.

A number of user roles are provided:

- Default-Global Admin
- Default-Provider Admin
- Default-Customer Admin
- Default-Site Admin

Each of these roles have a relevant landing page, menu layout and access profile. These elements as well as the theme can be customized.

Note: Users cannot modify their own User Role or the associated Access Profile, Menu Layout, Landing Page or any of the Configuration Templates or Field Display Policies associated with the Role.

Finally, user roles are subject to specific user role rules. This means that a particular user role may be tied to a specific Hierarchy type. For example, a Site Admin role may only be assigned to users who reside at a Site hierarchy level.

14.5.4. Role Management

Provider administrators can manage the roles that are available for administrators, operators, and users at lower levels in the hierarchy.

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

Procedure

1. Log in as provider administrator.
2. Choose **Role Management > Roles**.
3. To add a role, click **Add**.
4. Enter or select the following role settings:

Setting	Description
Name*	Name of the role. This field is mandatory.
Hcs Component Access*	Controls which HCM-F components (FF or SA) that users with this role have access to. Used with **Hierarchy Type** and **Service Assurance Role Type** when mapping roles to HCM-F. This field is mandatory.
Service Assurance Role Type*	Controls read/write access to HCM-F components. Used with **Hierarchy Type** and **Hcs Component Access** when mapping roles to HCM-F. This field is mandatory.
Hierarchy Type*	The type of hierarchy nodes applicable at the selected hierarchy level. For example, at Provider level, the following values are allowed: Provider, Reseller, Customer, and Site. While at the Reseller level, the following values are allowed: Reseller, Customer, Site. Controls which roles are available at which levels in the hierarchy. Also used with **Hcs Component Access** and **Service Assurance Role Type** when mapping roles to HCM-F. This field is mandatory.
Description	Description of the role.
Access Profile*	Permissions for resources are defined in Access Profiles. This field is mandatory.
Menu Layout	The menu layout assigned to the role. Controls the menu options available to users assigned to the role.
Landing Page	The home page assigned with the role. Controls what the home page looks like for users assigned to the role.
Theme*	The name of the theme assigned to the role. The theme controls the overall look and feel of the GUI. This field is mandatory.
Self Service Feature Display Policy	The selected Self Service Feature Display Policy that is associated to the role.
Self Service Links	Provide useful links to Self Service end users.
Custom Interfaces	Add Interface Types and Names for the role. The available Interface Type is InterfaceBusinessAdminPortal that adds access to the Business Admin Portal to the role. The available Business Admin Portal type names are added by a system level administrator.

For Custom Interfaces, see: *Business Admin Portal Custom Interface*.

5. Click **Save** to save the role.
6. To modify an existing role, click the role. Change the role settings as needed and click **Save**.

14.5.5. Clone a Role

Use this procedure to clone an existing role for a specific hierarchy node (provider, reseller, customer, or site).

Procedure

1. Log in as hcsadmin or provider administrator.

   Note:

   Administrators can clone roles associated with, or below, their level in the navigation hierarchy.

2. Choose **Role Management > Roles**.
3. Click the role that you want to clone.
4. Choose **Action > Clone**.
5. Enter a unique name for the role in the **Role** field. Make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).
6. (Optional) Add a description for the role in the **Description** field.
7. Click **Save** to save the role to the hierarchy that appears in the breadcrumb.

14.5.6. Create a Service Assurance Only Role

To restrict an administrator to performing only service assurance tasks, you need to create the appropriate service assurance only role.

Procedure

1. Log in as hcsadmin or provider administrator.
2. Chose **Role Management > Roles**.
3. Click **Add**.
4. Enter a name, and optionally a description, for the role.
5. Select the hierarchy type for the role.

   Controls the hierarchy level that the role is available at.
6. From the **Hcs Component Access** drop-down, choose **Service Assurance Only**. The privileges, menu layout, and landing page values are automatically set to the appropriate values for a service assurance only role and cannot be overridden.
7. Optionally, select a theme for the role.
8. Click **Save**.

14.5.7. Create a Fulfillment Only Role

To restrict an administrator to performing only fulfillment tasks, you need to create the appropriate fulfillment only role.

Procedure

1. Log in as hcsadmin or provider administrator.
2. Choose **Role Management > Roles**.
3. Click **Add**.
4. Enter a name, and optionally a description, for the role.

5. Select the hierarchy type for the role.

   Controls the hierarchy level that the role is available at.
6. From the **Hcs Component Access** drop-down, choose **Fulfillment Only**.
7. Choose the privileges for the role.
8. Optionally, select a menu layout, landing page, and theme for the role.
9. Click **Save**.

14.5.8. Create a Custom Self-Service Role

A default Self-Service feature display policy is available in VOSS-4-UC. When providers, resellers, customers, and sites are added in VOSS-4-UC, the default Self-Service feature display policy is assigned automatically to the Self-Service role at each level of the hierarchy. The default Self-Service feature display policy allows you to perform the following tasks in the Self-Service interface:

- Add Voicemail
- Enable Remote Destination Profile (RDP)
- Manage phones and phone lines (but adding smart devices is not allowed)
- Assign configuration templates for phones, RDP, and voicemail
- Link to Launch Webex from Self-Service interface

Most options are set to **Show**, rather than **Hide** to indicate that the Self-Service user can view and edit the item in the Self-Service interface. For example, My Availability, Speed Dials, Call Forward Basic, Advanced Call Forwarding, Ring Schedules, Advanced Timer options, Password, and PIN are all set to **Show**.

Perform this procedure to modify the default Self-Service feature display policy, create a custom Self-Service role, and assign the custom Self-Service role to users.

Procedure

1. Log in as hcsadmin or provider administrator.
2. Clone the default feature display policy:
   a. Choose **Customizations > Self Service Feature Display Policy**.
   b. Choose the Default Self-Service feature display policy. The Self Service Feature Display Policy (Default) screen opens.
   c. Click **Action > Clone**.
   d. On the **Base** tab, type a new name for the Self-Service feature display policy in the **Name** field.
   e. Change options on the **Base**, **Phones**, **Personal Phones**, **My Information**, **Voicemail**, or **Call Forward** tabs as required:

      On the **Phones**, **Personal Phones** and **Voicemail** tabs, there are two similar check boxes (one associated with entitlement, the other not). For example, on the **Voicemail** tab, the first check box is labeled **User can enable Voicemail (Add a Voicemail Account)** and the second check box is labeled **User can enable Voicemail only if the user is entitled to Voicemail**.

      If the Entitlement Feature is used, that is an Entitlement Profile is associated to the subscriber on the **Entitlement Profile** drop-down on the **Subscriber Management > Subscribers** screen,

then choose the second check box. If an Entitlement Profile is not associated to the subscriber, then select the first check box, as the second check box is no longer applicable.

Similarly, select the appropriate check boxes on the **Phones** and **Personal Phones** tabs.

To	Do
Allow users to add their own smart devices	On the **Phones** tab, select the **User can add own smart devices** check box.
Add more phones or devices from Cisco Unified Communications Manager	On the **Phones** tab, complete information to add the phones or devices to the **Device Configuration Templates for User** area of the screen.
Change the Default RDP configuration template	On the **Personal Phones** tab, choose a different template from the **Device Configuration Template for End-User Remote Destination Profile Add** drop-down menu.
Change the Default Voicemail configuration templates	On the **Voicemail** tab, choose different templates from the drop-down menus.
Show/hide individual Voicemail options such as Voicemail Basic, Voicemail Devices, Phone Notification Device, Voicemail Alternative Extensions	On the **Voicemail** tab, choose **Show** from the specific drop-down menus.
Show WebEx link in the Self-Service interface	On the **My Information** tab, choose **Show** from the **Link to Webex self service portal** drop-down menu. Note: The WebEx link (Protocol, Address, Port, and Site Name) must be defined in **Device Management > WebEx > Servers** and the subscriber must have access to WebEx on the **WebEx** tab (**Subscriber Management > Subscribers**). Ensure that when you expand the WebEx user form, the **Enable CET** and **Enable PMR** check boxes under **Privilege** are selected.
Hide Self-Service options from users	Choose **Hide** from the appropriate drop-down menus.

f. Click **Save**. The custom Self-Service feature display policy appears in the list and can be assigned to Self-Service roles.

3. Assign the custom Self-Service feature display policy to one or more Self-Service roles.
   a. Choose **Role Management > Roles**.
   b. Choose a provider, reseller, customer, or site level Self-Service role.
   c. From the **Self Service Feature Display Policy** drop-down menu, choose the custom Self-Service feature display policy you created in step 2.
   d. Click **Save**.
   e. If desired, repeat substeps b to d for other Self-Service roles.

4. If a Cisco Unified Communications Manager sync or LDAP sync is not performed, manually assign the custom Self-Service role to one or more existing users.

   Note:

   You do not need to perform this step for new users who are added to the system in the future. New users are automatically assigned the Self-Service role that you specify for the reseller, customer, or site when it is added to the network.

   a. Log in as provider, reseller, or customer administrator.
   b. Choose **User Management > Users**.
   c. Choose the user for whom you want to assign the custom Self-Service role.
   d. From the **Base** tab, choose the custom Self-Service role from the **Role** drop-down menu.
   e. Click **Save**.

14.5.9. Business Admin Portal Custom Interface

The Business Admin Portal Custom Interface that is associated with a user role can be managed from the **Business Admin Portal Profiles** menu by adding instances or cloning and modifying existing instances down to a required hierarchy.

Default Business Admin Portal Profiles

Upon installation, the Business Admin Portal Interface Type provides three profile instances:

- `default`

  This instance is used when creating a role. The name “default” at the user’s hierarchy level or first level upwards is applied.

  The default profile has the following properties:

  – The **Enable Business Admin** checkbox is checked.
  – No access the Business Admin Portal Menus: site management, tools.
  – Only view access to data from other Business Admin Portal Menus, including example model counts and charts.

  The system level administrator can clone the instance down the hierarchy and modify it to create custom default instances of the interface type.

- `Read Only`

  This instance:

  – The **Enable Business Admin** checkbox is checked.
  – has the same properties as the `default` instance
  – is applied to all Operator administrator user roles by default

- `Full Access`

  This instance is a profile with full access to all Business Admin Portal Menus menus and features.

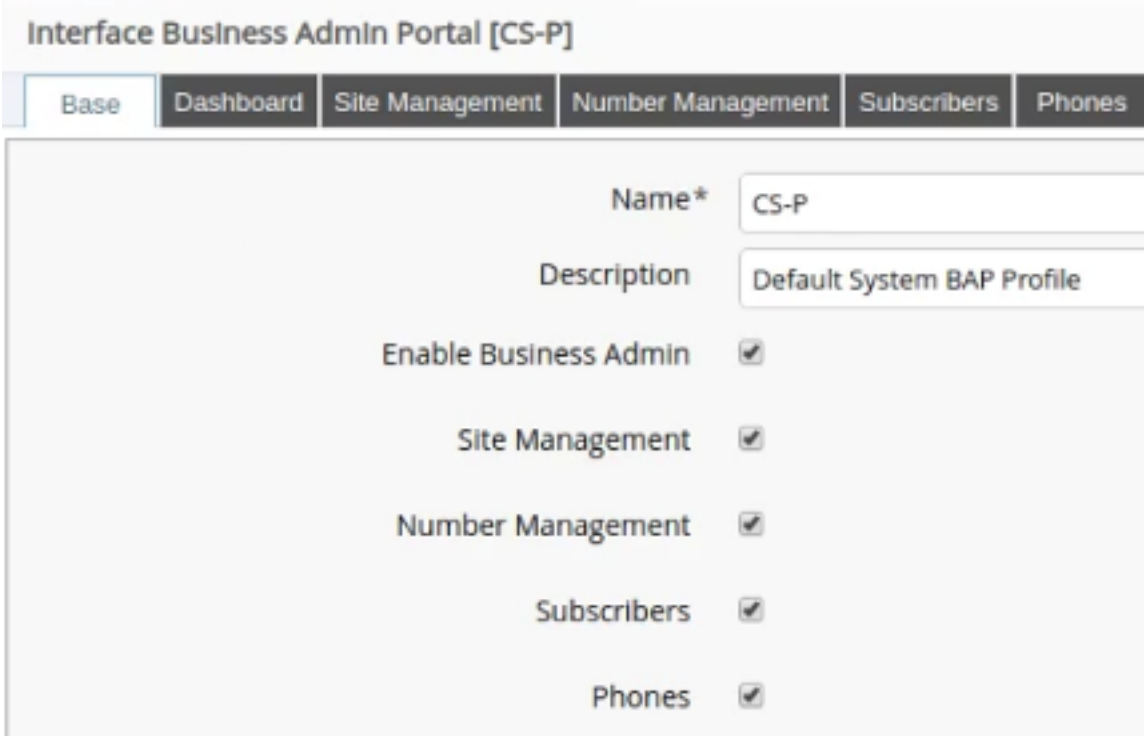
Manage Business Admin Portal Profiles

1. Log in as a system level administrator (above provider level).
2. Choose **Role Management > Business Admin Portal Profiles**.
3. To add a Business Admin Portal Interface Type, click **Add**. The default custom interface can also be cloned to a required hierarchy and modified.
4. Enter or select the following settings:
    1. On the **Base** tab: provide a name and description and select the available menus.
    2. On the **Base** tab: check / uncheck the **Enable Business Admin** checkbox to enable or disable the **Dashboard** tab and feature tabs.
    3. On the **Base** tab: if custom features are needed to be added to the **Quick Actions** card for a Feature Area, use the **Custom Features** list:
        - Choose an **Icon** title. For a list icons corresponding to the titles, see *Business Admin Portal Interface Custom Icon Names Reference*.
        - Enter a title and choose the Feature Area.
        - Similar to Menu Layout configuration options, choose a model type and set up any further configuration associated with the model type. Note that the model type needs to be exposed in a user's Access Profile if the custom interface is associated with a user. Refer to the Custom Feature example image.
    4. On the **Dashboard** tab, move features from the **Available** transfer box to the **Selected** box to enable them on the menu landing page.
    5. On each feature tab, move features from the **Available** transfer box to the **Selected** box to enable them on the feature dashboard.

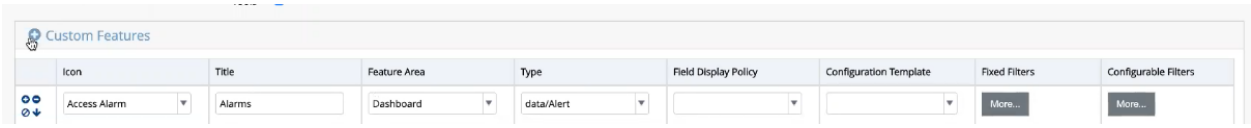
       If no features are selected, the menu item will show, but no features will be available.
    6. On the **Miscellaneous** tab, functionality and display options can be configured for the Business Admin Portal GUI:
        - **Display About Information**: the **Settings > About** menu can be shown or hidden.
        - **Allow Data Export**: if enabled or disabled, the **Export** action is either available or not on list and form pages.
        - **Transaction Log Actions**: for transaction instances and its list view, options are available to enable or disable actions on these; such as Replay and Cancel.
        - **Transaction Log Display Fields**: when viewing a transaction instance, options are available to show or hide selected information on the transaction, such as its logs and sub-transactions.
5. Click **Save** to save the named instance.

The created instance can be selected as a **Name** of the InterfaceBusinessAdminPortal Interface Type by a provider level admin when creating or modifying a user role. See: *Role Management* and *Create a Business Admin Portal Role*.

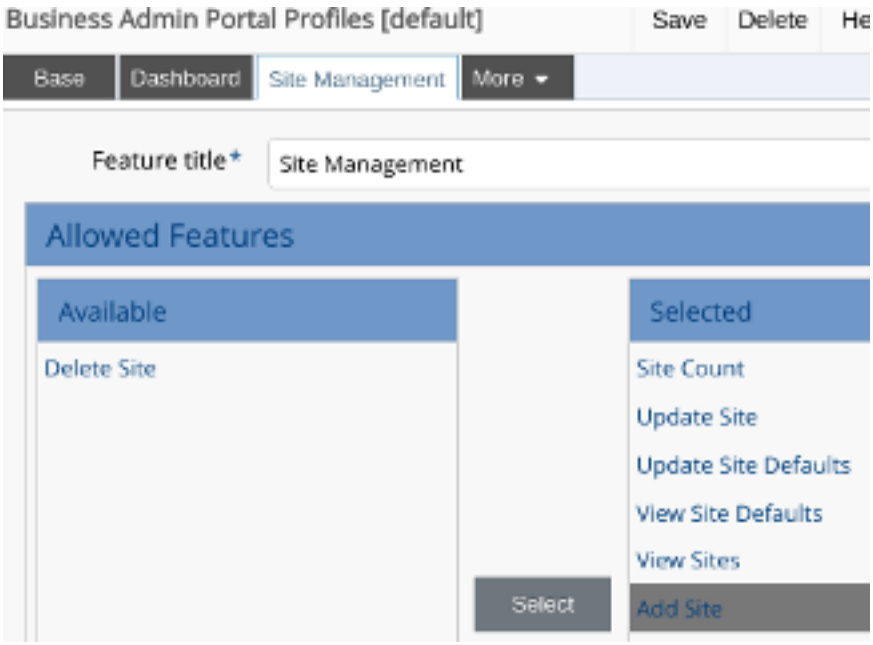
Base tab example:



Custom Feature example:



Feature Transfer boxes example:



14.5.10. Create a Business Admin Portal Role

A role custom interface is available to assign to an administrator user so that the administrator can access the Business Admin Portal. Refer to the “Business Admin Portal” online help or documentation for details on this interface.

Procedure

1. Log in as a provider administrator.
2. Choose **Role Management > Roles** and either choose an existing role to modify or create a new role (refer to “Clone a Role”).
3. Click + next to **Customer Interfaces**, and add an entry to the Custom Interfaces group:
   a. From the **Interface Type** drop-down, choose **InterfaceBusinessAdminPortal**.
   b. From the **Name** drop-down, choose the required interface name. See: *Business Admin Portal Custom Interface*.
4. Click **Save**.

   An administrator with this user role will be able to log in on the Business Admin Portal when appending the following endpoint to the login URL:

   `https://<VOSS-4-UC IP>/business-admin/`

14.5.11. Themes

Themes control the look and feel of the entire GUI interface. This contains all aspects of the presentation including the images, logos, colors, fonts, sizing and positioning. Login and interface header text can also be managed by the VOSS-4-UC theme feature.

Themes can also be managed using the ‘Themes Interface’ in the Business Admin Portal. See “Create a Theme in the Business Admin Portal” in the Business Admin Portal Guide for more details.

New themes can be added and existing themes can be edited. These are associated with a user’s role. There is no limit to the number of themes that can be added and applied. It is a common practice to have a theme associated with a specific customer (company).

The default theme that applies to the GUI when the system is initially built, is available on the VOSS-4-UC system and can be used as the baseline template. The theme is in the form of a Cascading Style Sheet (CSS) to be exported, edited and re-imported as required.

While all aspects of the exported CSS can be modified, we recommend that the default theme is used as a template in terms of basic design in order to prevent usability or functional issues.

The CSS file itself is simple to export and edit. Clear headers in the CSS file indicate which area of the GUI the design applies to. The headers include the following components:

- Navbar
- Shortcut menu
- Hierarchy breadcrumbs
- Quick search
- Tree menu

- Toolbar
- List
- Form

Images can be stored with the theme or referenced with the use of relative path names.

The ability to view themes created at a given hierarchy level can be restricted from users at a lower hierarchy level by use of the **Hide from Lower Hierarchies** check box. If this check box is checked for a particular theme, that theme will no longer be visible on the Themes list view screen at the lower level hierarchy.

The theme feature is applied to either the Administration or Self-Service interface. If no Interface is specified, the new login theme will also have its interface set to Administration.

It also includes a **Use this Theme to style Login page** check box, which when selected, applies the chosen look and feel to the Login page across the system. Currently, the system allows only a single theme to be applied to the Login page per Interface. This means that a new or updated theme with Interface and Login page setting that corresponds to an existing theme, will result in the disabling of the Login page style on an existing theme with the same Interface setting.

The Login page theme can also be applied to the Login page during the log in process by adding a suffix to the login request URL. See *Set the Login Page Theme*.

14.5.12. Theme Field Reference

Base

Theme Name *	name	The name that is given to the Theme.
Use this Theme to style Login page	is_login_theme	Should Login page use this theme? Applies to the relevant theme's login page: either the Self-service or admin.
Site Title	title	The title for the site
Import File *	import_file	
Backup Enabled	backup	Create backup if existing theme exists

Login Page Details

Title	title	Title displayed at top of login page.
Banner text	banner	Banner text displayed at bottom of login page.

14.5.13. Add a Theme

1. Prepare the theme file:
    a. Create a folder and add a file skin.css with the required name of the theme. The name of the folder must be the same as the intended theme name (only alphanumeric characters can be used, with no spaces or special characters).
    b. Add any CSS overrides to the file. Note that only the definitions as shown in the export of a provided CSS file `skin.css` can be modified.
    c. Add required image files in this folder (if any).

d. Create a .zip archive file with the same filename as the folder.

Refer to *Download and Update a Theme* for details.

2. Add the theme to the system:
   a. Choose the hierarchy level at which the theme will be created.
   b. Choose **Role Management > Themes** to open the **Themes** list view.
   c. Click **Add** on the button bar to open the **Themes** input form. Note that themes can only be customized by a Provider Administrator (or higher).
   d. Enter the **Theme Name** (same as the file name created above).
   e. Enter an appropriate **Site Title** if required. The site title entered here is the title displayed in the browser tab.
   f. Click the **Browse** button to import the created theme zip file. Wait until the system displays the file chosen in the **Import File** field.
   g. If the theme must also apply to the login page, select the **Use this Theme to style Login page** check box.
   h. To set login banner text and notices on the login page, refer to *Set the Login Page Theme*. The **Use this Theme to style Login page** check box does not have to be selected for banner text to show.
   i. If you want to hide the theme from lower level hierarchies, select the **Hide from Lower Hierarchies** check box. Users logged in at lower level hierarchies will not be able to see that particular theme on the **Themes** list view screen.
   j. For details on the **Theme Customization** tab controls, refer to *Create a Theme in the Business Admin Portal*. .. note:

```
If any details are added on this tab, *all* fields should be provided with␣
↪input.
```

   k. Click **Save** on the button bar when complete.

14.5.14. Download and Update a Theme

1. Choose the hierarchy level at which the theme will be applied. Note that themes can only be customized by a Provider Administrator (or higher).
2. Choose **Role Management > Themes** to open the **Themes** list view.
3. Click the theme that you want to download.
4. Click **Action > Download** on the button bar to download the theme. The exported file is a .zip archive with the name of the theme. The archive contains a folder with the theme name and files called skin.css and skin.less in it.
5. Refer to the recommended practice to edit the Less file at the end of this topic, otherwise save the file and open the CSS file in a text editor.
   - Headers are clearly marked and apply to design areas within the GUI.
   - Colors, sizes, fonts, images, and so on, can all be overwritten with the required formats.

- Images must be identified with the correct file path name. Preferably, do not use '/' preceding the path name; rather use relative paths, in other words a path relative to the CSS file location. For example, if your created an image sub-folder called 'img', use 'img/myimage.png'. After upload, the image should be viewable when opening the URL: *http://<hostname>/www/themes/mytheme/img/myimage.png*

6. When editing is complete, make sure the directory folder name is the same as your theme name. Compress the folder and save the file with the theme name and a `.zip` file extension.

   An error message will display on the user interface if the file does not have a valid file extension.

   Note that any files or folders inside the zip file archive that start with a '.' character will be silently discarded when unzipping the theme. For example, if the zip archive contains any files named `._.DS_Store` or `.directory`, they will be ignored.

7. Choose **Role Management > Themes**:

   a. For an update, choose the theme name and click **Browse** adjacent to **Import File** and then open the same theme name. Optionally select the **Backup Enabled** check box to create a backup of the current theme on the server. Click **Save** to complete the import process.

      If a theme update does not require an updated CSS in a zip file but only updates the text of the theme, then no file upload is required. For information about the other fields on this form, refer to *Add a Theme*.

   b. To delete a theme, choose it from the list and click **Action > Delete**.

The preferred way to edit a theme is to edit and compile the Less files. Refer to the "Less files and Theme Customization" topic in the "Advanced Configuration Guide".

- All changes that are made directly in the CSS files will have to be manually carried over after each changes in the Less files.
- Edit the Less files and compile them to get the new CSS files.
- The aim with Less is that a theme can be customized with the minimum of technical knowledge (as with for example Twitter Bootstrap `[http://getbootstrap.com/customize/>]`.

For an introduction to Less, visit the official website `[http://lesscss.org/]`. To compile the Less theme, a Less compiler is required. The following list shows examples:

- Online `[http://lesscss.org/usage/index.html#online-less-compilers>]`
- on your desktop `[http://lesscss.org/usage/index.html#guis-for-less]`
- IDE `[http://lesscss.org/usage/index.html#editors-and-plugins]`

14.5.15. Set the Login Page Theme

1. Choose the hierarchy level in which the theme was created or to which the theme belongs.
2. Choose **Role Management > Themes** to open the Themes list view.
3. Click the required **Theme Name** that you want to use for the Login page.
4. On the **Base** tab, select the **Use this Theme to style Login page** check box.

   If the check box is selected, and a theme with the same Interface already has the Login page check box selected, this will result in the disabling of the check box on the existing theme. There can only be one Interface-Login page combination on the system, so that any new themes or updates to existing themes may modify other themes on the system with the same Interface by disabling their Login page attributes. If no Interface is specified, the new login theme will also have its interface set to Administration.

5. On the **Login Page Details** tab, enter the required text in the **Title** field and **Banner Text** field. The text entered in the **Title** field will be displayed at the top of the Login page, above the logo. The text entered in the **Banner Text** field will be displayed at the bottom of the Login page, below the **Log In** button.

   The banner text input box allows for multi-line input so that paragraphs can be created.

   The maximum character length of the banner text is 2048 characters.

   Banner text is displayed in the format that it is entered into the input box upon configuration. If cookie and security policy references are added, these show as links that open in new browser tabs.

6. In the **Banner Text** field, references to the cookie policy and privacy policy are added to the text as placeholders:

   - `{{cookie_policy}}`
   - `{{privacy_policy}}`

   Input boxes are available on the Banner input form to add a caption and URL for each.

   Although the cookie and privacy policy references are both optional, both their caption and URL fields become mandatory if they are used. The placeholder reference is then also required in the banner input box.

   For suggested input on the use of cookies by VOSS-4-UC in the cookie policy text, see *VOSS-4-UC Cookie Policy*.

   Note that if a browser has a blocker installed that prevents new tabs from opening, this will affect the functionality of the links in the login banner.

   Privacy policy links can also be added to user menus. Refer to *Privacy Policy Menu Items* and *Manage Privacy Policy Menu Items*.

   To customize the banner text style, refer to the topic on “Theme Banner Customization” in the “Advanced Configuration Guide”.

7. Click **Save** on the button bar when complete to implement the selection.

The Login page theme can also be applied to the login page during the log in process. Do this by adding the suffix ‘?theme=default’ to the login request url.

For example: `https://instance/login/?theme=default`,

where ‘default’ is one of the themes available in VOSS-4-UC. This usage in the URL will apply and override any theme that is set as the login theme.

14.5.16. Login Banner

A banner, typically a security notice or user agreement, can be configured at a hierarchy level to show on the Administrator and Self-Service login page before login.

High level administrators who have access to the `data/LoginBanner` model can configure the banner. A banner can be created so that:

- Only one instance is allowed per hierarchy

If an administrator or Self-Service user logs in and belongs to a hierarchy for which there is no defined login banner, the first banner higher up on the hierarchy is displayed. If no banners are configured, then the user logs in without a banner.

The banner text is displayed in the format that it is entered into the input box upon configuration.

When the banner is configured, users will see the banner displayed on the login page after they enter their credentials and when they click the **Login** button. An **Agree** and **Cancel** button is shown beneath the banner. Users then need to click the **Agree** button to complete the login. If they click **Cancel**, they are returned to the login page.

Note: This banner is independent of the text on the login screen that may contain a privacy policy reference. The privacy policy text and reference on the login page is configured as a part of the Login Page Details when managing a theme - see *Set the Login Page Theme*.

14.5.17. Self-service Theme Customization

This section provides steps to customize and add a Self-Service theme.

To customize an existing Self-service theme:

1. Choose the hierarchy level at which the theme will be applied. Note that themes can only be customized by a Provider Administrator (or higher).
2. Choose **Role Management > Themes** to open the **Themes** list view.
3. Click the Self-service theme that you want to download.
4. Click **Action > Download** on the button bar to download the theme. The exported file is a .zip archive with the name of the theme. The archive contains a folder and a `.css` file with the theme name in it, for example `voss_selfservice.zip` contains `voss_selfservice/voss_selfservice.css`.
5. Modify the `.css` file, for example `voss_selfservice.css`. Use your browser to inspect the elements of the theme on the GUI that you wish to customize.
6. When editing is complete, make sure the directory folder name is the same as your theme name. Compress the folder and save the file with the theme name and a `.zip` file extension.

   An error message will display on the user interface if the file does not have a valid file extension.
7. Return to **Role Management > Themes**:

   a. For an update, select the theme name and click **Browse** next to **Import File**, and then open the same theme name. Optionally select the **Backup Enabled** check box to create a backup of the current theme on the server. Click **Save** to complete the import process.

   If a theme update does not require an updated CSS in a zip file but only updates the text of the theme, then no file upload is required. For information about the other fields on this form, refer to *Add a Theme*.

The preferred method to add a new Self-service theme is to downloading an existing theme to maintain directory structure and file naming conventions.

To add a new Self-service theme to the system:

1. Choose the hierarchy level at which the theme will be created.
2. Choose **Role Management > Themes** to open the **Themes** list view.
3. Click **Add** on the button bar to open the **Themes** input form. Note that themes can only be customized by a Provider Administrator (or higher).
4. Enter the **Theme Name** (same as the file name created above).
5. Enter an appropriate **Site Title** if required. The site title entered here is the title displayed in the browser tab.

6. Click the **Browse** button to import the created theme zip file. Wait until the system displays the file chosen in the **Import File** field.
7. If the theme must also apply to the login page, select the **Use this Theme to style Login page** check box.
8. To set login banner text and notices on the login page, refer to *Set the Login Page Theme*. The **Use this Theme to style Login page** check box does not have to be enabled for banner text to show.
9. Click **Save** on the button bar when complete.

Self-service Banner Style

To customize the Self-service banner style, find the element `.banner-text` in the CSS file and customize it, for example:

```
.banner-text {
    background-color: #515150;
    color: #FFFFFF;
}
```

Minimal Theme Customization

In order to customize the Self-service theme to support the minimal mode, the elements below are available.

Important: If your theme uses a dark colors, the minimal theme may need to be modified to provide a contrasting text and background display.

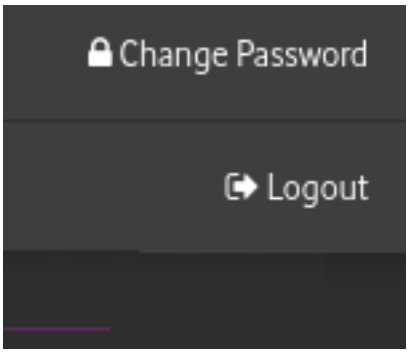
The examples below are minimal mode image snippets and theme settings:


```
.minimal-mode-container {color: white;}
.minimal-mode-container .overlay {background-color: #2e2e2e!important;}
```

- resized logo (`<number>` variable)
- resized tagline (`<number>` variable)


```
.logo-holder-header {padding: <number>px <number>px;}
.ss-tagline {height: <number>px; width: <number>px;}
```

- contrasting drop-down menu items and text




```
.minimal-mode-menu ul {background: #3e3e3e;}
.minimal-mode-menu ul li {border-bottom: 1px solid #2e2e2e;}
.minimal-mode-menu ul li > a {color: white;}
```

14.5.18. Menu Layouts

Menu layouts define the view a user has of the menu content and structure on the GUI. This is fully customizable up to three levels deep and can be created or edited to represent the content any user needs to have access to. The association of the defined view of the menu is made with the user's role and menu layouts can be created directly on the GUI.

To refine a view of model entities for a user, a Field Display Policy (FDP) and Configuration Template (CFT) for a model can be applied. The FDP and CFT for a specific model is applied as part of the menu layout - in other words in the menu structure, the FDP and CFT are attributes of the specific model entry for that menu layout. This means that:

- Different FDPs and CFTs for a specific model can define menu layout variations for that model.
- The required FDP and CFT should be available and defined before creating new menus.

If a menu layout applies to the list view of a model, this list can be filtered by means of a number of filter options that apply to the displayed list. Only instances where the values of a model attribute that match the filter, are then shown.

Default menu layouts are provided with VOSS-4-UC. These include defaults for pre-defined hierarchy based user roles, namely System Administrator (hcsadmin), Provider Administrator, Reseller Administrator, Customer Administrator and Site Administrator. The details of these default menu layouts can be viewed and easily edited to either remove or add entries, update entries (for example with an alternative FDP), change default values (for example with an alternative CFT), or change the order and groupings of the items.

The menu layout is an attribute of the user role. Each user must be assigned a User Role, thus the user will see the menu layout based on this user role. See *User Roles*.

Menu layouts can also be copied via the Clone option so they can be edited or exported and re-imported.

Designers who have access to tag or version tag can apply these to a menu layout so that it can be uniquely identified to track and control changes.

Refer to the Best Practices Guide for additional details.

14.5.19. Best Practices Menus

In addition to a default set of menus, VOSS-4-UC also provides best practice menus for provider and customer administrators, including the associated access profiles and landing pages. The names of these

items can be identified by the word `Enhanced` in the model name.

These menus have a more business-oriented structure and include additional options based on best practice adaptations that may also be included in VOSS-4-UC.

The best practice menus have the following features:

- A menu order, nesting and naming convention according to common business use.

  The top-down order of the menus follow the logical order of tasks and system hierarchies that are used to carry out these tasks.

  For example, for provider administrators, the **Cisco UC App Management** menu provides menus only for these Cisco devices, while SMTP server and other settings carried out by providers are arranged under **Provider Configuration**. Similarly, the **Cisco Subscriber Services** menu has sub-menus for all the functionality associated with these subscribers in VOSS-4-UC.

- Additional naming conventions that identify the menu type:
  - Where a menu refers to an *adaptation*, the menu name indicates this with an asterisk (*) appended, for example **Move Phone and Services** *.
  - Where a menu is for a *form view* (input or edit), the first word in the menu name is in capitals, for example **ADD Internal Number Inventory**. Note that this does not apply to menu names that start with abbreviations and acronyms like E164, HCS, LDAP and so on. In this case, the capital rule will apply to the next word in the menu item name.
- Menus for URLs:
  - Menus are provided for VOSS-4-UC portals so that is easy to launch into another portal.

Important: In the case of menus that use URLs, you need to update the URLs to match your configuration.

To modify and to assign your modification of a best practice menu to a user role, consider the following:

- Managing menu layouts - see: *Create a Menu Layout*. Also consider using the Menu Diff Tool to easily modify menus - see the Advanced Configuration Guide for details.
- Field Display Policies associated with menu items are available. For further configuration, see: *Add or Edit a Field Display Policy*.
- Configuration Templates associated with menu items are available. For further configuration, see: *Workflow for Creating Configuration Templates*.
- Access Profiles for the best practices menus are provided - see the list under the **Access Profiles** menu. If any access profiles need to be modified to align with a modified menu, see: *Access Profile Permissions and Operations*.
- Landing Pages for the best practices menus are provided - see the list under the **Landing Pages** menu.

14.5.20. Create a Menu Layout

Note: To work on an existing menu layout, we recommend that you clone the menu layout and work on the clone.

---

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

2. Choose the hierarchy for the menu layout.
3. Choose **Role Management > Menu Layouts**.
4. Click **Add** to open the **Menu Layouts** input form.
5. Enter a **Name** and a **Description** for the menu layout.
6. Add (by clicking **+** next to **Menu Items**), and optionally nest **Menu Items** for each required menu item:
    a. Choose an **Icon** name from the dropdown to be displayed on the GUI menu. To see the icons, refer to *Business Admin Portal Interface Custom Icon Names Reference*.
    b. Enter a **Title**.
    c. For a list view of a model, select from the **Type** drop-down list and choose List as the **Display as** value. For the selected model type, choose a default **Field Display Policy** and **Configuration Template**. If a User Role is associated with the menu layout, then users with this role see the model type according to these.

    If **List** is chosen as the **Display As** type, then the resulting list can also be filtered. See *Configurable Filters in Menus and Landing Pages*.
    d. **Href** is generally used for external links. It can however be used for links within the application to link directly to a form. For example, the **Add Phone** form would have the HREF value of `api/relation/SubscriberPhone/add`. In such cases, any associated Field Display Policies and Configuration Templates for the menu item can only be added by using a menu import in JSON format or on a bulk load sheet.

    Note that `view/` type models should not be referenced as **Href** - only from the **Type** drop down. The `view/` model types always open the "Add" form - without having to use the href with `/add/`.

    If **Href** is used, choose the **Display as** format of the item as follows:

    - Form - Show an input form. The **Href** value points to a model instance with the pkid, for example `data/Countries/5331a739d0278d7893e26d2e`, or ends with "/add/".
    - IFrame - A URL specified as the **Href** value opens as an IFrame for cross-launching.
    - External Link - A URL specified as the **Href** value opens as a new browser tab.

      Note: pop-up blocking should be disabled on user browsers for the external link to resolve.
    - Tree - If available, a tree view of resource to display. **Href** provides the tree path.
    - List - List view of a resource referenced by **Type** or **Href**. A tool (`tool/[toolname]`) can also be presented as a list, for example

      `/api/tool/Transaction/?entity=data/Event&operation=execute`
    - Wizard - Execute a wizard referenced by **Href** (wizard resource ends with "/0/"). For example:

      `/api/wizard/AddressWizard/0/`
    e. Arrange the desired order of the menu items by clicking the up or down arrow to move the menu items up or down respectively.
7. Click **Save** on the button bar when complete to create the menu layout.

To modify an existing menu layout, click the relevant menu layout name from the **Menu Layouts** list view and edit the appropriate fields as described above. Click **Save** when complete.

Updates in the menu layout are available for the user only when logging in again.

When complete, assign the menu layout to the appropriate roles.

14.5.21. Menu Layout Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Menu Layout.
Description	description	A description of the Menu Layout.
Menu Items	menu_items	The list of menu items and -sub items that belong to the Menu Layout.

Menu Items

Title	Field Name	Description
Title	title	The menu item title as it will show on the menu.
Type	type	The chosen model type from the **Type** drop-down list to associate with the Title.
Href	href	If a direct reference to a model type is used for the menu item, the specified path.
Field Display Policy	field_display_policy	The chosen **Field Display Policy** that is associated with the Menu Item.
Configuration Template	configuration_template	The chosen **Configuration Template** that is associated with the Menu Item.
Display As	display	Choose the display format of the model types of the menu item. The format can be a **Form** for a single instance, or a **Tree** or **List** for more than one instance. Default = List.
Menu Items	menu_items	The list of nested menu items that belong to the Menu Layout.

Configurable Filters

Fixed Filters cannot be removed.

Title	Field Name	Description
Configurable Filters	filter_options.[n]	For **List** option only.
Filter By	filter_by	Attributes of the **Type** can be chosen from the drop-down list.
Filter Type	filter_type	Choose the matching operator for the filter.
Filter String	filter_string	Choose the value that the matching operator should match by.

14.5.22. Landing Pages

This is the user's home page, which is seen when the user logs in and then uses the application **Home** button.

The landing page configuration options provide an opportunity to set up short-cut links to frequently used functionality, and to enhance the look and feel on the user's GUI. Images and links can be added in vertical or horizontal patterns with unlimited boxes and shortcuts which can then be assigned to a user's role.

A default page is loaded in the system and associated to pre-defined roles in the hierarchy, for example Provider, Customer, and Site administrators.

These editable configurations provide an easy mechanism to define direct links to areas in the system which can be used as short-cuts by the administrators in line with their role.

Existing images can be used or new images can be added in line with branded look and feel.

Landing pages can also be copied via the Clone option so they can be edited or exported and re-imported.

For designers with access to the tag function, this enables the landing page to be uniquely identified and a tag version can be applied to track and control changes.

The CSS of the Theme can be used to control the layout of the landing page.

Refer to the Best Practices Guide for additional details.

14.5.23. Create a Landing Page

Refer to the Landing Page Definition topic.

Note: To work on an existing landing page, we recommend that you clone the required landing page and work on the clone.

---

1. Log in as the provider administrator.
2. Choose the hierarchy level for the landing page.
3. Choose **Role Management > Landing Pages** to show the list view of Landing Pages (if configured). Note that this option is only available to Provider Administrators (or higher).
4. Click the **Add** button.
5. On the **Base** tab, enter a name for the Landing page.
6. Click the + button on the **Meta Tasks** field and fill in the necessary information. See *Landing Page Definition* for details about available fields.
7. Click the + button on the **Sections** field and fill in the necessary information. See *Landing Page Definition* for details about available fields.
8. On the **Welcome Header** tab, enter the required Header Text, which is a single line static welcome message displayed on top of the Landing page.
9. Enter the required Line Text, for the welcome line displayed under the header, Use [userrole] as a placeholder to insert the current user's role. to serve as the header, for example `/www/img/landingPageIcons/User.png`.
10. Click **Add** adjacent to links, for each required link in the section, and enter the link details.

    Choose an **Icon** name from the dropdown to be displayed *only on* the landing page. To see the icons, refer to *Business Admin Portal Interface Custom Icon Names Reference*.

    The available fields are for menu items when creating Menu Layouts. If Type is selected, field display policies and configuration templates can be applied. The link Type is displayed as the chosen Display As item:

- Form - Show an input form (for an Href value, a resource ends with "/add/").
- Inline List - The link points to the first five list of items. See also *Landing Page Definition* for more information on this field.
- List - List view of a resource referenced by Type or Href. If **List** is chosen as the **Display As** type, then the resulting list can also be filtered. See *Configurable Filters in Menus and Landing Pages*.
- Tree - A tree view of resource to display (if the system Href provides a tree path).
- Wizard - Execute a wizard referenced by the Href. The wizard resource URL ends with "/0/".
- IFrame - A URL specified as the Href value opens as an IFrame for cross-launching.

11. Arrange the desired order of the sections by clicking the up or down arrows to move the sections up or down respectively.
12. Click **Save** when complete to create the landing page.

To modify an existing landing page, click the relevant landing page name from the Landing Page list view and edit the appropriate fields as described above.

When complete, assign the Landing Page to the appropriate roles.

14.5.24. Landing Page Definition

The landing page definition comprises the following:

- Name - A landing page name.
- Meta Tasks - Allows you to add one or more shortcut buttons at the top of the home page screen (directly below the line text - if configured).
- Sections - One or more items displayed as a distinct block on the landing page. Sections are further broken down to:
  - Title - The heading given to the section.
  - Image URL - The image or icon that is displayed for a section. For example, if a theme was uploaded with landing page images and inside a sub folder of the theme folder is a file called *mytheme/img/landingpage/landing1.png*, then the URL would be: */www/themes/mytheme/img/landingpage/landing1.png*.
  - links - One or more links for a section, described in the table below.

See also *Landing Pages*.

Meta Tasks / Links Field	Description
Button Text (Meta Tasks section only)	Text that is displayed in the task's button.
Link Text (Links section only)	The text that is displayed as the link. If the link is displayed as Inline Form, then a field name from returned data type may be specified instead. This field is mutually exclusive with Columns. Note that if the display is **Inline List**, then all displayed links show this text.
Type	The **Model Type** that is displayed or targeted by the link. If this field is populated, then the Href field (below) should be blank. For example, if **Model Type** is selected as `data/User` and the **Display As** option is `List`, then the menu link shows the list of instances of `data/User`.
Href	API URL on which the client performs retrieves the link's data from If this field is populated, then the Type field (above) should be blank. An example **API URL** would be /api/relation/SubscriberPhone/ for a list of items of type relation/SubscriberPhone.
Field Display Policy	If specified, the Form URI is extended to apply the policy to the returned form. For example, if **Model Type** is selected as `data/User/add` and **Display As** option is `Form`, then a Field Display Policy that is available for `data/User` can be selected to apply to the form in order to for example hide or rename input fields.
Configuration Template	If specified, the Form URI is extended to apply the template to the returned form. For example, if **Model Type** is selected as `data/User/add` and **Display As** option is `Form`, then a Configuration Template that is available for `data/User` can be selected to apply to the form in order to, for example, provide default values.
Display As	Determines how the link is displayed. The options are: • **Form** - The link opens using a form widget. • **Inline List** - The link points to the first five list of items. • **List** - Link target is rendered using the list widget. The list can be filtered. • **Tree** - Display the link target using a tree widget. • **Wizard** - Display the link target as a wizard. • **IFrame** - Display the link target in an iFrame. Used for x-launch. If the **Inline List** option is chosen, the **Display Multiple Columns** field is visible. The first five items are displayed in the section. If the list is longer than five items, a link to the whole list is displayed after the first five.

If **List** is chosen as the **Display As** type, then the resulting list can also be filtered. See: *Configurable Filters in Menus and Landing Pages*.

14.5.25. Landing Page Field Reference

Welcome Header

Title	Field Name	Description
Header Text *	header	A single line static welcome test displayed on top of the landing page.
Line Text *	line	Text for the welcome line displayed under the header. Use [userrole] as a placeholder to insert the current user's role.
Meta Tasks	meta_tasks	Definitions for the meta task shortcut buttons.

Base

Title	Field Name	Description
Meta Tasks	meta tasks	Definitions for the meta task short-cut buttons.
Sections	sections	The list of section items that belong to the Landing Page.

Meta Tasks

Title	Field Name	Description
Display As	display	Select the display format of the model types of the menu item. The format can be a **Form** for a single instance, or a **Tree** or **List** for more than one instance. Default = List.
Button Text	button_text	Text for the button.
Type	type	The selected model type from the **Type** drop-down list to associate with the Title.
Href	href	If a direct reference to a model type is used for the menu item, the specified path.
Field Display Policy	field_display_policy	The selected Field Display Policy that is associated with the Menu Item.
Configuration Template	configuration_template	The selected Configuration Template that is associated with the Menu Item.

Sections

Title	Field Name	Description
Title *	title	The section title as it will show on the Landing page.
Image URL	image	Optional URL to image to be displayed as section image.
Links	links	List of links that belong to section.

Links

Title	Field Name	Description
Display As	display	Choose the display format of the model types of the menu item. The format can be a **Form** for a single instance, or a **Tree** or **List** for more than one instance. Default = list.
Display Multiple Columns	is_multicolumn	Determines if link is shown as multiple columns or not.
Link Text	link_text	Text for the link.
Columns	columns	Determines if links are shown as single or multiple columns.
Type	type	The selected model type from the **Type** drop-down list to associate with the Title.
Href	href	If a direct reference to a model type is used for the menu item, the specified path.
Field Display Policy	field_display_policy	The selected Field Display Policy that is associated with the Menu Item.
Configuration Template	configuration_template	The selected Configuration Template that is associated with the Menu Item.

14.5.26. Configurable Filters in Menus and Landing Pages

Click **More...** in the **Configurable Filters** column to open the dialog to enter one or more filter options. If more than one filter is added, this results in a logical AND of the filter application.

- **Filter By** - attributes of the selected Type can be selected from the drop-down list.
- **Filter Type** - select the matching operator to apply when the attribute is matched to the **Filter String** value:
  - Contains
  - Does Not Contain
  - Starts With
  - Ends With
  - Equals

  - Not Equal
- **Filter String** - select the value that the matching operator should match by.
- **Ignore Case** - check box to manage the case of the **Filter String** value.

When the menu item or landing page link is then selected, a pop-up filter box is displayed and the administrator is prompted to apply or modify the filter. If a **Filter String** value is entered on **Configurable Filters**, this value can also then be accepted or modified in the pop up box.

The list view of the results footer row indicates that a filter has now been applied to the list and this filter can then be further modified and removed from the list view as usual - see *Filtering Lists*.

Important: Standard list view filters on model types (for example if accessible by other landing pages or menu items) can still be used as described in *Filtering Lists*, but these will be removed and replaced by any Configurable Filters on landing page links or menu items for the corresponding model type.

Fixed Filters

Only high-level administrators can add and modify pre-defined **Fixed Filters** to menus and landing pages. For these administrators, this option also shows on the Menu Layout and Landing Page design input forms and presents the same interface options as Configurable Filters.

These filters are not visible to the lower level administrators and will *always* apply when the menu item or landing page link is used by them. Fixed filter results can however be filtered further by Configurable Filters.

14.5.27. Deploy a Customized Credential Policy

A default credential policy called HcsCredentialPolicy ships with VOSS-4-UC. However, you can deploy a customized credential policy at a provider, reseller, or customer hierarchy node.

When you set a customized credential policy as the default credential policy at a hierarchy node, all users and admins at or below that hierarchy node are subject to the customized credential policy, except for any users or admins that are explicitly assigned a different credential policy.

Credential Policy Inheritance

Unless explicitly assigned a credential policy, users and admins are subject to the default credential policy set at a hierarchy node at or above their location. The default credential policy for the hierarchy node closest to the user or admin location is used. If no customized credential policies are deployed, all users and admins are subject to the HcsCredentialPolicy credential policy, which is the default credential policy at the sys.hcs level.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where you want to deploy a customized credential policy.
3. Choose **Role Management > Credential Policy**.
4. Either clone the HcsCredentialPolicy credential policy, or add a new credential policy:
   - To clone the HcsCredentialPolicy policy, click **HcsCredentialPolicy**, then click **Action > Clone**.

- To add a new credential policy, click **Add**. The credential policy settings default to the settings for HcsCredentialPolicy.

5. Provide a name for the credential policy.
6. Modify the credential policy settings as needed.

Field	Description
Idle Session Timeout	The number of minutes a user session can be idle before being automatically logged off. The minimum setting is 1 minute and the maximum is 525600 minutes (365 days). The default is 20 minutes.
Absolute Session Timeout	The number of consecutive minutes a user can be logged in, regardless of session activity, before being automatically logged off. A value of 0 disables absolute session timeout. The maximum is 525600 minutes (365 days). The default is 1440 minutes (24 hours).
Password Expires	The number of months that can elapse between password resets. The default is 6 months.
User Must Change Password on First Login	Select this check box to force users to change their password on initial login. Default = clear.
Lock Duration	The number of minutes a lock will be held when user is locked out. The default is 30 minutes.
Disable Failed Login Limiting per User	Select this check box to not limit the number of times a user can fail to log in before the account is locked. Default = clear
Failed Login Count per User	Selecting this check box will result in user account being disabled if failed login attempt reaches 'Failed Login Count per User' within 'Reset Failed Login Count per User (minutes)'. This field is clear by default.
Reset Failed Login Count per User	After this number of minutes from the last login attempt, the failed login count is reset to 0. The default is 5 minutes.
Disable Failed Login Limiting per Source	Clear this check box to limit the number of times any user from the same IP address can fail to log in before the account is locked. The default is to disable the limit. Note: Do not enable source login rate limiting for a credential policy that will apply to Self Service users. A separate credential policy is recommended for administrators and users that do not use Self Service if source login rate limiting is required.
Failed Login Count per Source	If source login rate limiting is enabled, enter the number of times any user from the same IP address can fail to log in before the IP address is blocked. The default is 10 times.
Reset Failed Login Count per Source	If source login rate limiting is enabled, this value is the number of minutes from the last login attempt from the IP address after which the failed login count is reset to 0. The default is 10 minutes.

Field	Description
Number of Questions Asked During Password Reset	Enter the number of security questions users or admins must answer when resetting their own password with the **Forgot Password** link. The default is 3.
Password Reset Question Pool	Contains a list of possible security questions that users or admins must answer when resetting their own password with the **Forgot Password** link.
Password Reuse Time Limit	The number of days from the date the password was created that the password cannot be reused. The valid range is 0-365 days. The default is 15 days. Setting it to 0 disables the reuse time limit.
Minimum Password Length	The minimum length of a password in characters. The minimum allowed value is 8. The default is 8.
Enable Password Complexity Validation	Select this check box to enable the rule on how complex a password must be. The complexity rule requires a password to contain at least one of each of the following: • Uppercase letter • Lowercase letter • Digit • Special character (see below)
Inactive Days Before Disabling User Account	The number of days users or admins can go between logging in without having their account disabled. Setting it to 0 disables the inactive time limit. The default is 0.
Session Login Limit Per User	The number of concurrent login sessions a user may have. Setting it to 0 disables the session login limit. The default is 0. If the session limit value is set to 1 or more and the user exceeds the session limit when starting a new session, the oldest login session will be disconnected.
Number of Different Password Character	The minimum number of character changes (inserts, removals, or replacements) required between the old and new passwords.
Minimum Password Age	The number of days within which a user cannot change their password. A zero (0) value means that password age validation is disabled. The minimum value is 1 day and the maximum is 365 days.

Acceptable special characters are:

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

Note:

We recommend that you make a credential policy only more restrictive than HcsCredentialPolicy in order to not have a policy that is too insecure.

7. Click **Save**.

   Note:

   If a user is already logged in when the credential policy is changed, changes do not take effect until the user logs out and logs in again.

8. Choose **Role Management > Default Credential Policy**.

9. Provide a name for the Default Credential Policy at this hierarchy node.
10. From the **Credential Policy** drop-down, choose the credential policy you just cloned or added.
11. Click **Save**.

Every user and administrator at or below the hierarchy node is now subject to the default credential policy, unless the user or administrator was explicitly assigned a different credential policy.

Note: Timeout limits will initiate the display of timeout limit notifications in the GUI - see: *Timeout Limit Notifications*.

14.5.28. Session Timeout Rules

The following rules apply to the idle session timeout and absolute session timeout values that can be applied to users via a credential policy:

- Setting the absolute session timeout to 0 disables it.
- The absolute session timeout takes priority over the idle session timeout. Therefore, setting the absolute session timeout to a value less than the idle session timeout effectively disables the idle session timeout.
- Credential policy session timeouts do not apply to SSO authenticated users. For SSO authenticated users, VOSS-4-UC honors the SessionNotOnOrAfter SAML 2.0 attribute, which is equivalent to an absolute session timeout, although controlled by the IDP.

Note: Timeout limits will initiate the display of timeout limit notifications in the GUI - see: *Timeout Limit Notifications*.

14.5.29. Timeout Limit Notifications

Timeout Limit Notifications are displayed in accordance with the Credential Policy that is associated with a user. See: *Deploy a Customized Credential Policy* and *Session Timeout Rules*.

From 60 seconds before the session limit, in other words before a session expires, a warning message "Session will expire in [n] seconds" will show in the GUI and will count down.

If the idle session limit generated the message (and the idle session limit is set to less than the absolute session limit), the user has the option to click the **Stay Logged In** button to extend the session. If the absolute session timeout is about to be reached, the user has the option to click the **Log Out Now** button to return to the login screen or to click **OK** to dismiss the message and finalize work before logout. All transactions submitted after clicking **OK** will be processed.

If the user does not click a button on the warning message box, the user is logged out and the GUI returns to the login screen.

SSO users see the message:

"Your Single sign-on session will expire in [n] seconds. All transactions submitted after clicking **OK** will be processed. When the session expires, you will be automatically redirected to the log-in page."

For the GUI theme modification of the notification, refer to the Advanced Configuration Guide.

14.5.30. Privacy Policy Menu Items

In order to comply with General Data Protection Regulation (GDPR) requirements, VOSS-4-UC provides the means to manage privacy policy notices on the user interface.

By default, high level system administrators above the Provider level hierarchy can manage privacy policy references that are available on user menus. These administrators can provide the required access to the `data/PrivacyPolicy` data model and add menus to lower level administrators if required.

Privacy policy references can be set up for each hierarchy. If one is not added to a specific hierarchy, the one at the next higher hierarchy applies.

When a privacy policy applies to a user hierarchy:

- On the admin GUI, a privacy policy menu item is added to the bottom of the user's menu. The title of the menu item is the name of the created policy.
- On the Self-service GUI, a side button bar menu item is added. The title of the menu item is **Privacy Policy**.

When selecting the menu item, the link URL of the policy opens on a new browser tab.

Note:

- For the admin GUI, the Privacy Policy menu item is not visible from a menu layout and cannot be managed from **Role Management > Menu layouts**.
- Login page privacy policy links are managed from **Role Management > Themes**. Refer to *Set the Login Page Theme*.

14.5.31. Manage Privacy Policy Menu Items

1. Log in as an administrator with the required privacy policy management permissions and menu access.
2. Choose the menu item, for example by default, **Role Management > Privacy Policy Configuration**. The list view shows privacy policy names and links at various hierarchies in the system. Privacy policies can then be added, modified and deleted.
3. To add a privacy policy, navigate to the hierarchy at which the privacy policy should be added and click **Add**.
4. Add a Name, Privacy Policy URL and click **Save**. Note that this name becomes the menu item name.

On the admin GUI, a privacy policy menu item is added to the bottom of the user's menu - for users at the specified hierarchy or lower and without a privacy policy on their own hierarchy. On the Self-service GUI, a side button bar menu item is added.

14.5.32. VOSS-4-UC Cookie Policy

When formulating a cookie policy, customers should include details on the use of cookies by VOSS-4-UC. The text below provides details on the use of cookies in VOSS-4-UC that can be included in the policy:

```
VOSS-4-UC uses cookies for the following purposes:

Personalisation - we use cookies to store information about your most recent settings,
preferences and to personalize our website for you.

The cookies used for this purpose are:

hierarchyTreeSaveStateCookie
resourceTreeSaveSelectedCookie
resourceTreeSaveStateCookie
ace.settings
sso_login_url

Security - we use cookies as an element of the security measures used to protect
user accounts, including preventing fraudulent use of login credentials, and to
protect our website and services generally.

The cookies used for this purpose are:

* Administrator login:

  csrftoken
  sessionid

* Self-service login:

  csrftoken
  sessionid
  session
  rbacInfo
```

14.6. Access Profiles

14.6.1. Access Profiles: Overview

Access profiles define model types that a user is permitted to access. Access profiles are assigned to users via Roles.

Note: Access Profiles (APs) are subject to the following requirements:

- Default APs: adhere to the following hierarchy of permissions: **Provider > Reseller > Customer > Site**. For instance, default Customer APs have less permissions than Provider APs.
- Cloned APs: the cloned AP has equal or less permissions than the AP of the admin user who creates the clone.

When a System Upgrade is performed, the default access profiles are updated in accordance with the above.

Note: Existing cloned APs are **not** upgraded. You have to manually update them, or re-clone and modify them from the upgraded, default versions as needed.

14.6.2. Access Profile Permissions and Operations

Administrators *above* Provider level can maintain Access Profiles as a part of Role Management. In particular, a profile assigned to a role can provide a general set of permissions and well as Type-specific operations which are associated with specific models.

For Type-specific operations, wild cards may be used in model references, for example `data/*`.

Note:

- Type-specific permissions that are also configured as general permitted operations will override the general permissions.

The default access profiles show typical configurations, for example an Operator-type profile at a hierarchy would *only* require **Read** type-specific permissions, while the administrator profile at the same hierarchy would have **Create**, **Update** and **Delete** permissions for the same type.

The lists below provide details on the types of settings.

- **Miscellaneous Permissions**

  Many of these are general permissions that can be overridden per model as **Type Specific Permissions**.

  The explanations below show the affect of enabling the permission.

  - **Api Root**: Access to API root endpoint is permitted.
  - **Device Type Root**: Access to API `device` type model root endpoint is permitted.
  - **Export Data**: General permission to export data.
  - **Help**: On-line help button is shown.
  - **Help Export**: Help data can be exported.
  - **Login**: Login is allowed.
  - **Meta Schema**: Meta schema is accessible.
  - **Model Type Choices**: Access to API choices endpoint of model types is permitted.
  - **Model Type Root**: Access to API model root endpoint is permitted.
  - **Operations**: Operations on models are permitted.
  - **Tag**: Models can be tagged.
  - **Tool Root**: Access to API tool root endpoint is permitted.
  - **Upload**: Uploads are allowed.

- **Type Specific Permissions**

  These are typically available from the **Action** menu or menu bar on the GUI when listing or showing the type.

  Note:

  - The available permissions can vary according to the selected type.
  - If the **Create** type specific permission is enabled for a model type, this also enables **Clone** of a model instance.

Typical operations are listed below:

- **Create**, **Delete**, **Read**, **Update**: management operations on models.
- **Configuration Template**, **Field Display Policy**: create these for the model.
- **Export**, **Export Bulkoad Template** : allow export formats of the model.
- **Bulk Update**: from a GUI list view, more than one item can be selected and updated.
- For system level administrators above provider level (hcsadmin or entadmin): **Purge** for device models. From a list or instance view, remove the local database instance but retain it on the device.

  Note: This operation is only applicable in cases where the Unified CM is still online and available in the VOSS-4-UC system.

- For designers: **Migration**: a migration template can be obtained.
- For designers: **Tag** and **Tag Version**: a model instance can be tagged and a version provided.

14.6.3. Access Profile Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Access Profile.
Description	description	A description for the Access Profile.
Full Access	full_access	Enabling this flag, grants the user full system access.
Miscellaneous Permissions	miscellaneous_permissions	The list of miscellaneous operations permitted by this Access Profile.
Type Specific Permissions	type_specific_permissions	The list of types that are permitted by this Access Profile.

Type Specific Permissions

Title	Field Name	Description
Permitted Type *	type	The type that is permitted by this Access Profile. This field supports the use of the * wildcard.
Permitted Operations	operations	The operations that are permitted by this Access Profile for the given type.

14.7. Customizations

14.7.1. GUI Customization

The system allows for the user interface to be customized by a provider administrator (or higher) as required.

This customization includes:

- Theme selection
- Menu Layout customization and associated Field Display Policies
- Landing Page customization
- Field Display Policies
- Configuration Templates

14.7.2. 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.
  - 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.

14.7.3. Field Display Policies

Field Display Policies are applied to certain item types in order to modify the default form that is displayed when these items are created or accessed.

With Field Display Policies, the fields on an item detail form can be grouped, disabled, and on-line help text can be added for a field. A field can be provided with a new label and its position on the form can be moved up or down.

More than one Field Display Policy can apply to a particular item type so that the selection of a particular policy will present another view of the form.

A Field Display Policy for an item type can be applied from a Menu Layout by selecting and associating it with the item on the Menu Layout. The Menu Layout is then selected to be part of a user Role so that users who have this role and log in will be able to have the item displayed according to the relevant Field Display Policy.

For example, a system may have users at Provider, Customer and Site administration hierarchy levels - all of whom may access the same items, but perhaps some item fields need to be hidden for administration users at a certain level. Field Display Policies can then be made that are applied to the Menu Layout associated with the administration users at these levels.

A quick way to add a Field Display Policy is to clone an existing Field Display Policy, modify it as required and then to select it for the model on a user's menu layout. In this way a user's interface can be modified from the point of user access to the model on the menu.

There is a unique constraint on the name of the Field Display Policy per hierarchy level. The same name can be used on another hierarchy, but a new name is needed at the same hierarchy.

A Field Display Policy can also be selected for a form that is part of a Wizard.

If a Field Display Policy is called 'default', it will apply to a model by default.

14.7.4. Rules When Creating a Field Display Policy

When creating groups and selecting the field transfer boxes of a group, a number of rules apply.

Regarding notation: if the fields belong to objects or arrays, the names in the transfer boxes are shown in dot notation. Refer to the target model type on-line help field reference to distinguish object types from array types.

To understand the rules below, consider a selected Target Model Type with the fields as listed below. Where the name starts with “A”, the field is an array and where it starts with an “O” it is an object. The values “x”, “y”, “z” are also objects. The field “F” is neither object or array.

- A, A.x, A.x.b, A.x.c, A.x.d, A.y.r, A.y.s, A.y.t
- F
- O, O.v, O.z, O.z.a, O.z.b, O.w.d

The following inclusion rules apply:

- If a parent object or array field is included, the parent and all its children will be displayed in the GUI. For example, if O.z is selected, O.z is saved as the fields and the GUI will display O.z and also inner fields O.z.a and O.z.b.
- If a specific selection and order of child elements are required, select these child elements and order them. For example, if O.w.d, O.z.b, F are selected, these three fields are saved in that order in the FDP group fields and the GUI shows only the inner field O.w.d, followed by the inner field O.z.b and lastly the field F.
- Inclusion of child fields in a group without the inclusion of the parent fields will display these child fields at the root level of the form. For example, if O.w.d, O.z.b are selected, these fields are saved as is in the FDP group fields list and only the inner fields O.w.d and O.w.b are shown in the GUI.
- Array children fields without their parent fields will be ignored by the GUI. Therefore, if the child fields of an array field are selected, the parent field should also be selected. For example, if A.y.s, A.y.t are selected, A and A.y should be selected.
- Array fields may not be split into different groups.
- The parents of fields cannot be in one group and its children in another. For example, O.z cannot be in Group 1 if O.z.a, O.z.b and O.w.d are in Group 2.
- Fields of the same object and members of the same array type cannot belong to more than one group. For example:
  - If A.y.s is selected for Group 1, then A.y.t cannot be selected for Group 2.
  - If O.z.a is selected for Group 1, then O.z.b cannot be selected for Group 2
- You can split the first level children of object fields into different groups. For example:
  - O.v can be in Group 1 while O.z is in Group 2.
  - For second level children: O.z.a can be in Group 1 and O.w.d can be in Group 2.
- To hide a field, do not move it to a Selected box. For example, to hide O.z.b, select O.z.a, O.w.d.

To order fields in a group, arrange them in the Selected box. Use the **Move Up** and the **Move Down** buttons under the box.

The following ordering rule applies:

The ordering of child fields and their parents depend on the presence of siblings, other parents and children. If a child is selected in a group and not its parent, but a sibling of that parent is selected, then the sibling's order will affect the order of the fields.

The logic of order resolution starts from parents to children, according to the rules below.

For example, we select fields in this order in Group 1:

C.z, A.x.b, A.x.c, B, A.y, A.x, C, C.w

Result:

- Parent fields on their own are considered first, hence our initial order is B, C.
- However, parent A is not selected; only the children. We determine where A was mentioned. In this case the children of parent field A were mentioned before the parent fields B or C. Hence children of A will eventually be ordered before B and C.
- Next we consider the selected first level child fields: C.z, A.y, A.x, C.w. The order becomes: A.y, A.x, B, C, C.z, C.w
- We now move down the levels: A.x.b, A.x.c.

Thus the final display order will be:

A.y, A.x, A.x.b, A.x.c, B, C.z, C.w

Further examples below illustrate the presence of parents, siblings and children on the selected order.

- We add fields C.w, A, C, B, A.x, A.y.

  Result: The order is: A, A.x, A.y, C, C.w, B.
- We add fields A.x.b, A.x.c, A.y, A, B

  Result: The order is: A, A.x, A.x.b, A.x.c, A.y, B.

  Note that A.x was added and that A.y is placed after A.x, since the children were ordered before A.y while A.x was never selected.

14.7.5. Clone a Field Display Policy

1. Login as provider administrator or higher.
2. Choose the desired hierarchy.
3. Choose **Customizations > Field Display Policies** to show the list of existing Field Display Policies.
4. Click on the field display policy that you want to clone.
5. Choose **Actions > Clone**.
6. Update the necessary fields for the cloned Field Display Policy. Refer to "Rules When Creating a Field Display Policy" for more information.
7. Click **Save**.

The cloned Field Display Policy is available to be applied to the item by selecting it in a Menu Layout that is available to a Role.

14.7.6. Add or Edit a Field Display Policy

A Field Display Policy can be added or edited.

1. Login as provider administrator or higher.
2. Choose the desired hierarchy.
3. Choose **Customizations > Field Display Policies** to show the list of existing Field Display Policies.
4. Click **Add** on the button bar to create a new Field Display Policy and enter a new name in the **Name** field. Alternatively, you can edit an existing Field Display Policy by clicking on it and editing the fields as described below. If the name is 'default', the Field Display Policy is applied by default. There is a unique constraint on the name of the Field Display Policy per hierarchy level, so the same name as the original can be used on another hierarchy, but a new name is needed at the same hierarchy.
5. Complete the following field display policy details:
    a. Optionally enter a Description for the Field Display Policy.
    b. Choose the model reference for the **Target Model Type** from the drop-down list.
    c. Click **Add** next to **Groups**, and complete the following:
        - Title - Enter the label text to be shown for the attribute. This is mandatory, and is the name that will be shown on the created tab.
        - Display as Fieldset - Select this check box to make sure that all fields are shown on the same page instead of a separate tab.
        - Number of Columns - Enter the required number of columns. The fields in the 'Selected' area (see Fields below) will be displayed in the number of columns specified in this field. The default is to display the fields in a single column.
        - Fields - Configure the fields that will be displayed on the tab. Choose the fields in the 'Available' area of the screen and click **Select** to move them to the 'Selected' area of the screen. Fields displayed in the 'Available' area are determined by selected Target Model Type. To adjust the position of a field in relation to the other fields, click on a field and use the **Move Up** and **Move Down** buttons.
    d. Click **Add** next to **Field Overrides** and complete the following:
        - Field - Choose the field name from the drop-down for which you want to create override text (a different label).
        - Title - Enter the required label text.
        - Help Text - Enter text to display as the field on-line help and form tool tip for the attribute. If no text is added, the model attribute description is shown.
        - Disabled - Select the **Disabled** check box if you want to hide the field (grey it out).
        - Input Type - Choose the required option from the drop-down to determined how the input field is displayed.
6. Click **Save** on the button bar to save the Field Display Policy.

The created Field Display Policy is available to be applied to the item by selecting it in a Menu Layout that is available to a Role.

14.7.7. Field Display Policy Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Field Display Policy.
Description	description	A description for the Field Display Policy.
Target Type Model *	target_type_model	The target model type to which the Field Display Policy applies.
Groups	groups.[n]	The groups that describe groupings of attributes that are displayed together on the user interfcae.
Title *	title	The name of a specific group of attributes.
Display as Fieldset	display_as_fieldset	Render this group as a fieldset in the form.
Number of Columns	num_cols	The number of columns of fields.
Fields	fields.[n[]	Model fields that will form part of the particular group.
Field Overrides	field_overrides.[n]	Field display policy overrides to apply to a model fields.
Field *	field	Name of the model field to override.
Title	title	New title to display for field.
Help Text	help_text	New help text to display for field.
Disabled	disabled	Will set the field to read-only if checked.
Input Type	input_type	Overrides the input type of the field.

14.7.8. Configuration Templates

Configuration templates are used to define values for attributes of any model. The values can be fixed values or existing macros visible from the hierarchy context where the configuration template is applied. The templates provide a useful way to define default values for items that are exposed in the GUI (visible, invisible or read-only). They also provides a mechanism to map data from data input via the GUI or device model events to other models or Provisioning Workflows in the system.

One may want to hide attributes of a model while setting them to a specific fixed value (for example a hard-coded setting); or one may wish to derive the value based on a macro (for example, look up the value based on data in the system).

For example, if a model has an attribute that is defined to be a date string, a Configuration Template for the attribute can be defined as a macro `{{fn.now \"%Y-%m-%d\"}}` in order to set the current date stamp as the value, such as `2013-04-18`. Designers can access reference material for details on macros.

Another example is a model such as the Quick Add Subscriber that limits the user input to a few fields, whilst deriving the value of other hidden attributes from various Configuration Templates that are each applied to different underlying models that make up a Subscriber (for example, Voicemail account settings, conference account settings, phone, line, device profile settings, and so on).

When an instance of the model is added or updated, the Configuration Template that has been enabled for the model applies. For array elements of data models, a list and a variable can be specified to be looped through so that a value is applied to each element in the model array.

More than one Configuration Template can be created for a model. These can then be used as needed. Configuration Templates can also be applied to models in the design of for example Provisioning Workflows.

A Menu Layout that can be associated with a user role can also apply a Configuration Template to a model that is selected as a menu item.

For administrators at Provider Administrator level or higher, a quick way to create a Configuration Template would be to open a similar template from for example the **Configuration Templates** menu and to customize a clone of it.

Administrators at levels above the Site Administrator can also customize these templates, including Field Display Policies.

Note:

- When modifying Configuration Templates via the GUI, numerical values need to be entered using the `fn.as_int` function, for example:

  ```
  {{ fn.as_int 14 }}
  ```

- In a multi-cluster environment, Configuration Templates that result in device model drop-down lists on the GUI may contain duplicates. Any duplicated item can be selected by the user.

14.7.9. Workflow for Creating Configuration Templates

Procedure

1. Log in as Provider Administrator or higher.
2. Choose **Customizations > Configuration Templates**.

   The list of templates appears.
3. Click the template that you want to clone.

   The template information appears.
4. Click **Action > Clone**.
5. Edit the required generic template fields, such as **Name**, **Description**, **Target Model Type**, as well as the fields specific to the selected model (see “Configuration Template Field Reference” for the generic field descriptions).

   Note: Certain fields only populate choices depending on specific conditions.

   For example, when creating a device instance Configuration Template in a multi device or clustered environment, the values in drop-down fields in the template that originate from a device will be the values from *all* the devices in the cluster. This list could therefore include duplicates, but in such a case, any duplicate may be chosen if required.

   ---

6. Click **Save**.

   The new cloned template appears at the selected hierarchy level.

Example: Create a template for the Cisco 6941 SCCP Phone

1. Enter the hierarchy where the Cisco Unified Communications Manager you want to use exists. This step is required if the fields are to populate values because some of the values are derived from the actual device model through the API.
2. Click the **Default CUCM Phone Template**, and then click **Action > Clone**.

   Note: Do not click **Save** yet.
3. Change the template **Name** and **Description**.
4. Edit the template fields:
   - From the **Device Protocol** drop-down, choose **SCCP**.
   - From the **BAT Phone Template** drop-down, choose **Standard 6941 SCCP**.
   - From the **Device Security Profile** drop-down, choose **Cisco 6941 - Standard SCCP Non-Secure Profile**.
   - From the **Product** drop-down, choose **Cisco 6941**.
   - From the **BLF Presence Group** drop-down, choose **Standard Presence Group**.
   - In the remaining fields, use the cloned default values.

   Tip: If you know the values for the fields, you can type the files in the fields instead of selecting the values from the list.
5. Click **Save**.

14.7.10. Configuration Template Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Configuration Template.
Description	description	A description for the Configuration Template.
Foreach Elements	foreach.[n]	Iterates over the list returned by the macro and appends array elements to the specified field.
Property *	property	The field property to iterate over.
Macro List *	macro_list	The macro that produces the list to iterate over.
Context Variable *	context_var	The context variable that will contain the data from the iteration.
Schema Defaults	schema_defaults.[n]	Applicable only when the configuration template is used directly in API requests. This attribute contains a list of paths to the properties of the template section that must be used to enrich the default values of the schema. All paths specified must refer to array attributes.
Target Model Type *	target_model_type	The target model type and name that the Configuration Template applies to.
Merge Strategy	merge_strategy	Determines how this CFT will be merged into another CFT when it is being processed in a PWF. Default: additive.
Template *	template	The contents of the template, such as defaults and macros. The names shown in the template are determined by the attribute names of the Target Model Type.

14.7.11. Configuration Mapping Files

Phone, device, and line configuration mappings allow a higher level administrator, e.g. BAP Administrator to better manage and control the lists of items available for selection on the GUI, as well as the ability to define the settings and templates used for each item.

Phone Configuration Mapping

The Phone and Device Profile mappings serve a number of purposes. These allow a higher level administrator to:

- Control the list of phone types available for selection.
- Define the configuration settings used when a specific phone type is selected.
- Define a set of “feature” templates that can be selected by the lower level administrator.

Phone Profiles

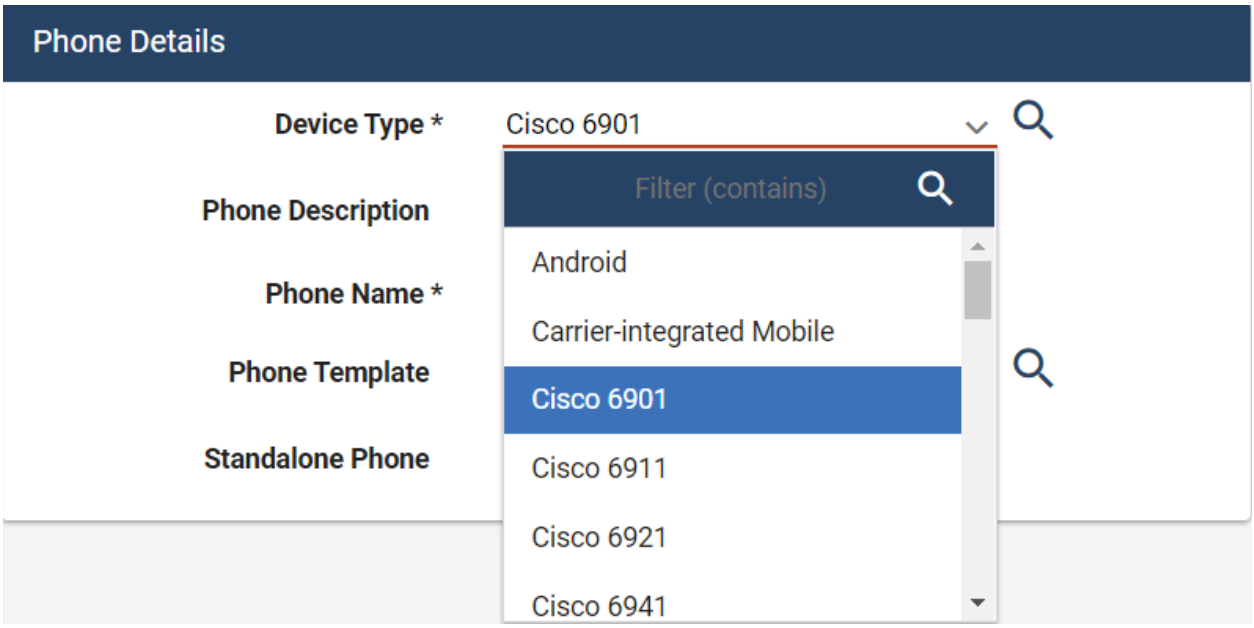
These mapping profiles define a list of phone types that can be selected along with:

- Custom name (profile name) for the phone type
- The actual phone type
- Protocol
- Button Template
- Security Profile
- Configuration Template (CFT)

Profile Name *	Phone Type *	Protocol *	Button Template	Security Profile	Base Configuration Template *
Default (6901)	Cisco 6901	SIP	Standard 6901 SIP	Cisco 6901 - Stand	Basic Phone CFT

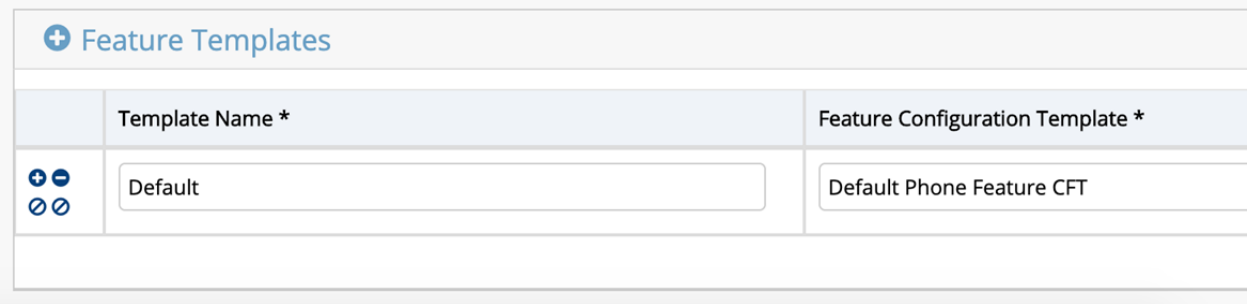
The Profile Name is what will be presented in dropdowns to the lower level administrator inside the Business Admin Portal.

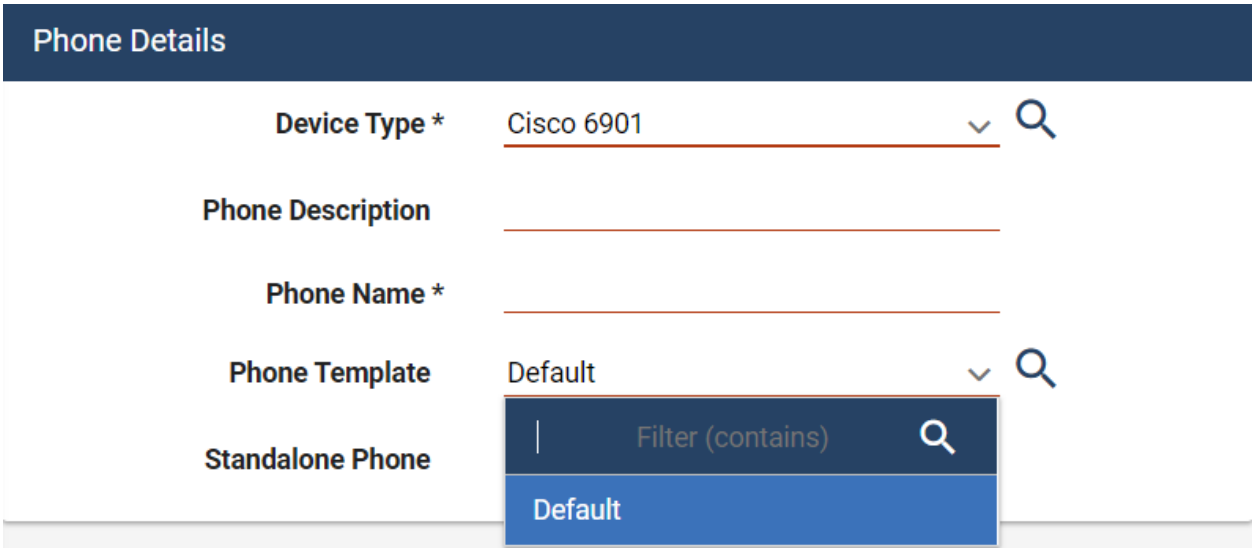
For example, if the administrator selects “Default (6901)”, then the phone will be provisioned as a Cisco 6691 SIP device with Standard 6901 SIP button template and the Cisco 6901 - Standard SIP Non-Secure Profile security profile. Additionally, all configuration captured in Basic Phone CFT will also be used.



Feature Templates

The “Feature Templates” section of the Phone and Device Profile config mapping allows a higher level administrator to configure a list of feature templates. These will be presented to the BAP administrator user for selection when adding a Phone or Extension Mobility and will contain configuration settings that is applied on top of the settings mentioned above.





Configuration Template Input Contexts

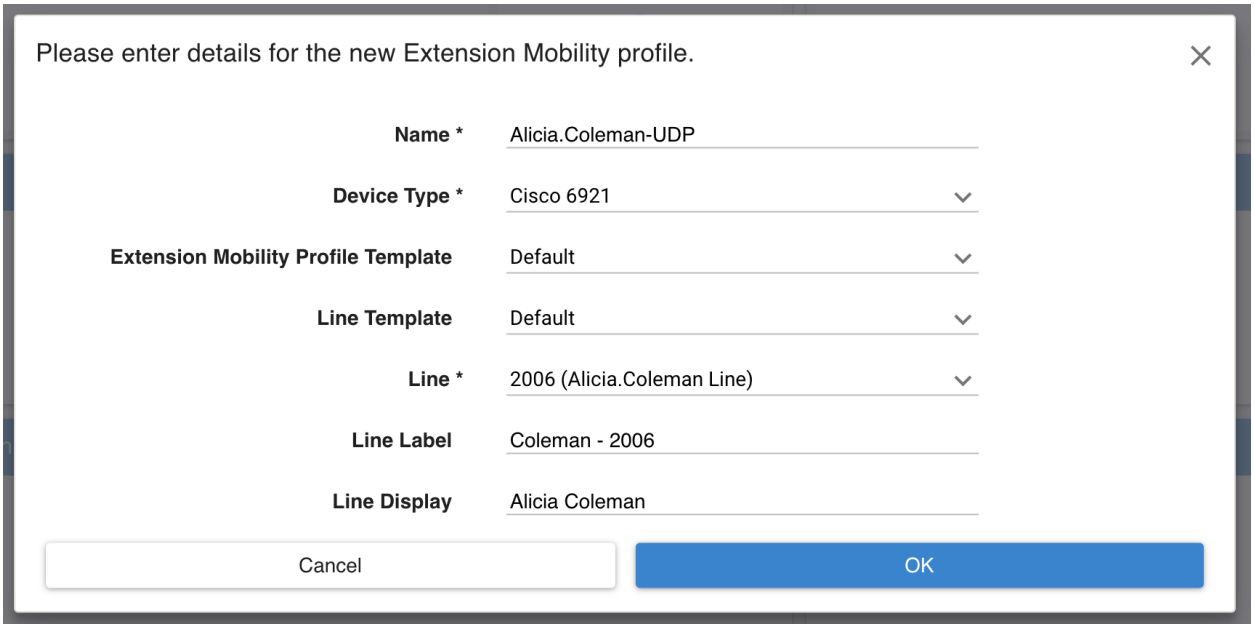
The following context macro variables are available when defining configuration templates for the phone mappings above.

Macro	Description
`{{ input.standalone }}`	Flag whether it is a standalone phone or being associated with a Subscriber.
`{{ input.username }}`	Username of the Subscriber the phone is being associated with. Only when standalone is false.
`{{ input.device_type }}`	The user selected device type. This in fact is the Phone mapping profile name.
`{{ input.template_name }}`	The user selected feature template.
`{{ input.name }}`	The user entered phone name.
`{# input.lines #}`	The user entered list of lines.
`{{ input.lines.0. directory_number }}`	The number of the first line.
`{{ input.lines.0. template_name }}`	The user selected Line template.
`{{ input.lines.0.label }}`	The user entered line label.
`{{ input.lines.0.display }}`	The user entered line display.
`{{ pwf.user }}`	Object containing all UCM user settings of the associated subscriber. Only when standalone is false.

Device Profile Configuration Mapping

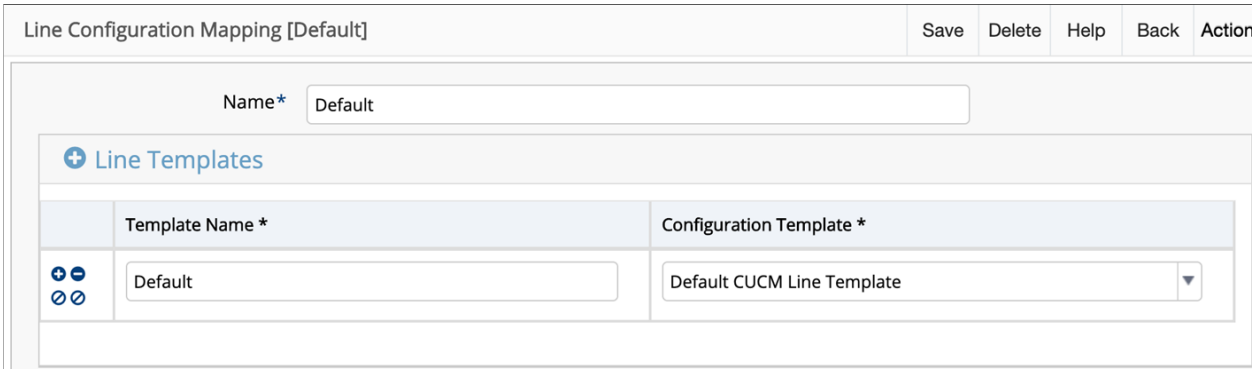
The setup for Device Profile configuration mapping is identical to that for Phone Configuration Mappings.

The phone type list and feature templates are presented to the BAP administrator when adding an Extension Mobility service on the Subscriber management dashboard.



Line Templates

A list of line templates can be configured and these will be presented to the BAP administrator when new lines are be created, for example when adding a new phone.



14.7.12. Dropdown Filters

Administrators with access to the **Dropdown Filters** menu can manage the items available in dropdown lists on input forms. A filter would typically be used to define a shorter dropdown list.

Filters can be added, removed, modified and two existing filters can also be merged to define a new filter.

The Dropdown Filter list macro name that is generated starts with `DDF__` and is of the format (dots and slashes replaced by underscores):

`DDF__<target model type> _<target model name>_<target field>`

This is also the name shown in the **Dropdown Filters** list view at the hierarchy at which is was created.

Add a Dropdown Filter

1. Navigate to the required hierarchy.
2. Select the **Dropdown Filters** menu and click **Add**.
3. Choose **Create a Dropdown Filter** From the **Select a Dropdown Filter Action** dropdown list.
4. Choose the **Target Model** and **Target Field** names to which the filter is to be applied.

   This is the dropdown field on an input form on the GUI. Click **Help** on the input form to see the names.
5. Identify the associated **Model Type** and **Dropdown Field** of the **Dropdown Filter specifications**.

   This can differ from the form names. Click **Help** on the input form to verify.
6. Set up the **Filter Fields**. Compare a **Filter Field** to a **Filter Field Value**:
   - contained in or not contained in
   - equal or not equal

   Note that:
   - The **Filter Field** can differ from the **Target Field**. In other words, the dropdown list can be filtered according a filter applied to *another* field that belongs to the **Model Type**.
   - The **Filter Field value** can also take the *name* of a named macro that resolves to a value, for example: `macro.SITENAME`.

7. Add **Additional Parameters** to the filter:
   - direction:hierarchy direction for search: [up|down|local|parent|below|above] (`below` and `above` exclude current hierarchy)
   - device: device name
   - ndl: network device list that the device belongs to
   - limit: number of results
   - skip: start number of results - can be used for paging
   - title: character or regular expression: only return values matching its value

   For details and examples, refer to the topics on macro syntax in the Advanced Configuration Guide.
8. Click **Save**. A dropdown filter is created.

   This filter is a named list macro that will be added to the GUI Rule which is in place at the selected hierarchy for the **Target Field** on the GUI input form of the selected **Target Model Name**.

When a created dropdown filter is opened, the macro is shown in the **Macro** field at the bottom of the form. Users who have menu access to the list of named macros can also see the dropdown filter macros by filtering the list by name starting with `DDF__`.

Example of a Dropdown Filter

Consider the filter:

- **Target Model Name**: `relation/LineRelation`
- **Target Field**: `callForwardAll.callingSearchSpaceName`
- **Model Type**: `device/cucm/Css`
- **Dropdown Field**: `name`
- **Filter Field**: `name`
- **Filter Condition**: `Contains`
- **Filter Field Value**: `Cu2`
- **Additional Parameter**: **Parameter Title**: `Direction`
- **Additional Parameter**: **Parameter value**: `up`

The list macro that is created applies to the GUI rule for the input field `callForwardAll.callingSearchSpaceName` of the input form for `relation/LineRelation` at the selected hierarchy. The list macro would then be:

```
{# device/cucm/Css | name /Cu2/i | direction: up #}
```

If you have access to the Macro Evaluator, you can test this macro. Also refer to the topic on Macro Syntax in the Advanced Configuration Guide for more details.

In the **Dropdown Filters** list view at the hierarchy, the **Filter Name** shows as:

`DDF__relation_LineRelationTarget_callForwardAll_callingSearchSpaceName`

Merged Dropdown Filters

Two existing dropdown filters can be merged to create a new dropdown filter. The merged filter is a dropdown list that uniquely combines the lists from the two dropdown filters.

Merge Dropdown Filters

1. Navigate to the required hierarchy.
2. Select the **Dropdown Filters** menu.

   Check that the two dropdown filters that you want to merge are showing in the list view at the hierarchy. Otherwise, add the dropdown filters.
3. Choose **Merge Existing Dropdown Filters** from the **Select a Dropdown Filter Action** dropdown list.
4. Choose the **Target Model** and **Target Field** names to which the filter is to be applied.
5. Choose the two dropdown filters from the **Dropdown Filters to merge** form.
6. Click **Save**. A merged dropdown filter is created.

Note: Only two filters can be merged.

If you wish to merge more than two dropdown filters, first create a merged filter of each filter pair and select it to be merged.

When a created merged dropdown filter is opened, the macro is shown in the **Macro** field at the bottom of the form. The macro uses the `fn.list_extend_no_dup` macro function to uniquely merge the two dropdown filter lists. The macro syntax is of the format

```
{{ fn.list_extend_no_dup macro.DDF__<filter name 1>, macro.DDF__<filter name 2> }}
```

Refer to the topic on Macro Syntax and List Functions in the Advanced Configuration Guide for more details.

14.7.13. Line Delete Preferences

When deleting a phone, device profile or remote destination profile from VOSS-4-UC, the line or lines (Cisco Unified CM lines) in use by the phones or devices are not automatically deleted.

Line Delete Preferences provides the ability, for a reseller administrator (or higher) to control whether the lines are deleted when deleting the phone or device, or updated (using values contained in a specified configuration template).

A new menu (default = **Customizations > Line Delete Preferences**) allows the configuration of the following:

- Allow deletion of a line
- Allow update of a line
- Configuration template to use for update (if enabled)

When:

- a phone, device profile or remote destination profile is deleted
- a line is deleted or changed from a phone, device profile or remote destination profile

then the following logic applies:

Allow Line Deletion if unused

- If the line is not shared with another phone or device, the line will be deleted and the number inventory updated.
- If the line exists on another phone belonging to the same user as the deleted device, no action is taken.

Allow Line Update after Device Deletion

- If the line is not shared with another phone or device, the line is updated with the details from the selected configuration template.
- If the line is shared with another phone or device belonging to another user, the line is updated with the details from the selected configuration template specified in **Line Update Configuration Template name**.
- If the line is shared with another phone or device belonging to the same user, then no update is performed.

Note: To determine the user associated with a phone, the owner ID must be set on the deleted phone.

Affected Models

- Model Type: device/cucm/Phone
  - Operation: Delete
  - Phase: Post Execution
  - Workflow: LineDeletion_PhoneDataSync_PWF
  - Synchronous: False
- Model Type: device/cucm/DeviceProfile
  - Operation: Delete
  - Phase: Post Execution
  - Workflow: LineDeletion_PhoneDataSync_PWF
  - Synchronous: False
- Model Type: device/cucm/RemoteDestinationProfile
  - Operation: Delete
  - Phase: Post Execution
  - Workflow: LineDeletion_PhoneDataSync_PWF
  - Synchronous: False

14.7.14. SMTP Server

A SMTP server can be configured at a hierarchy to allow for email messages to be sent from VOSS-4-UC. This functionality is available in:

- Quick Add Subscriber - a check box becomes available on the input form if enabled in **Global Settings** on the **Email** tab. See the Advanced Configuration Guide.

- File Transfer Destinations that can be configured by high level system admininistrators to transfer audit data for licensing. See the Advanced Configuration Guide.

Input the SMTP server details on the input form.

Note:

- Only one SMTP server can be set up at a hierarchy.
- If a SMTP server is configured on a level above a hierarchy, this server will be used.

14.7.15. Email

Provider administrators can test email messages and manage email templates if an email SMTP server is set up and the setting is enabled in **Global Settings**. See: *SMTP Server* and *Global Settings*.

Send Test Email

This option allows for an email message to be sent from and to a specified email address and by selecting an email HTML template to test in the email body.

Email HTML Templates

Email templates contain placeholders for the email subject and body text, which is in HTML markup. The HTML markup and can be modified as required (for example by using an external WYSIWYG HTML editor).

To modify a template for a specific hierarchy, clone the default to the hierarchy.

When adding a HTML template from the list view, the **Name** can only be “Test Email Template” or “Quick Add Subscriber”.

By default, the following email templates are provided:

- Test Email Template
  - Clone this template to your hierarchy if you want to customize it.
  - The HTML template name “Test Email Template” cannot be changed.
- Quick Add Subscriber
  - This template is used if the setting is enabled in **Global Settings**.
  - Clone this template to your hierarchy if you want to customize it.
  - The HTML template name “Quick Add Subscriber” cannot be changed.

Values from the Quick Add Subscriber input form can be used to populate the template by adding variables to the HTML template. The following variables are available for the template:

Field name on input form	Variable available in HTML
Username:	`{{ pwf.EMAIL.username }}`
First name:	`{{ pwf.EMAIL.firstname }}`
Last name:	`{{ pwf.EMAIL.lastname }}`
One time password:	`{{ pwf.EMAIL.password }}`
One time PIN:	`{{ pwf.EMAIL.pin }}`
Email:	`{{ pwf.EMAIL.email }}`
Extension:	`{{ pwf.EMAIL.extension_number }}`
Mobile Number:	`{{ pwf.EMAIL.mobile_number }}`
Entitlement Profile:	`{{ pwf.EMAIL.entitlement_profile }}`
Phone Type:	`{{ pwf.EMAIL.phone_type }}`
Phone Names:	`{{ pwf.EMAIL.phone_names }}`
Jabber Device Names:	`{{ pwf.EMAIL.jabber_names }}`

Therefore, you can for example include user details as follows in your HTML template:

```
<p>Username: {{ pwf.EMAIL.username }}</p>
<p>First name: {{ pwf.EMAIL.firstname }}</p>
<p>Last name: {{ pwf.EMAIL.lastname }}</p>
```

14.8. Authentication Management

14.8.1. User Authentication

When logging in to the user interfaces, the credentials of the user can be authenticated based on user credentials in:

- The internal system database
- An LDAP-based external authentication server
- A SAML-based identity management server

Administrator users are users that are able to log in to the administrator interface. Presence of an administrator interface means that a system user instance exists.

Subscribers are system users that have, and are linked to, user accounts in one or more UC applications. Subscriber management supports the management of UC application user accounts that in turn may also be configured for local, LDAP or SAML authentication.

API users are system users that connect directly to VOSS-4-UC using the API. The system controls access to its service through HTTP basic authentication.

14.8.2. Credential Policies

VOSS-4-UC helps secure user accounts by authenticating user sign-in credentials before allowing system access. Administrators can specify settings for, among other things, failed sign-in attempts, lockout durations,

password reset questions, and so on. The number of questions in the Password Reset Question Pool must be equal to (or more than) the number set in the Number of Questions Asked During Password Reset field. Collectively, these rules form a credential policy, which can be applied at any hierarchy level, and determine user sign-in behavior at that specific level.

A credential policy is not mandatory at specific levels in the hierarchy. However, a default credential policy is provided at the sys.hcs level. Administrators at lower levels can copy and edit this default policy if necessary. Administrators can also save it at their own hierarchy level so that it can be applied to the associated users at that level. If the administrators at the various levels do not create a credential policy at their level, it is inherited from the closest level above them. If a Provider Administrator has defined a credential policy, but a Customer Administrator has not, the customer automatically inherits the credential policy from the Provider. A different credential policy can also be defined for each user.

For each administrator user where IP address throttling (sign-in Limiting per Source) is required, manually create and assign a credential policy. The credential policy must have IP address, and username and email throttling enabled.

The default credential policy is defined at the sys.hcs level.

Note: Credential Policies are not applicable for SSO authenticated users. For LDAP Synched users, only the session timeouts are applicable.

14.8.3. Standard Users and Login

When creating a system user that uses the standard authorization method, the password is stored in the internal system database. VOSS-4-UC uses the PBKDF2 algorithm with an SHA256 hash, a key stretching mechanism recommended by the National Institute of Standards Technology (NIST), Computer Security Resource Center (CSRC).

When logging in as a standard user, go to the URL:

`https://{hostname}/login`

A log in page theme can be applied to the log in page during the log in process by adding the suffix `?theme={theme_name}` where `{theme_name}` is an available theme. For example:

`https://{hostname}/login/?theme=default`

When logging in, the username can be entered in either of the following formats:

`{username}@hierarchy` or `{email address}`

The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

The hierarchy on the log in form is prefixed with `sys`.

For example: `johndoe@sys.VS-OPS.VS-Corp.Chicago`

14.8.4. LDAP Users and Login

When creating a system user using the LDAP authorization method, specify the LDAP server and the LDAP username. The LDAP username corresponds to the log in Attribute Name specified in the LDAP network connection.

When logging in as an LDAP user, go to the URL:

`https://{host name}/login`

Regardless of the log in Attribute Name specified in the LDAP network connection, the user email address can be used to log in.

When logging in with LDAP credentials, the username is in the format:

`{user ID}[@hierarchy]`

Note:

- `@hierarchy` is not required when the user ID corresponds to the user's email address.
- `{user ID}` corresponds to the log in attribute name (for example email address, user principal name, sAMaccountName). The log in attribute name is configured in the Authentication attribute of the LDAP device connection associated with this hierarchy.
- The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

14.8.5. SSO Users and Login

When creating a system user using the SSO authorization method, the SSO Identity Provider must be specified and the SSO username.

When logging in as an SSO user, go to the URL:

`https://{host name}/sso/{SSO login URI}/login`

For example:

`https://host.Agency1.CustomerA.com/sso/CustomerA/Agency1/login`

This URL format also applies to self-service users.

Log in using the relevant SSO identity provider credentials.

14.9. Subscriber and User Synchronization

14.9.1. Subscriber and User Synchronization: Overview

Users that have been pushed to Cisco Unified Communications Manager are synchronized between the Subscriber Management and User Management functions of VOSS-4-UC. An addition, update, or deletion of a user in one place is automatically reflected in the other.

Subscribers and Default Entitlement Profiles

New users added to VOSS-4-UC using Subscriber Management are checked for entitlement against the nearest default entitlement profile located above the site where the user is being added. If no default entitlement profile exists, the user is not restricted. If a default entitlement profile is found, and the user being added has devices or services to which the user is not entitled based on the default entitlement profile, the user add will fail.

14.10. Self Service

14.10.1. Self Service: Overview

Using the VOSS-4-UC Self Service interface, users can configure their own phone settings, including voicemail, call forwarding, availability, and speed dials.

To access the Self Service interface, a user must be assigned a SelfService role in VOSS-4-UC. A user may get a SelfService role in one of the following ways:

- Automatically when synced from LDAP, if the LDAP Sync has the User Role configured to a SelfService role.
- By default when synced from Cisco Unified Communications Manager.
- Manually assigned by an administrator using **User Management > Users**.

To access the Self Service interface, the user enters https://<service-ip-or-node-name>/selfservice/#//login?theme=cisco_selfservice in the browser URL field.

Note: Access to the Self Service interface and the VOSS-4-UC Administrative GUI are mutually exclusive. Therefore, if an administrator needs access to the Self Service interface, the administrator needs a second user configured in VOSS-4-UC with a SelfService role assigned to it.

14.10.2. Self-Service and User Configuration

As an Administrator, you can:

- Configure various aspects of the Self-Service interface
- Provide user access to Self-Service
- Configure services for the users as required

This table provides a summary of the configurable items for the Self-Service interface.

Configurable Items in Self-Service Interface

Task or Item	Description
User access	A user can log in to the Self-Service GUI if a 'System User' entry exists for the user. A 'System User' entry is created automatically when a user is added as a subscriber. You can grant a user access to Self-Service by creating a user with a **Self-Service** role directly in the System user interface. A user with this role is not able to view devices or any services associated with the devices. Manually added users also cannot view personal information such as first name, last name, address, department, etc.
User Authentication	Self-Service authentication is controlled by the administration interface using the same three authentication methods: **Standard**, **LDAP**, and **SSO**.
GUI Themes and Branding	The Self-Service GUI interface can be branded by configuring Cascading Style Sheets and images and logos. It uses the same theme upload and download interface used for the administrator GUI. The theme itself however, is different between the administrator and Self-Service interface (based on the user role). The log in page theme is also loaded from the URL: https://<host>/selfservice/#/login?theme=mytheme
Personal Phones (Remote Destinations)	You can automatically assign a remote destination profile (RDP) to a user so that they can manage their own personal phones and simultaneous ring settings. Select the **User can enable Personal Phone Management (add Remote Destination Profile)** check box on the **Personal Phones** tab under **Customizations > Self Service Feature Display Policy** If no RDP is associated to the user, the Personal Phones management interface in self-service is hidden. Multiple RDPs for each user are not supported. The Personal Phones management interface in Self-Service is also hidden if a user has more than one RDP associated.

For more information, see:

- *Add Subscribers*
- *Create and Update a User*
- *User Authentication*
- *Download and Update a Theme*
- *Create a Custom Self-Service Role*

Task or Item	Description
Dual-Mode Phones - Mobile ID	If a user has a dual-mode device associated, they can manage the phone number and simultaneous ring settings for the device. If no dual-mode device is associated, the relevant settings are hidden in the Self-Service interface.
Voicemail	Voicemail settings are only visible in the Self-Service interface if the user has a voice mailbox. Click the **Voicemail** tab of **Customizations > Self Service Feature Display Policy** to set voicemail settings, notification devices, and SMS Interfaces.
Passwords and PINS	Users can modify their own Passwords and PINs if the Self-Service Feature Display Policy is set to 'Show' these items. Click the **My Information** tab of **Customizations > Self Service Feature Display Policy** to change this setting.
Link to a WebEx server	Users have a link to their WebEx server from the Self-Service interface if this item is set to 'Show'. Click the **My Information** tab of **Customizations > Self Service Feature Display Policy** to change this setting.
Hyperlinks to predetermined objects or items such as a support site or downloadable User Guide	As the administrator, you specify the hyperlinks that appear in the Self-Service interface. Refer to the VOSS-4-UC "Self-Service Guide".
Call Forwarding	Displays the call forwarding status of a user's phone lines. You can specify whether Basic or Advanced call forwarding is set to 'Show' in the Self-Service interface. Click the **Call Forward** tab of **Customizations > Self Service Feature Display Policy** to change this setting.

For more information, see:

- *Configure Phones*
- *Voicemail: Overview*
- *Create a Custom Self-Service Role*

14.10.3. Create a Self-Service Link

1. Navigate to the required hierarchy.
2. Click **Add** and enter a Name for the set of links.
3. Enter one or more Description and Link. The Description will display on the Self-Service GUI. The Link is in the format of a URL, for example: `http://...`

15 Dial Plan Management

15.1. Dial Plan Overview

15.1.1. Overview

VOSS-4-UC Provider solution supports the HCS dialplan tools as described in this chapter.

Optionally, VOSS-4-UC also supports a next generation dial plan as described in Appendix: Optional Features of this guide. This optional dial plan is independent of the hierarchy schema approach of the first generation dial plan. However, it can also be used in conjunction with schema-based dial plan management.

15.2. Dial Plan Workflow

15.2.1. Dial Plan Example Workflow

Dial plan procedures available in VOSS-4-UC are found in this section. However, additional procedures and more detailed information about dial plans can be found in the “Provider HCS Dial Plan Management Support Guide”.

Procedure

1. Optionally, deploy country dials plans for countries other than United States or United Kingdom. See the “Provider HCS Dial Plan Management Support Guide”.

   If you are using country dial plans other than US or UK, you must complete this step before continuing to the next step.
2. Apply customer dial plan at customer.
3. Apply site dial plan at site.
4. Optionally, configure Class of Service at site.
5. Add Directory Number Inventory at customer or site.
6. Optionally, configure E.164 Inventory at customer or site.
7. Optionally, configure E.164 Number to Directory Number associations at customer or site.
8. If not using Site Location Codes (that is, you have deployed a Type 4 Dial Plan), configure Directory Number Routing at site to enable intra- and inter-site calls.

9. Optional, configure Short Codes at site.
10. Edit Site Defaults as follows:
    a. On the **Device Defaults** tab, set the Default VOSS-4-UC Device CSS to an appropriate device Class of Service.
    b. On the **Line Defaults** tab, set the Default CUCM Line CSS to an appropriate line Class of Service.
11. For offnet PSTN call configuration, see the “Provider HCS Dial Plan Management Support Guide”.
12. For Local Breakout (LBO) configuration, see “IOS Device Management”.
13. For user, phone, and line configuration, see “Subscriber Management”.

15.2.2. 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 modify.

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*.

15.2.3. Create a Site Dial Plan

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.

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
   - 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.

15.2.4. Update a Site Dial Plan

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:

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**.

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.

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.

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

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.

What to Do Next

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

15.2.5. 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.

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**.
   - 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.

15.2.6. 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

15.2.7. 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.

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.
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.

15.2.8. Configure Short Code

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.

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:

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.

15.3. Number Management

15.3.1. 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.

15.3.2. 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.
  - 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.

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.

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.

15.3.3. 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:

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**.

15.3.4. View E.164 Number Inventory

Use this procedure to view the inventory of E.164 numbers.

Note: In VOSS-4-UC, the country associated with the E.164 number is displayed.

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to limit the scope of E.164 numbers being viewed.
3. Choose **Dial Plan Management > Number Management > E164 Inventory**.

   A table containing this information is displayed:

Column	Description
E164 Number	The individual E.164 number in the inventory.
Country	The country associated with the E.164 number.
Associated Flag	Indicates the E.164 number has been associated with a Directory Number
Hierarchy	Indicates the hierarchy of the site the E.164 number was created for.

15.3.5. Delete E.164 Numbers from the Inventory

Use this procedure to delete numbers from the E.164 inventory.

Note: You cannot delete E.164 numbers that are associated with a Directory Number.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to limit the scope of E.164 numbers being deleted.
3. Choose **Dial Plan Management > Number Management > E164 Inventory**.
4. Perform one or both of these options:
   - To delete one number, click the number, then click **Delete**.
   - To delete multiple E.164 numbers, select the check box next to each number you want to delete, then click **Delete**. Use column filtering to narrow and refine the list of items to select for a batch delete.
5. Click **Yes** in the confirmation window.

15.3.6. 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.
- 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.

15.3.7. 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.

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.

   - `\+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

15.3.8. 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)**.

   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.

15.3.9. Number Cooling

Pre-requisites

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

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).

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.

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*

15.3.10. 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)

15.3.11. Delete Site Directory Numbers

Use this procedure to delete one or more directory numbers at a site. You can bulk delete all directory numbers at a site using this procedure, or you can delete all directory numbers at a site automatically when you delete the site.

Procedure

1. Log in at any level. Select an available site from the hierarchy node breadcrumb at the top of the view if you are not at the Site level.
2. Choose **Dial Plan Management > Number Management > Directory Number Inventory**.
3. From the list of directory numbers, choose the directory number(s) to be deleted, by clicking on one or more check boxes in the leftmost column. To bulk delete all directory numbers at the site, select the check box at the top of the leftmost column. 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 for deletion.
4. Click **Delete** to delete the directory number(s).
5. From the popup window, click **Yes** to confirm the deletion. When the delete action is complete, the directory number(s) disappears from the list.

15.3.12. 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:

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.

15.3.13. View the Ranges of E.164 Numbers Associated with a Range of Directory Numbers

Use this procedure to view the ranges of E.164 numbers that are associated with a range of Directory Numbers (DNs).

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the site where the E.164 numbers and DNs are associated.
3. Choose **Dial Plan Management > Number Management > E164 Associations (N to N DN)**.

   A table containing this information is displayed:

Column	Description
E164 Number	The starting E.164 number in the range
DN Number	The starting DN in the range
Range	One of the following: • 1 - To indicate that one E.164 number and DN are associated. • 10 - To indicate that a range of ten numbers including the starting E.164 and starting DN are associated. • 100 - To indicate that a range of 100 numbers including the starting E.164 and starting DN are associated. • 1000 - To indicate that a range of 1000 numbers including the starting E.164 and starting DN are associated.
Hierarchy	Indicates the hierarchy of the site where the E.164 number range and DN range association was created

15.3.14. Disassociate a Range of E.164 Numbers from a Range of Directory Numbers

Use this procedure to disassociate a range of E.164 numbers from a range of Directory Numbers (DNs).

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

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the site where the E.164 numbers and DNs are associated.

3. Choose **Dial Plan Management > Number Management > E164 Associations (N to N DN)**.

   An E164 Associations (N to N DN) table containing this information is displayed:

Column	Description
E164 Number	The starting E.164 number in the range
DN Number	The starting DN number in the range
Range	• 1 - To indicate that one E.164 number and DN are associated • 10 - To indicate that a range of ten numbers including the starting E.164 and starting DN are associated • 100 - To indicate that a range of 100 numbers including the starting E.164 and starting DN are associated • 1000 - To indicate that a range of 1000 numbers including the starting E.164 and starting DN are associated
Hierarchy	Indicates the hierarchy of the site where the E.164 number range and DN range association was created

4. Perform one of these options:
   - To disassociate multiple ranges, select the check boxes in the far left column of the table, for the ranges you want to disassociate.
   - To disassociate one range, click its row in the table. The details about the association appear.
5. Click **Delete**.
6. Click **Yes** to confirm the disassociation.
   - The translation pattern mapping between the E.164 range and DN range is deleted from Cisco Unified Communications Manager.

     The E164 number association with the DN Number will be removed on the Directory Number list view display and in any Lines drop-down list and Lines displays.
   - If the site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwDelE164AssociationEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

15.3.15. 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.

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 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.

15.3.16. View the Sets of E.164 Numbers Associated with One Directory Number

Use this procedure to view the sets of E.164 numbers that are associated with one Directory Number (DN).

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the site where the DN and E.164 numbers are associated.
3. Choose **Number Management > E164 Associations (N to 1 DN)**.

   A table containing the following information is displayed:

Column	Description
DN Number	The associated DN.
Hierarchy	The hierarchy of the site where the E.164 number range and DN association was created.

4. Click a DN in the table to select it.

   Details about the sets of E.164 numbers that are associated with the DN appear in read-only format.

15.3.17. Disassociate a Set of E.164 Numbers from a Directory Number

Use this procedure to disassociate a set of E.164 numbers from a Directory Number (DN). When you disassociate a set of E.164 numbers from a DN, multiple translation patterns are deleted. In other words, for each association you delete, a translation pattern is deleted from Cisco Unified Communications Manager.

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

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy path to the site where the E.164 numbers and DN are associated.
3. Choose **Dial Plan Management > Number Management > E164 Associations (N to 1 DN)**.

   An E164 Associations (N to 1 DN) table containing the following information is displayed:

Column	Description
DN Number	The DN number
Hierarchy	Indicates the hierarchy of the site where the E164 number range and DN range association was created

4. Perform one of the following:
   - To disassociate multiple associations, click the check box in the far left column of the table, beside the numbers you want to disassociate.
   - To disassociate one association, click its row in the table. The details about the association appear.
5. Click **Delete**.
6. Click **Yes** to confirm the disassociation.
   - The translation pattern mapping between the E.164 set and the DN is deleted from the Cisco Unified Communications Manager.

     The E164 number association with the DN Number will be removed on the **Directory Number** list view, and in any **Lines** drop-down list and **Lines** displays.
   - If the site has one or more SIP Local Gateways associated with it, the HcsSipLocalGwDelMultiE164AssociationEVT event is generated. If enabled, the IOS Command Builder generates the default IOS commands associated with the event for each SIP Local Gateway.

15.3.18. Migrate Translation Patterns for E.164-to-DN Associations

Use this procedure if you manually configured the Translation Patterns in the E164Lookup partition to associate E.164 numbers to directory numbers for DDI routing. We recommend that you migrate your existing Translation Patterns to use the E.164-to-DN Association feature for VOSS-4-UC.

Note: Perform this procedure only once. For example, if you performed this procedure when you upgraded to VOSS-4-UC, do not perform it again when upgrading to a later VOSS-4-UC release.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Add the appropriate E.164 inventory at **Dial Plan Management > Number Management > Add E164 Inventory**.
3. View the E.164 number inventory: **Dial Plan Management > Number Management > E164 Inventory**.
4. Verify that the selected DN inventory is available for association: **Dial Plan Management > Number Management > Directory Number Inventory**.
5. Remove the previously added Translation Patterns: **Device Management > CUCM > Translation Patterns**.
6. Create the appropriate E.164-to-DN associations: **Dial Plan Management > Number Management > E164 Associations (N to N DN)**. These associations restore the appropriate Translation Patterns in the E164Lookup partition for the selected customer.

7. View the new Translation Pattern: **Device Management > CUCM > Translation Patterns**.

15.4. Cisco Shell Schema Groups

15.4.1. 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.

15.5. Configure Cisco Unified Communications Manager Translation Patterns

15.5.1. How to Configure Cisco Unified Communications Manager Translation Patterns

Introduction

Sometimes it may be necessary to update the default dial plan translation patterns that are deployed as part of the default dial plan schemas that are delivered with the VOSS-4-UC template package. For example, you may want to make your default national number translation patterns more restrictive. Also, you could deploy additional translation patterns that are specific to a customer deployment. For example, you could add customer-specific blocking patterns that are not defined in the standard country dial plan schema.

Caution: The Cisco HCS default dial plan includes most common translation and route patterns. These translation and route patterns are usually added automatically when a customer dial plan, site dial plan, and voice mail service is provisioned. If you want to update translation and route patterns using VOSS-4-UC, you must have a full understanding of the Cisco HCS dial plan. Refer to the "Provider HCS Dial Plan Management Support Guide".

Use this procedure to update Cisco Unified Communications Manager (Unified CM) translation patterns that are provisioned by the dial plan schema or to add new translation patterns from VOSS-4-UC that are not part of the standard dial plan package. For more information on Unified CM translation patterns, refer to "Cisco Unified Communications Manager Administration Guide, Release 10.0(1)".

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the node where you want to add or edit the translation pattern.
3. Perform one of:
   - If you are signed in as provider or reseller administrator, choose **Device Management > CUCM > Translation Patterns**.
   - If you are signed in as customer administrator, choose **Device Management > Advanced > Translation Patterns**.
4. Perform one of:
   - To add a new translation pattern, click **Add**, then go to Step 5.
   - To edit an existing translation pattern, click on the pattern to be updated and go to Step 6.
5. From the **CUCM** drop-down menu, choose the hostname, domain name, or IP address of the Cisco Unified Communications Manager to which you want to add the translation pattern.

   Note:

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

   Important:

   If you are adding or editing a translation pattern at any hierarchy node above a site level, the only Unified CMs that appear in the **CUCM** drop-down list are Unified CMs that are located at the node where you are adding the translation pattern, and all Unified CMs in hierarchies above the node where you are adding the translation pattern. If you are adding or editing a translation pattern at a site level, the Unified CM that appears in the **CUCM** drop-down list is the Unified CM in the site's Network Device List (NDL). If the site does not have an NDL, or the NDL at the site does not have a Unified CM, then the drop-down list is empty and a translation pattern cannot be added to the site.
6. In the **Translation Pattern** field, enter a unique name for the translation pattern, or modify the existing name of the translation pattern if desired. You can include numbers and wildcards (do not use spaces), in the **Translation Pattern** field. For example, enter 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +. This field is mandatory.
7. In the **Partition** field, enter a unique name for the route partition, or modify the existing name of the partition if desired. This field is mandatory.
8. In the **Description** field, enter a description for the translation pattern and route partition if desired. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).

9. Complete at minimum, the mandatory fields on each tab as appropriate (see below):

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

10. Click **Save** when complete to save the new or updated translation pattern.

Translation Patterns: Pattern Definition Fields

Option	Description
MLPP Precedence *	From the drop-down menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this translation pattern: • Executive Override - Highest precedence setting for MLPP calls. • Flash Override - Second highest precedence setting for MLPP calls. • Flash - Third highest precedence setting for MLPP calls. • Immediate - Fourth highest precedence setting for MLPP calls. • Priority - Fifth highest precedence setting for MLPP calls. • Routine - Lowest precedence setting for MLPP calls. • Default - Does not override the incoming precedence level but rather lets it pass unchanged. Default: Default Corresponding Unified CM Attribute: MLPP Precedence.
Route Class *	From the drop-down menu, choose a route class setting for this translation pattern: • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data The route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. The Default setting uses the existing route class of the incoming call. You can use non-default route class settings to translate an inbound T1 CAS route class digit into a Unified CM Cisco Unified Communications Manager route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration. If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class. Default: Default Corresponding Unified CM Attribute: Route Class.
Calling Search Space	From the drop-down menu, choose the calling search space for which you are adding a translation pattern, if necessary. Default: None Corresponding Unified CM Attribute: Calling Search Space.

Option	Description
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call, select the Use Originator's Calling Search Space check box. If the originating device is a phone, the originator's calling search space is a result of device calling search space and line calling search space. Whenever a translation pattern chain is encountered, for subsequent lookups Calling Search Space is selected depending upon the value of this check box at current translation pattern. If you select the Use Originator's Calling Search Space check box at current translation pattern, then originator's Calling Search Space is used and not the Calling Search Space for the previous lookup. If you clear the Use Originator's Calling Search Space check box at current translation pattern, then Calling Search Space configured at current translation pattern is used. Default: Clear Corresponding Unified CM Attribute: Use Originator's Calling Search Space.
Block this pattern	Indicates whether you want this translation pattern to be used for routing calls (such 8[2-9]XX) or for blocking calls. Default: Clear (meaning translation pattern is used for routing calls). Corresponding Unified CM Attribute: Block this pattern.
Block Reason	If you click Block this pattern radio button above, you must choose the reason that you want this translation pattern to block calls. From the drop-down menu, choose one of: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded Default: No Error Corresponding Unified CM Attribute: <entry box next to Block this pattern>.
Provide Outside Dial Tone	Outside dial tone indicates that Unified CM routes the calls off the local network. Select this check box for each translation pattern that you consider to be off network. Default: Selected Corresponding Unified CM Attribute: Provide Outside Dial Tone.
Urgent Priority	If the dial plan contains overlapping patterns, Unified CM does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Select this check box to interrupt interdigit timing when Unified CM must route a call immediately. Default: Clear Corresponding Unified CM Attribute: Urgent Priority.

Option	Description
Do Not Wait for Interdigit Timeout on Subsequent Hopes	When you select this check box along with the Urgent Priority check box and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), Unified CM does not start the interdigit timer after it matches any of the subsequent patterns. Note: Unified CM does not start the interdigit timer even if subsequent patterns are of variable length or if overlapping patterns exist for subsequent matches. Whenever you select the Do Not Wait For Interdigit Timeout On Subsequent Hops check box that is associated with a translation pattern in a translation pattern chain, Unified CM does not start the interdigit timer after it matches any of the subsequent patterns. Note: Unified CM does not start interdigit timer even if subsequent translation patterns in a chain have Do Not Wait For Interdigit Timeout On Subsequent Hops check box cleared. Default: Clear Corresponding Unified CM Attribute: Do Not Wait for Interdigit Timeout On Subsequent Hops.
Route Next Hop By Calling Party Number	Select this check box to enable routing based on the calling party number, which is required for call screening based on caller ID information to work between clusters. Default: Clear Corresponding Unified CM Attribute: Route Next Hop By Calling Party Number.

Translation Patterns: Calling Party Transformations Fields

Option	Description
Use Calling Party's External Phone Number Mask	Select the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. Default: Default Corresponding Unified CM Attribute: Use Calling Party's External Phone Number Mask.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is cleared, no calling party transformation takes place. Default: None Corresponding Unified CM Attribute: Calling Party Transform Mask.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).

Option	Description
Calling Line ID Presentation *	Unified CM uses calling line ID presentation/restriction (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party phone number on the called party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change calling line ID presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling number. • Restricted - Choose if you want Unified CM to block the display of the calling number. For more information about this field, see topics related to calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Note: Use this parameter and the Connected Line ID Presentation parameter, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to configure call display restrictions. Together, these settings allow you to selectively present or restrict calling and/or connected line display information for each call. See topics related to device profile configuration settings and phone settings for information about the Ignore Presentation Indicators (internal calls only) field, and for more information about call display restrictions, see topics related to call display restrictions in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Line ID Presentation.

Option	Description
Calling Name Presentation *	Unified CM uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party name on the called party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change calling name presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling name information. • Restricted - Choose if you want Unified CM to block the display of the calling name information. For more information about this field, see calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Name Presentation.
Calling Party Number Type *	Choose the format for the number type in calling party directory numbers. Unified CM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of: • Unified CM - the Unified CM sets the directory number type. • Unknown - The dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a subscriber by using the shortened subscriber name. Default: Unified CM Corresponding Unified CM Attribute: Calling Party Number Type.

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

Translation Patterns: Connected Party Transformations Fields

Option	Description
Connected Line ID Presentation *	Unified CM uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party phone number on the calling party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change the connected line ID presentation. • Allowed - Choose if you want to display the connected party phone number. • Restricted - Choose if you want Unified CM to block the display of the connected party phone number. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Line ID Presentation.
Connected Name Presentation *	(CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party name on the calling party phone display for this translation pattern. Choose one of: • Default - Choose if you do not want to change the connected name presentation. • Allowed - Choose if you want to display the connected party name. • Restricted - Choose if you want Unified CM to block the display of the connected party name. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Name Presentation.

Translation Patterns: Called Party Transformations Fields

Option	Description
Discard Digits	Choose the discard digits instructions that you want to be associated with this translation pattern. See topics related to discard digits instructions in the Cisco Unified Communications Manager System Guide for more information. Default: None Corresponding Unified CM Attribute: Discard Digits.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed. Default: None Corresponding Unified CM Attribute: Called Party Transform Mask.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#);the international escape character +; and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).
Called Party Number Type *	Choose the format for the number type in called party directory numbers. Unified CM sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CMUnified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of: • Unified CM - Use when the Unified CM sets the directory number type. • Unknown - Use when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a subscriber by using a shortened subscriber number. Default: Unified CM Corresponding Unified CM Attribute: Called Party Number Type.

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

15.6. Configure Cisco Unified Communications Manager Route Patterns

15.6.1. How to Configure Cisco Unified Communications Manager Route Patterns

Introduction

Sometimes it may be necessary to update the default dial plan route patterns that are deployed as part of the default dial plan schemas that are delivered with the VOSS-4-UC template package.

Caution:

The Cisco HCS default dial plan includes most common translation and route patterns and in most cases, should be added automatically when a customer dial plan, site dial plan, and voice mail service is provisioned. If you wish to update translation and route patterns using VOSS-4-UC, you must have a full understanding of the Cisco HCS dial plan. Refer to the VOSS-4-UC Dial Plan Management Guide.

Use this procedure to update Cisco Unified Communications Manager (Unified CM) route patterns that are provisioned by the dial plan schema or to add new route patterns from VOSS-4-UC that are not part of the standard dial plan package. For more information on the latest Unified CM route patterns, refer to http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Make sure the hierarchy path is set to the node where you want to add or edit the route pattern.
3. Perform one of:
   - If you are logged in as provider or reseller administrator, choose **Device Management > CUCM > Route Patterns**.

- If you are logged in as customer administrator, choose: **Device Management > Advanced > Route Patterns**.

4. Perform one of:
   - To add a new route pattern, click **Add**, then go to Step 5.
   - To edit an existing route pattern, click on the pattern to be updated and go to Step 6.
5. From the **CUCM** drop-down menu, select the hostname, domain name, or IP address of the Unified CM to which you want to add the route pattern.

   Note:

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

   Important:

   If you are adding or editing a route pattern at any hierarchy node above a site level, the only Unified CMs that appear in the **CUCM** drop-down list are Unified CMs that are located at the node where you are adding the route pattern, and all Unified CMs in hierarchies above the node where you are adding the route pattern. If you are adding or editing a route pattern at a site level, the Unified CM that appears in the **CUCM** drop-down list is the Unified CM in the site's Network Device List (NDL). If the site does not have an NDL, or the NDL at the site does not have a Unified CM, the drop-down list is empty and a route pattern can not be added to the site.
6. In the **Route Pattern** field, enter the route pattern, or modify the existing route pattern if desired. This field is mandatory. Enter the route pattern, including numbers and wildcards (do not use spaces); for example, enter 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +.
7. If you want to use a partition to restrict access to the route pattern, choose the desired partition from the **Route Partition** drop-down. If you do not want to restrict access to the route pattern, choose <None> for the partition.

   Note:

   Make sure that the combination of route pattern, route filter, and partition is unique within the Unified CM cluster.
8. In the **Description** field, enter a description for the route pattern and route partition if desired. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).
9. Complete at minimum, the mandatory fields on each tab as appropriate (see below):
10. Click **Save** when complete to save the new or updated route pattern.

Route Pattern: Pattern Definition Fields

Tip:

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

Option	Description
MLPP Precedence *	From the drop-down menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern: • Executive Override - Highest precedence setting for MLPP calls • Flash Override - Second highest precedence setting for MLPP calls • Flash - Third highest precedence setting for MLPP calls • Immediate - Fourth highest precedence setting for MLPP calls • Priority - Fifth highest precedence setting for MLPP calls • Routine - Lowest precedence setting for MLPP calls • Default - Does not override the incoming precedence level but rather lets it pass unchanged Default: Default Corresponding Unified CM Attribute: MLPP Precedence.
Apply Call Blocking Percentage	Select this check box to enable the Destination Code Control (DCC) feature. By enabling DCC, all calls other than flash and higher precedence calls made to destination are filtered and allowed or disallowed based on the Call Blocking Percentage quota set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default. Note: The **Apply Call Blocking Percentage** field gets enabled only if the MLPP level is immediate, priority, routine, or default. Default: Clear Corresponding Unified CM Attribute: Apply Call Blocking Percentage.

Option	Description
Call Blocking Percentage	Enter the percentage of calls to be blocked for this destination in numerals. This value specifies the percentage of lower precedence calls made to this destination that get blocked by the route pattern. This percentage limits the lower precedence calls only; the flash and higher precedence calls made to this destination are allowed at all times. Values between 0 and 99 are allowed. Note: Unified CM calculates the maximum number of low priority calls to be allowed through this route pattern based on the call blocking percentage that you set for this destination. Note: The **Call Blocking Percentage** field gets enabled only if the **Apply Call Blocking Percentage** check box is selected. Default: None Corresponding Unified CM Attribute: <Entry box next to Apply Call Blocking Percentage>.
Route Class *	From the drop-down menu, choose a route class setting for this route pattern: • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data The route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. The Default setting uses the existing route class of the incoming call. You can use non-default route class settings to translate an inbound T1 CAS route class digit into a Unified CM route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration. If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class. Default: Default Corresponding Unified CM Attribute: Route Class.
Route List (Mandatory if gateway or trunk is not specified)	Choose the route list for which you are adding a route pattern. Default: None Corresponding Unified CM Attribute: Gateway/Route List.
Gateway/Trunk (Mandatory if route list is not specified)	Choose the gateway or trunk list for which you are adding a route pattern. Note: If the gateway is included in a Route Group, this drop-down menu does not display the gateway. When a gateway is chosen in the drop-down menu, Unified CM uses all the ports in the gateway to route or block this route pattern. This action does not apply for MGCP gateways. Default: Clear Corresponding Unified CM Attribute: Gateway/Route List.

Option	Description
Block this pattern	Indicates whether you want this route pattern to be used for routing calls (such 8[2-9]XX) or for blocking calls. Default: Clear (meaning route pattern is used for routing calls). Corresponding Unified CM Attribute: Block this pattern.
Block Reason	If you click Block this pattern radio button above, you must choose the reason that you want this route pattern to block calls. From the drop-down menu, choose one of: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded Default: No Error Corresponding Unified CM Attribute: <entry box next to Block this pattern>.
Call Classification *	Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. When adding a route pattern, if you clear the **Provide Outside Dial Tone** check box, you set Call Classification as OnNet. Default: OnNet Corresponding Unified CM Attribute: Call Classification.
Allow Device Override	When the check box is selected, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet. Default: Clear Corresponding Unified CM Attribute: Allow Device Override
Provide Outside Dial Tone	Leave this check box selected to provide outside dial tone. To route the call in the network, clear the check box. Default: Clear Corresponding Unified CM Attribute: Provide Outside Dial Tone.
Allow Overlap Sending	With overlap sending enabled, when Unified CM passes a call to the PSTN, it relies on overlap sending in the PSTN to determine how many digits to collect and where to route the call. Select this check box for each route pattern that you consider to be assigned to a gateway or route list that routes the calls to a PSTN that supports overlap sending. The Client Matter Code (CMC) and Forced Authorization Code (FAC) features do not support overlap sending because the Unified CM cannot determine when to prompt the user for the code. If you select the **Require Forced Authorization Code** or the **Require Client Matter Code** check box, the system clears the **Allow Overlap Sending** check box. Default: Clear Corresponding Unified CM Attribute: Allow Overlap Sending
Urgent Priority	If the dial plan contains overlapping patterns, Unified CM does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Select this check box to interrupt interdigit timing when Unified CM must route a call immediately. Default: Clear Corresponding Unified CM Attribute: Urgent Priority.

Option	Description
Require Forced Authorization Code	If you want to use forced authorization codes with this route pattern, select the check box. The FAC feature does not support overlap sending because the Unified CM cannot determine when to prompt the user for the code. If you select the **Allow Overlap Sending** check box, you should clear the **Require Forced Authorization Code** check box. Default: Clear Corresponding Unified CM Attribute: Require Forced Authorization Code.
Authorization Level *	Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern. Range is 0 to 255. Default: 0 Corresponding Unified CM Attribute: Authorization Level
Require Client Matter Code	If you want to use client matter codes with this route pattern, select this check box. The CMC feature does not support overlap sending because the Unified CM cannot determine when to prompt the user for the code. If you select the **Allow Overlap Sending** check box, you should clear the **Require Client Matter Code** check box. Default: Clear Corresponding Unified CM Attribute: <Entry box next to Authorization Level>.

Route Pattern: Calling Party Transformations Fields

Option	Description
Use Calling Party's External Phone Number Mask	Select the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. Note: The calling party transformation settings that are assigned to the route groups in a route list override any calling party transformation settings that are assigned to a route pattern that is associated with that route list. Default: Default Corresponding Unified CM Attribute: Use Calling Party's External Phone Number Mask
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is clear, no calling party transformation takes place. Default: None Corresponding Unified CM Attribute: Calling Party Transform Mask
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).

Option	Description
Calling Line ID Presentation *	Unified CM uses calling line ID presentation/restriction (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party phone number on the called party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change calling line ID presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling number. • Restricted - Choose if you want Unified CM to block the display of the calling number. For more information about this field, see topics related to calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Line ID Presentation.
Calling Name Presentation *	Unified CM uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want the Unified CM to allow or restrict the display of the calling party name on the called party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change calling name presentation. • Allowed - Choose if you want Unified CM to allow the display of the calling name information. • Restricted - Choose if you want Unified CM to block the display of the calling name information. For more information about this field, see calling party number transformations settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Calling Name Presentation.
Calling Party Number Type *	Choose the format for the number type in calling party directory numbers. Unified CM sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Unified CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of: • Unified CM - the Unified CM sets the directory number type. • Unknown - The dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a subscriber by using the shortened subscriber name. Default: Unified CM Corresponding Unified CM Attribute: Calling Party Number Type.

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

Route Pattern: Connected Party Transformations Fields

Option	Description
Connected Line ID Presentation *	Unified CM uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party phone number on the calling party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change the connected line ID presentation. • Allowed - Choose if you want to display the connected party phone number. • Restricted - Choose if you want Unified CM to block the display of the connected party phone number. If a call that originates from an IP phone on Unified CM encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Line ID Presentation.

Option	Description
Connected Name Presentation *	Unified CM uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Unified CM to allow or restrict the display of the connected party name on the calling party phone display for this route pattern. Choose one of: • Default - Choose if you do not want to change the connected name presentation. • Allowed - Choose if you want to display the connected party name. • Restricted - Choose if you want Unified CM to block the display of the connected party name. For more information about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide. Default: Default Corresponding Unified CM Attribute: Connected Name Presentation.

Route Pattern: Called Party Transformations Fields

Option	Description
Discard Digits	Choose the discard digits instructions that you want to be associated with this route pattern. See topics related to discard digits instructions in the Cisco Unified Communications Manager System Guide for more information. Default: None Corresponding Unified CM Attribute: Discard Digits.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed. Default: None Corresponding Unified CM Attribute: Called Party Transform Mask.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#);the international escape character +; and blank. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified CM Attribute: Prefix Digits (Outgoing Calls).

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

15.7. Configure Directory Number Routing

15.7.1. 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.

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.
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.

15.8. Provision Emergency Calls

15.8.1. 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”.

15.8.2. Emergency Handling

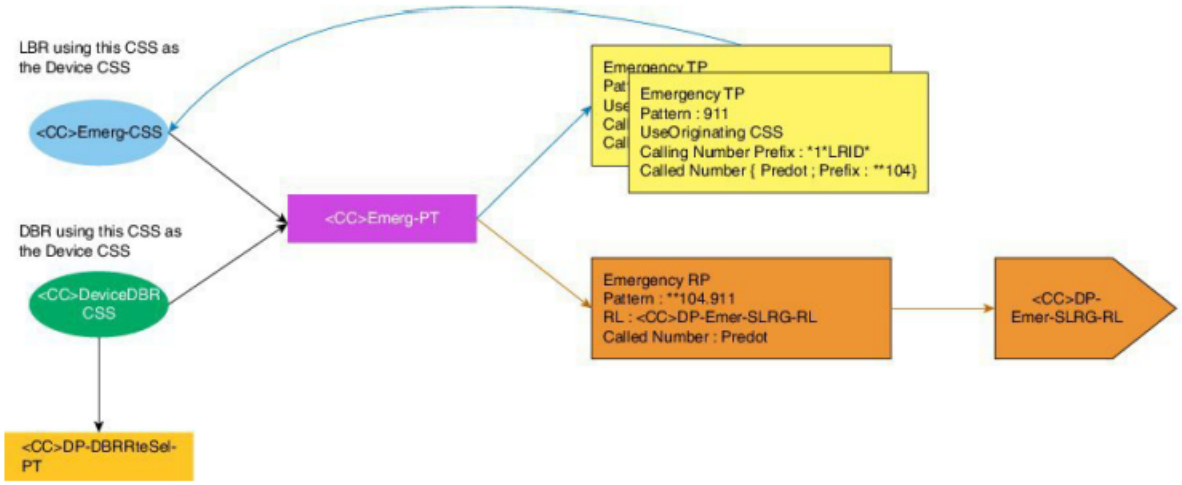
Emergency handling is device-based. It uses the device pool local route group to handle call routing. When a phone has no Direct Inward Dial (DDI) or the phone has DDI but it is in a remote location, emergency handling uses the Site’s Emergency number.

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



15.9. Configure SIP Route Patterns

15.9.1. 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:
   - 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.

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.

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.

15.10. Configure SIP Profiles

15.10.1. 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.

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

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.

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.

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

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

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

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.

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.

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.

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

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.

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)

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.

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

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.

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.

15.11. Configure SIP Trunk Security Profiles

15.11.1. 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**.
   - 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.

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.

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.

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.

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.

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** .

15.12. Configure SIP Trunks

15.12.1. 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.

- 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".

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

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

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

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)

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

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)

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)

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)

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

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

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

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

Option	Description
Connected Party Transformation CSS	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)

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

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

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)

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

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.

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

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

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

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)

15.12.2. Delete 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**.
3. From the list of trunks, choose the SIP trunk to be deleted, by clicking on its box in the leftmost column.
4. Click **Delete** to delete the SIP trunk.
5. From the popup window, click **Yes** to confirm the deletion.

15.12.3. 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**.

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

15.12.4. 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**.

15.13. Configure Route Groups

15.13.1. 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.

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:
   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.

15.13.2. 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.

15.14. Configure Route Lists

15.14.1. 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**.

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".

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.

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.

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.

15.15. Configure Date Time Groups

15.15.1. 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**.

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**.

15.16. Configure Locations

15.16.1. 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*.

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.

Between Locations Fields

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

RSVP Settings Fields

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

15.17. Configure Device Pools

15.17.1. 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**.

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**.

15.17.2. 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.

15.17.3. 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.

15.17.4. 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

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

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.

15.17.5. 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

15.17.6. 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

15.17.7. 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.

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.

15.17.8. 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.

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.

15.17.9. 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.

15.17.10. 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.

15.17.11. 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.

15.18. Associate Local Route Groups to a Device Pool

15.18.1. 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**.

15.19. Configure CTI Route Points

15.19.1. 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:
   - 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**.

15.19.2. 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.

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.

15.19.3. 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**

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.

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.

15.20. Configure Time Periods and Schedules

15.20.1. 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.

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.

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.

15.20.2. 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.

- 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:

- 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.

16 Subscriber Management

16.1. General Subscriber Management Tasks

16.1.1. Add Subscribers

Use this procedure as a high-level workflow to add one or more subscribers in VOSS-4-UC.

Note: If Enable CSS filtering is enabled at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the particular site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

If Enable CSS filtering is not enabled, then the list of available calling search spaces includes all CSSs that are configured on VOSS-4-UC.[1]

---

1. Log in as customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.
2. On the **Subscribers** form, click **Add**.
3. Choose the site to which you want to add the subscriber (only required if logged in as a customer administrator).
4. Configure the details on the following tabs (see below).
5. When you are finished adding information for the subscriber, click **Save**.
6. Repeat steps 2 to 5 to add another subscriber.

User

On the **User** tab, complete fields to add a Unified CM user and a VOSS-4-UC user.

Consider the following when adding a user:

- Use only alphanumeric characters.
- A selected Entitlement Profile will be associated with the Subscriber.
- The options available in the **Service Profile** drop-down menu are those that were imported from Unified CM.

[1] This only applies to the VOSS-4-UC *Provider* deployment.

- If an existing phone is to be associated with a user, choose the device from the **Associated Devices** group.
- After an existing phone is associated to the user in the **Associated Devices** group **Device** drop-down menu, click **Save**. The subscriber is updated so that the **Phones** tab is populated with the information of the new phone associated with the user.
- If the added user is configured as an LDAP user, the **Password** and **Repeat Password** fields are hidden. The **Enable Mobility** check box is auto-selected if any of the following are included or added: a remote destination phone, mobile identity for a phone, or remote destination profile (RDP).

  If subscriber self-provisioning has been set up so that subscribers can add their own smart devices and the **Enable Mobility** check box is *not* selected, then the setting will be enabled when subscribers add a smart device on the Self-service interface.
- If the subscriber is entitled to use Webex Teams, you can add a standalone Webex Teams user by completing (at a minimum), the **Userid**, **Last Name** and **Email Address** fields and then going straight to *Add Subscribers* (Webex Teams tab).

  Note:

  To enable Extend and Connect in VOSS-4-UC, complete the following task:

  1. Select the **Enable Mobility** check box.
  2. Add the following three groups of users:
     a. Standard CCM End Users
     b. Standard CTI Enabled
     c. Standard CCM Admin User
- If a Customer is configured for EMCC, and if you want the subscriber to have access to the EMCC feature, select the **Enable EMCC** check box.
- Choose a **BLF Presence Group** for the subscriber from the drop-down. The chosen group specifies the destinations that the subscriber can monitor and is configured in Cisco Unified Administration. BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. The Busy Lamp Field default is set according to the selected number and specifies the Standard Presence Group that is configured with installation.
- Choose the Primary Extension for the subscriber by choosing from the **Pattern** drop-down list, which includes all lines available to the subscriber. The selected option is displayed in the Primary Line column for the subscriber on the **Subscribers** list view.
- The Subscriber Language and Role can be set in the Site Defaults of the site hierarchy that the subscriber belongs to. If not set in the Site Defaults, hierarchy defaults apply.

Phones

On the **Phones** tab, click Phones **Add** and complete the required fields to add a new phone.

Consider the following when adding a phone:

- Modify the values for the following fields if desired: **Product Type**, **Device Protocol**, **Phone Button Template**, and **Device Security Profile**. The possible value options for these fields change depending on which associated fields are selected.

  For example, when you enter the **Device Name** with the product prefix and the MAC address, 79XX-type phones have the device name 'SEP' prefixed, while ATA-type phones have 'ATA' prefixed to the MAC address. Fields are validated and tooltips are available to assist you to select the **Product** type.

You can override the default Phone Button Template value by selecting from the **Phone Button Template** drop-down, or by entering a custom value in the **Phone Button Template** field. The entered value will be applied on Unified CM if the Unified CM allows it for that phone type.

- Modify phone-specific settings such as **DND Option** drop-down menu, **Do Not Disturb** check box, and **Hot Line Device**. The phone settings that are available differ depending on the product (phone) type selected, the device protocol (for example SIP or SCCP), and the Field Display Policy (FDP) applied by the administrator. You can select a Mobile User ID Name from the drop-down list when a Dual-Mode Phone for Android or iPhones is selected. This associates the selected user to the Mobile Identity feature on this phone and must match the Userid added on the **User** tab.
- The advanced settings fields are updated automatically for the phone based on the phone type. The phone is automatically associated to the user and is then displayed as an associated device when you view the subscriber after adding it. If a phone that has been associated with a user is also associated with another user, the Owner User ID defaults to the first user.
- In the **Line** section, complete line assignments. Note that when you select a Route Partition Name, the available Pattern options are filtered according to the selected partition. However, you can add a custom pattern by typing it into the **Pattern** field. The associated **Enduser** field identifies the user for Presence, but you can add a new User ID. VOSS-4-UC adds the user first and then adds the User ID.
- In the **Speeddial** section, add speed dial information. Available speed dials depend on the Phone Button Template.
- In the **Busy Lamp Field** section, specify Busy Lamp Field values. Fields include: **Position**, **Label**, **Blf Destination**, and so on.
- In the **Blf Directed Call Park** section, specify Busy Lamp Field Directed Call Park values. Values depend on a valid Directed Call Park on Unified CM.
- In the **Add On Module** section, specify Add On Modules if desired. The Add On Modules Load Name can be any value, but the Model has to be supported by the phone.
- In the **Service** section, add services that are valid IP services for Phones. To add a service to the device, a number must be added as the Uri Button index. If you do not add a number, only the service is added.
- Use the **Mobile Identity** section to configure mobile identity details when you select a Dual-Mode Phone. Fields include: **Name**, **Dual-Mode Device** (automatically populated from the **Device Name** field), and **Mobility Profile** (chosen from a drop-down list). The **Destination Number** field is a mandatory field and determines the destination number that is dialed when a call is made to the dual-mode phone.
- Use the **Remote Destination** section to configure your remote destinations when a Dual Mode Phone or Cisco Spark Remote Device is selected as the **Product**. Remote destinations represent the mobile (or other) phones that are able to accept transfer from the desktop phone and can be used to initiate calls. Set the Pattern for the Line Association to the Route Partition name. If you enter more than one Pattern and the new Pattern is not on the system, enter the Route Partition Name manually. The **Owner User Id** and **Dual Mode Device Name** fields are auto populated.

Note: When a CTI Remote Device is selected as the **Product**, a **CTI Remote Destination** section replaces **Remote Destination**. This allows you to configure your remote destinations specifically for a CTI Remote Device. The **Owner User Id** and **CTI Remote Device** fields are auto populated.

- Use the **Vendor Config** section of the tab to view and edit the configuration settings for each device. The available configuration settings depend on each Product type selected. Modify settings as required.

  Note that:

1. The administrator password from the `AdminLoginDetails` in Unified CM is not stored in VOSS-4-UC. Data in VOSS-4UC is obtained from Unified CM.
2. VOSS-4-UC cannot disable the `Override Enterprise/Common Phone Profile Settings` setting once this check box has been enabled in the Unified CM GUI.

   This setting needs to be disabled on Unified CM if the user wishes to disable it.

Extension Mobility

On the **Extension Mobility** tab, complete fields to configure extension mobility for the subscriber.

Consider the following:

- Only one EM Profile can be added for extension mobility in VOSS-4-UC. If a subscriber is associated with more than one EM profile on the Unified CM, and you sync with VOSS-4-UC, both will be displayed:
  - on the subscriber's EM tab (this tab)
  - on the **Extension Mobility** list view (see *Standalone Extension Mobility*).
- As with the **Phones** tab, **Product**, **Protocol** and **Phone Button Template** fields change, depending on the selection of an associated field.

  The considerations regarding the fields on this tab are the same as on the **Phones** tab with the exception of remote destination information, which is not available on extension mobility (see *Consider the following when adding a phone* under **Phones** above).
- Ensure that you associate the extension mobility profile and target phone for login with the extension mobility service.
- If the Enable Extension Mobility Cross Cluster (EMCC) feature is enabled on the **User** tab, you must choose a CSS for this device from the **Extension Mobility Cross Cluster CSS** drop-down. The selected CSS is used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. New CSS's or existing CSS's can be added or modified in Unified CM. Refer to the Cisco Unified Communications Manager Features and Services Guide for more details if required.

See also *Standalone Extension Mobility* to add or edit an extension mobility profile, and associate it to one or more subscriber.

Single Number Reach

On the **Single Number Reach** tab, note that you cannot add more than one Remote Destination Profile for Single Number Reach. However, you can add more than one Remote Destination Rdp.

Note:

To enable Extend and Connect in VOSS-4-UC, make sure to complete the following task:

1. Select the **Enable Extend and Connect** check box.
2. Select the CTI remote device that you created from the **CTI Remote Device Name** drop-down list.

Voicemail

On the **Voicemail** tab, configure voice mail service for the subscriber if a valid Cisco Unity Connection server is available.

Consider the following when configuring voice mail:

- You can leave the PIN and Password empty, in which case the default credential policy on the Cisco Unity Connection is used.
- If the user on Cisco Unity Connection is LDAP integrated, the **Password** field is visible but should be ignored.
- The **Voicemail Line** drop-down list only shows lines with status 'Available' or 'Used', but you can also add values manually. The Cisco Unity Connection server uses this line as a caller ID, so you should set it to the subscriber's default line.
- When Voicemail is added for a Subscriber, all **Call Forward To Voicemail** check boxes, except **Call Forward All**, will be enabled on the chosen Line, and the Voicemail Profile setting will be set based on the Site Default Doc setting "Default CUCM Line Voicemail Profile" (**Site Management > Defaults > Line Defaults**).

WebEx

On the **WebEx** tab, add details if a valid server is available. The mandatory fields on this tab are populated with the values entered on the **User** tab.

Note: Any updates on the **User** tab do not update these values; values are populated only during the Add workflow.

Webex Teams

On the **Webex Teams** tab, click Webex Teams User +, and select the check boxes to select the desired Enabled Services and Roles for the subscriber:

Consider the following:

a. Webex Teams is only available if a Webex Teams Service has been created at the required customer level (see *Create Webex Teams Service*), and if the **Webex Teams** check box has been selected in the Entitlement Profile associated to the Subscriber.

b. The Webex Teams User fields, **Login Enabled** and **Invite Pending** check boxes are read-only and can not be edited.

c. "Enabled" is displayed in the Webex Teams column on the **Subscribers** screen next to the subscriber once successfully added as a Webex Teams user.

d. The Subscriber e-mail address is required to enable Webex Teams for the Subscriber.

Contact Center Subscriber

Contact Center Management

The Subscriber feature supports adding, removing or updating UCCX agent capabilities to a Subscriber.

The **Contact Center** tab is only available if:

- UCCX device has been added and is available to the hierarchy.
- Contact Center Service has been configured and is available to the hierarchy.
- Entitlement Profile: the **Contact Center** check box has been selected and associated to the Subscriber.

Consider the following for the Agent:

- Since UCCX restricts the use of special characters, these are restricted in the **Alias**.
- **Team**, **Resource Group** and **Skill** names need to be set up or synced from the UCCX device before they can be assigned.
- **Automatic Available** is enabled by default.
- An IPCC extension is automatically managed for the Unified CM user associated with the Contact Center Agent.
- It is possible to change the the agent's **Controlled Device**. The device in question must already be associated with the Subscriber before attempting to set or change it.

16.1.2. Subscribers List View

The Subscribers list view provides a list of all subscribers located at the specified hierarchy level. This list view provides a central point from which you can manage subscribers by viewing their details under the following column headings:

Note: Descriptions are only included for column headings that are not self explanatory.

Column Heading	Description
User ID	
First Name	
Last Name	
Email	
User Type	CUCM Local, VOSS-LDAP Synced, or CUCM-LDAP Synced.
Entitlement Profile	The Entitlement Profile associated with the Subscriber.
Located At	Displays an abbreviated version of the hierarchy showing the lowest point in the hierarchy. The hierarchy type is shown in brackets. When you filter on this column, do not use text included inside the brackets in the filtering criteria. For example: “SiteName (Site)”, where (Site)= the hierarchy node type, only search using the “SiteName” portion of the field.
PrimaryLine	The subscriber’s primary extension number, as selected from the Pattern drop-down list when adding the subscriber.
ExtMobility	If a Subscriber is associated with more than one extension mobility profile on the Unified CM, and you sync with VOSS-4-UC, only the first extension mobility profile is displayed in this list view.
Single Number Reach	The remote destination number configured for the subscriber. Only if supported.
Voicemail	The Voicemail number allocated to the subscriber.
Conferencing	Enabled or disabled.
Webex Teams	Enabled or blank. Indicates whether or not the subscriber is enabled to use Webex Teams.
Contact Center	Enabled or blank. Indicates the contact center agent’s Team and extension if the subscriber is an agent.
Phone	The phone associated to the subscriber. When you filter on this column, the results include all phones at the hierarchy level and below, regardless of the Phone column in which they reside.
Phone 2	The second phone associated to the subscriber.
Phone n	The number of phone columns displayed in the list view will be the same as the maximum number of associated to a particular subscriber. For example, if a subscriber is associated to 10 phones, the list view will show 10 Phone columns.
Device	IP Address or Host Name.

Refer to the topics under Common Tasks for information on common functionality that can be perfomed in list views, this includes: selecting items, bulk delete and modify, ordering lists, filtering lists, navigating lists, performing a list search, and so on.

16.1.3. Modify Subscribers

Use this procedure to modify settings for one or more subscribers.

Procedure

1. Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.
2. Choose a site from the hierarchy breadcrumb.
3. Choose **Subscriber Management > Subscribers**.
4. Choose the subscriber to be updated by clicking on its box in the leftmost column, then click **Edit**.
5. Modify subscriber information as required, using the workflow described in Add Subscribers.

   Note:

   You can use the pop up form that is available when modifying the Subscriber on the Phones tab to add more than one phone. Also, instances of one-to-many or zero-to-many items can be deleted, such as a Phone.

   The line settings of a phone can be modified directly from the Subscriber form. When expanding the Line group of a Phone or Extension Mobility Profile, the Link to Line hyperlink on each Line form directs the user to the specific Line relation details. The details can then be modified and saved, after which the user will be returned to the base tab of the Subscriber form. The user can also navigate back to the base tab of the Subscriber by using the back button. When a user's menu layout has more than one entry for `relation/LineRelation` and associated Field Display Policy, then the form opened by the Link to Line hyperlink will apply the first one (searching from top to bottom) found in the user's menu layout, if one is available.
6. Click **Save**.

Note: Filtering on the following columns on the Subscribers list view is described in more detail below:

- Located At - Displays an abbreviated version of the hierarchy showing the lowest point in the hierarchy. The hierarchy type is shown in brackets. When you filter on this column, do not use text included inside the brackets in the filtering criteria. For example: "SiteName (Site)", where (Site) = the hierarchy node type, only search using the "SiteName" portion of the field.
- Device - You can filter on IP Address or Host Name.
- Phone - When you filter on this column, the results include all phones at the hierarchy level and below, regardless of the Phone column in which they reside.

16.1.4. Delete Subscribers

Use this procedure to delete one or more subscribers.

Procedure

1. Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.
2. Choose a site from the hierarchy breadcrumb.
3. Choose **Subscriber Management > Subscribers**.

4. Choose the subscriber to be deleted by selecting the check box in the leftmost column, then click **Delete**.
5. From the popup window, click **Yes** to confirm the deletion.

Note: For scenarios that include an LDAP-integrated Cisco Unified Communications Manager, the process for deleting a user is from the LDAP directory and not from the VOSS-4-UC system. Set up a data sync to synchronize the removal of the user.

When the delete action is complete, the Subscriber disappears from the list. All elements associated with the Subscriber are deleted, except Lines.

16.1.5. Move Subscriber

This feature provides a customer administrator (or higher) with the ability to move a subscriber from customer level to a site, as well as from one site to a different site under the same customer. Moving the subscriber from one site to another site on a different Unified CM cluster and CUCxn cluster is also supported.

This is done on the **Move Subscriber** screen accessed via the **Subscriber Management > Move Subscriber** (default menu option).

Subscriber Data

When moving a subscriber, the subscriber, phones, device profiles, SNR, voicemail and VOSS-4-UC data are processed. The subscriber will be updated with a new primary extension where appropriate.

The subscriber role at the destination hierarchy is selectable and an optional configuration template `MoveUpdateUserCustom_CFT` is available to make custom subscriber updates.

A device pool at the destination hierarchy is mandatory. You can select either the default device pool at the destination hierarchy or choose a different device pool from a drop-down list.

Phone Data

Desk phones can either remain at the old site or move with the subscriber. Other softphone devices, e.g. Jabber devices are always moved.

The default operation is to move all phones to the destination hierarchy, i.e. **Move Desk Phones to Destination Hierarchy** check box = Selected.

If the desk phones are not moved, i.e. check box = Cleared, desk phones remain at the original site and are disassociated from the subscriber.

An option is provided to create a new desk phone at the destination hierarchy. An existing phone is used as a template, and the model and phone button template can be selected from drop-down lists. An optional configuration template `MoveUpdatePhoneCustom_CFT` for the new phone can be chosen to make custom device settings available.

Line Data

Lines can be moved to the destination hierarchy if the move is on the same cluster. To enable moving of lines to the destination hierarchy, the `UserMove_AllowLineMove_MCR` macro must be cloned to the applicable hierarchy level and the value set to `{{ fn.true }}`.

Note that moving lines may not be supported by the customer dial plan; SLC based dial plans (types 1, 2 and 3) do not support moving of lines between sites. Make sure that the customer dial plan supports moving of lines between sites before attempting to move the line.

When moving to another Unified CM cluster, new lines must be defined. The CSS's for the new lines can be defined and a configuration template `MoveUpdateLineCustom_CFT` is available to make custom line updates.

Note that a check is performed to ensure that the first line across devices is common. This first line is used for SNR and voicemail. If the move is determined to be between sites hosted on the same Unified CM cluster, the subscriber data is moved to the new hierarchy and updated as above. It is assumed that the CUCxn (if used) will remain.

If the move is between different Unified CM clusters, the data defined above is re-provisioned on the new cluster and deleted on the original cluster, except for the Unified CM subscriber. When the Unified CM subscriber is local, the old subscriber is removed.

In the case of an LDAP user, the VOSS-4-UC subscriber is purged. The user is removed from the `device/cucm/User` model of the source Unified CM in VOSS-4-UC. The home cluster flag is maintained such that it is only set to true on the Unified CM cluster hosting the subscriber, even if the subscriber exists on other Unified CM clusters.

When moving between clusters, the CUCxn server can be retained. In this case, the model instances are moved. In the case that the CUCxn server changes, a new CUCxn subscriber is created against a chosen subscriber template. This will not copy custom settings for the CUCxn subscriber or any recorded prompts and messages.

Existing Services

Existing services associated to the subscriber such as phones and lines, device profiles, single number reach and Voicemail, which will be moved with the subscriber, are displayed on this tab.

Caveats

- Lines cannot be moved during cross cluster subscriber move, only within a Cisco Unified CM cluster.
- The first line on all devices must be common prior to the move. Replacing lines creates the same line layout on all devices.
- When moving cross cluster, the Unified CM cluster is changed. The CUCxn cluster may be retained or changed, based on the new site NDL. If the CUCxn cluster is changed, only basic voicemail is created - user customised configuration, as well as prompts and messages are not moved to the new CUCxn cluster.
- CUCxn cluster moves are only supported where the Unified CM cluster changes.

16.1.6. Class of Service

Customer administrators and higher level administrators can create and maintain a Class of Service (CoS) that apply to subscribers. A CoS specifies the Unified CM and Calling Search Spaces (CSS) for a subscriber's line, thereby indicating whether local, national and international numbers can be called.

An administrator can create a CoS at a customer level hierarchy. A Unified CM is specified. A drop-down list of those available at the customer level is shown.

Optional device and line CSSs can also be added - either selected from those existing on the Unified CM, or else added. Macros can also be used when adding new CSSs, for example: `CSS-Gold-{{macro.SITENAME}}`.

When a CoS is modified, the Unified CM cannot be modified. In order to refer to another Unified CM, either clone an existing CoS or else delete it and re-add it.

16.1.7. Add a Class of Service

1. As a customer administrator or higher, and choose **Subscriber Management > Class of Service**.
2. To add new CoS instance, click **Add**. If necessary, this will automatically direct the user to select a customer-hierarchy-level, if not already on it.
3. From the **CUCM** drop-down, choose the desired Unified CM.
4. Enter the Class of Service name in the **CoS Name** field.
5. From the **Device CSS** and **Line CSS** drop-downs, choose the desired CSS types to be associated to this CoS item.

   The value can also be a macro that evaluates to a valid CSS type which already exists on the selected Unified CM. Blank values are also allowed.

16.1.8. Configure Lines

Use this procedure as a high level workflow to configure one or more lines (directory numbers) in VOSS-4-UC. Note that if the Number Inventory feature has been enabled by the administrator, lines are not added; rather, lines are selected from a drop-down list of available numbers.

Note: The Lines interface in VOSS-4-UC provides an easy method to add, modify, or delete individual lines and associated line settings to, or from the system.

Procedure

1. On the **Lines** form, click **Add**.
2. Configure the line and its associated line settings using the following tabs. For more information on the values to fill in for the various line parameters such as partitions and CSS, refer to the “Provider HCS Dial Plan Management Support Guide” .

Note: If the **Enable CSS filtering** check box is selected at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the particular site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

If the **Enable CSS filtering** check box is clear, then the list of available calling search spaces includes all CSSs that are configured on the Cisco Unified Communications Manager (Unified CM).

Tab	Description
Directory Number Basic Information	Includes a directory number (mandatory), a route partition, calling search space, call pickup group (to which the line belongs), and other basic settings. The **Directory Number** field is either a drop-down list or a free text field, or a drop-down containing only the available directory numbers (depending on whether the Number Inventory feature is enabled or disabled). Only the actual Directory Number is mandatory.
Directory Number Advanced Information	Includes various profiles, groups, and advanced settings for the line; for example, voice mail profiles.
Shared Device Info	Shows any phones, device profiles, or remote destination profiles that have been associated with the particular line.
Line Settings for All Devices	Includes fields such as hold reversion ring duration, hold reversion notification interval, party entrance tone (chosen from a drop-down list).
AAR Settings	Automated alternate routing (AAR) handles the calls that are routed to the AAR Destination Mask or Voice Mail.
Park Monitoring	Includes text fields such as park monitoring forward no retrieve destination external or internal voice mail enabled check boxes, park monitoring forward no retrieve destination external, external calling search space, internal, internal calling search space, and park monitoring reversion timer text fields. Note:[1] If the **Enable CSS filtering** check box is selected at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the particular site. If the **Enable CSS filtering** check box is cleared, then the list of available calling search spaces includes all CSSs that are configured on the Unified CM.
Call Forwarded Information	Includes call forward all settings, call forward busy external and internal settings, call forward no answer external and internal settings, and so on.

3. When you are finished adding line information, click **Save**. All additions or changes to Lines and line settings in the system are also reflected in the Unified CM. After configuring a line, the transaction menu item (**Administration Tools > Transaction**) can be used to verify the configuration.
4. To modify existing line and line setting details, change the settings or add new line settings using the process described in Steps 1 to 6. For example, you can add additional directory URIs and directory URI partitions. Manual configuration must first be done on the Unified CM before URIs will function. Note that not all line settings are configured on the **Lines** form. Device specific settings such as caller ID display, line label, E.164 mask, and associated end user are configured from the **Lines** tab on the associated Subscriber Management **Phones** form.

16.1.9. Delete Lines

Use this procedure to delete one or more lines, or line settings.

Procedure

1. Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.
2. Choose a site from the hierarchy breadcrumb.
3. Choose **Subscriber Management > Lines**.
4. Choose one of the following methods to delete lines or line settings:
   - Choose an individual line to be deleted by clicking on its box in the leftmost column, then click **Delete**. From the popup window, click **Yes** to confirm the deleted line.
   - Delete multiple lines at once by checking the relevant check boxes, then clicking **Delete**. From the popup window click **Yes** to confirm the deleted lines.
   - Remove line settings from a line as required by removing them from the relevant tab of a selected line. Click **Save**.

When the delete action is complete, the line disappears from the list.

16.1.10. Add Agent Line (Phone)

Procedure

1. Choose **Subscriber Management > Agent Lines**.
2. On the **Agent Lines** screen, click **Add** to add a new agent line .
3. Complete the following:

[1] This only applies to the VOSS-4-UC *Provider* deployment.

Field	Description
Device Type	Select device type: Phone
Device Name	Select the name of the Cisco Unified Communications Manager Phone. This is a mandatory field.
Line	Select the line to be marked as an agent line. This is a mandatory field.
Application User	Select the application user to be associated with the Phone. This is a mandatory field.
Agent Line Prefix	CC_Line. This is read-only.

4. Click **Save** to add the agent line.

16.1.11. Line Search

The **Line Search** utility enables you to quickly search for all devices and services associated with a selected line.

A **Search Line** drop down of lines is the list of available lines on the Internal Number Inventory (INI) at a selected customer hierarchy and downwards, with used lines indicated as (used). The E164 number associated with the INI is also shown if available.

The devices and services search results per line can be:

- Phones (up to 10 results)
- Users (up to 10 results)
- Hunt Groups (up to 10 results)
- Call Pickup Group
- Device Profile
- Remote Destination Profile
- Voice Mail account

Search results are displayed as a list of grouped identifiers with links that allow you to directly navigate to the individual service or device details.

16.1.12. Phone Type Management

After you make changes to any phone model specific data in Unified CM, for example by loading a new BAT file, editing phone button templates, security profiles, and so on, then in order to utilize that data in VOSS-4-UC, you need to do a sync of the Unified CM.

Include the following models in the data sync - depending on what you changed:

- `device/cucm/PhoneType` - should always be included. Note this includes the expansion modules as well as the phone types.
- `device/cucm/PhoneButtonTemplate` - if button templates were changed
- `device/cucm/PhoneSecurityProfile` - if phone security profiles were modified

If you do a full sync or full import this will make the changes available in VOSS-4-UC. However, between full syncs, it is best practice to create a sync setup with a model type list that includes the above model types. This allows you to run an ad-hoc sync with a very limited scope as needed - if changes are made in the Unified CM that require a sync.

If adding new phone types to the system, you may also need to edit your device groups and entitlement profiles (if used) to have them show as options to the correct users.

16.1.13. Phone Onboarding with Cisco Activation Codes

VOSS-4-UC supports the Cisco Unified CM capability for device onboarding using Activation Codes. This provides a simplified method to register a new phone in the system. This is supported from UCM version 12.5 and later.

This feature allows administrators to create phones without MAC addresses and then share automatically generated activation codes with end users via Self Service or email. The end user can then enter the activation code into the physical device to initiate auto registration.

Once the phone has been activated and registered, the correct phone association takes place in VOSS-4-UC.

For more information on the detailed functionality of the Cisco Activation Code Device Onboarding capability, including supported devices, refer to the Cisco documentation.

The setup of the feature has been incorporated into our various Subscriber/Phone Management capabilities:

- Phones
- Subscribers
- Quick Add Subscriber
- Smart Add Phone

Note: The selected phone type must also be included in the Subscriber's entitlement profile.

Typical Workflow

At a high level in VOSS-4-UC, there are the following setup steps for this feature:

1. Initial Setup - enabling Phone types for activation code.
2. Per Subscriber/Device - setup of the phone details and generation of the activation code.
3. Provide the activation code to the user for use to onboard the device.

To complete the initial setup and enable the phone type(s) for activation code use:

1. Login as customer administrator or higher.
2. It can simplify things to navigate to the hierarchy level of the cluster(s) you want to enable
3. Enable activation code based registration for a target phone type:
    a. Browse to **Device Management > CUCM > Device Defaults**.
    b. Click the **Model**, e.g. Cisco 7821 on which you want to enable the phone registration activation code feature. Note the device column in the list view to ensure it is the device type on the right UCM cluster.
    c. Select the **Prefer Act Code Over Auto Reg** check box.

d. Click **Save**.

To complete the per Subscriber/Device setup to prepare the phone for onboarding:

1. Once enabled, you can add the phone, using any of the prescribed Subscriber Management methods (see above), making sure to select the **Use Activation Code Onboarding** check box. This will remove the device name as a BATXXXXXXXXXXX device name will be generated when adding the phone.
2. Once the phone has been successfully added, an activation code is generated, and displayed along with the code expiry time on the relevant **Phones** form (**Subscriber Management > Phones**).

   Note: The phone activation code must be used to register the phone before the specified expiry date.

3. The activation code is available in the end user's self service if the device was associated to a user. Alternatively email the activation code to the end user.
4. The end user registers the phone by entering the activation code into the physical device.
5. To see the list of phones that have been setup for activation codes but not yet activated, you can filter the phones list view for device names starting with, BAT, as once they register they have the appopriate device name prefix (e.g. SEP).

16.1.14. Configure Phones

Before You Begin

To ensure that the Add Phones work flows execute successfully, create and configure the following items first on Cisco Unified Communications Manager (Unified CM). Then import them into VOSS-4-UC:

- Softkey templates and phone button templates
- Service parameters and enterprise parameters that must be set for a subscriber service
- Custom SIP profiles
- Service profiles for Jabber
- Phone services

During the end-to-end creation of providers, customers, and sites, default values are created (for example, Site ID). If the dial plan for the site specifies Device Pool, CSS, and Partition names, these are available for selection. To identify these site-related values, refer to the naming conventions used in *Modify Site Defaults*.

The Site Defaults Menu item populates certain default values for phones. To view and edit the menu (depending on your sign-in level), choose **Site Management > Defaults** and click the site name in the list view. For phone parameter information, use the fields on the **General Defaults** and **Device Defaults** tabs. Refer to *Modify Site Defaults* for additional information regarding the values to fill in for phone parameters such as partitions and CSSs.

Note: If the **Enable CSS filtering** check box is selected at the customer dial plan, then the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the particular site. You can add a custom CSS in a CSS field if you know the exact syntax.

If the **Enable CSS filtering** check box is clear, then the list of available calling search spaces includes all CSSs that are configured on Unified CM.

Use this procedure as a high-level workflow to configure one or more phones and associated settings. If the Number Inventory feature is enabled, phone lines are not added. Instead, phones are selected from a drop-down list of available numbers.

The **Phones** screen is an integrated display to add, modify, or delete the following on the Unified CM device:

- A line
- Devices and device details related to the user
- The association of a line with the user's device
- For a Dual-Mode Phone, any provisioned mobile identity is added to the phone. You can add more remote destinations if necessary.
- The User is updated. For a Dual-Mode Phone, the Mobility User ID Name must be set.

When adding a device for a subscriber, ensure that the following properties of the selected device are related correctly:

- Product
- Protocol
- Security Profile Name
- Phone Template Name. If a new phone is added to Unified CM using COP files, the phone and associated template are only available in VOSS-4-UC after it has been synchronized with Unified CM.

Note: The **Registration Status** and **IP Address** columns in the **Phones** list view (filterable) or the field values on the instance form of a phone refer to the registration status and address of the phone on Unified CM, for example "None", "UnRegistered with CUCM-11-5-IP2", "Registered with CUCM-11-5-IP2".

These phone properties are automatically updated when an instance form of a phone is opened, and also by a service that runs periodically at a configured interval. Refer to the Metrics Configuration topic in the Advanced Configuration Guide for details on **RIS API data collector interval**.

An **Activate Phone Status Service** setting is enabled by default and can be managed by system level administrators. Refer to the Advanced Configuration Guide for details. When viewing a list of phones, the **status** action can be carried out by an administrator who has been assigned a role that has an access profile to enable this action. Carrying out this operation fetches the Unified CM phone IP address and status *directly* from the Unified CM and displays the data on the **Phones** list view **Registration Status** and **IP Address** columns, updating any existing data shown.

- Since the result of the **status** action is in real time, the current status of the list requires that the action carried out in order to see the latest values.
- There is no cache of data resulting from this action. Any values shown in the columns would not be current, but are the cached values from the RIS data collector if it is enabled.
- When carrying out the **status** action, the data in the **Registration Status** and **IP Address** columns can only be viewed.:
  - The latest data only shows for the *current* list of phones on the GUI.
  - The data in these columns is not stored in the database and *cannot be exported*.

Procedure

1. Sign in as a provider, customer, or site level administrator. If you are signed in as the site administrator, you can see a subset of the fields that are available on the interface.

2. Choose site from the hierarchy breadcrumb.
3. Choose **Subscriber Management > Phones**.
4. Click **Add**.
5. Configure the phone and its associated settings using the following tabs.

Tab	Description
Phone	Default values for **Device Protocol**, **BAT Phone Template**, **Device Security Profile**, and other fields are updated automatically based on the selected **Product** type. The **Vendor Config** area displays the configurable vendor features available for the selected phone type. Configure each field as required. The fields displayed vary depending on the selected **Product** (device type) and the **Device Protocol** (such as SIP or SCCP). The availability of the **Vendor Config** settings depends on the Field Display Policy. The supported features available for each phone type are retrieved from the related Unified CM. You can override the default **Phone Button Template** value by entering a custom value in the **Phone Button Template** field. The entered value will be applied on Unified CM if the Unified CM allows it for that phone type. Tip: If you don't see a template that you are looking for in the drop-down list (for example, for **Phone Button Template**, **Device Security Profile** or **SIP Profile**), edit the template on Unified CM, and then sync the template into VOSS-4-UC to have it appear in the drop-down list. Tip: If the **Product** type list does not contain the phone or endpoint you want, take the following steps. In Unified CM, install a COP file for the endpoint you want. Install the COP file only once for the Unified CM instance where the endpoint is added. Then in VOSS-4-UC, import the phone button template from Unified CM. Note: Follow these steps while creating a CTI Remote Device to enable Extend and Connect in VOSS-4-UC: 1. Enter the **Device Name**. For example, CTIRD<USERID>. 2. Choose the **Product** as **CTI Remote Device**. 3. Choose the **Owner User ID** from the drop-down list. 4. Choose the **SUBSCRIBE Calling Search Space** name from the drop-down list. 5. Choose the **Rerouting Calling Search Space** name from the drop-down list.
Lines	This tab serves two purposes. 1. To show all the lines that are associated with the device 2. To associate lines with the device. The Lines sections reflect the Lines object in Unified CM. You can add lines to this group and associate lines with the device. You can add custom lines by entering a line in the drop-down list (depending on the status of the Number Inventory feature).
Speed Dials	Allows you to configure speed dials for the device. Available speed dials depend on the device's **Phone Button Template**. The order in which Speed Dial entries are added matches the slots that are available in Unified CM.
Services	Used to set IP Phone services.
Busy Lamp Fields	Allows you to configure busy lamps for the device. Available busy lamp fields depend on the device's **Phone Button Template**.
Blf Directed Call Parks	Allows you to configure Busy Lamp Field directed call parks for the device. Available BLF-directed call parks depend on the device's **Phone Button Template**. Create BLF-directed call parks in **Call Routing > Directed Call Parks** on Unified CM before configuring them from this tab. The available BLF-directed call parks match those created for each specific Route Partition Name.

Tab	Description
Dual Mode Settings	Only applies to a Dual Mode Phone, Spark Remote Device, or CTI Remote Device, and allows you to enter the relevant Mobile Identity and Remote Destination (or CTI Remote Destination) parameters for the device. These parameters include Name, Destination Number, Owner User ID, Dual Mode Device Name (or CTI Remote Device), and Answer Too Soon and Too Late Timers.

6. When you are finished adding phones and phone settings, click **Save**.
7. To modify phone and phone settings, use the process described in Steps 1 to 6. When you modify a phone, the following workflow is executed (depending on what was modified):
    - When adding a line, a check is made to see if it exists. If the line does not exist, it is created.
    - When modifying a line, the Link to Line hyperlink on each Line form directs the user to the specific Line relation details. The details can then be modified and saved, after which the user will be returned to the base tab of the Phone form. The user can also navigate back to the Phone by using the back button. When a user's menu layout has more than one entry for `relation/LineRelation` and associated Field Display Policy, then the form opened by the Link to Line hyperlink will apply the first one (searching from top to bottom) found in the user's menu layout, if one is available.
    - The Phone and User Remote Destination are updated.

16.1.15. Move Phones

When phones are not assigned to users, you can move them between sites. Moving a phone between sites handles the situation where a phone is either physically moved or logically assigned to a different site. If a phone is assigned in the Associated Devices list of a CUCM User, the phone is moved as part of a Move User operation. See "Move Users".

Important - the following restrictions apply when you move phones:

- You cannot move phones that are assigned to subscribers.
- You cannot move phones between customers.
- You can move phones only between sites.
- You can move phones only between sites that reference the same NDL.
- You can move phones only between sites that have the same type of site dial plan.
- You can move phones only between sites that have the same country.

You can move phones in two ways:

- **Move phones by names** - To move multiple phones
- **Move phone by name** - To move one specific phone

1. Log in as a provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer whose phones you are moving.
3. Choose **Subscriber Management > Move Phones** or **Overbuild > Move Phones**.
4. In the **Action** field, select the move method.
    - If you choose **Move phones by names**:

1. Choose the site from which you are moving the phones from the **Move From Hierarchy** drop-down. The **Move To Hierarchy** field appears.
2. Choose the target site from the **Move To Hierarchy** drop-down.
3. Choose the phones you want to move.
   a. To move all phones between the sites, select the **Move All Phones** check box.
   b. To choose specific phones, click the **+** next to **Phones**, then choose a phone from the drop-down menu. You can type the first part of a phone name to narrow the selection list. Repeat this step to choose multiple phones.
4. Click **Save** to move the phones.

- If you choose **Move phone by name**:
  1. Choose the phone from the **Phone** drop-down. The **Move To Hierarchy** field appears.
  2. Choose the target site from the **Move To Hierarchy** drop-down.
  3. Click **Save** to move the phone.

5. Choose **Subscriber Management > Phones** to verify that the phones are moved to the target site.

16.1.16. Moving Phones from Site to Site

As an administrator, you can move phones from one site to another. Certain conditions must be met for a site-to-site move to succeed.

When you move a phone between sites, VOSS-4-UC checks the following conditions:

- The source and target sites must reference the same NDL.
- The source and target sites must have the same country configured.
- The source and target sites must have the same type of site dial plan deployed.
- The phones are assigned to subscribers or not
- The phones are under same customer or not
- The phones are moving between sites or not

Note: Quick Add Subscriber with phone/line/EM/SNR/voicemail can be added to site and moved across the sites within the same country.

Models and Relations Moved (SLC)

For moves between sites with SLC type dial plans:

- `device/cucm/Phone` (includes `device/cucm/Line`)

Note:

- Lines are disassociated from the phone
- Warnings are logged for any Lines associated with the phone

Models and Relations Moved (Non-SLC)

For moves between sites with non-SLC type dial plans:

- `device/cucm/Phone`
- `device/cucm/Line`
- `device/cucm/InternalNumberInventory`

Note: Warnings are logged for any Lines associated with:

- an E164 Inventory
- a Call Pickup Group
- a Hunt Group
- a Remote Destination

Moving Phones Between Non-SLC Sites with a DNR Configured

For moves between non-SLC sites with directory number routing (DNR) configured at *either* site, a warning appears stating that any lines associated to the phone being moved may not work correctly unless you take one of the recommended actions provided. See the Advanced Configuration Guide to perform the first recommended action.

Note:

- To see warning messages navigate to **Overbuild > Log Messages > Phone Move Logs**
- Movement of phones from Non-SLC to Non-dial plan site will not dissociate the lines, but movement from SLC to Non-dial plan site will dissociate the lines.

To support the Overbuild Tool for Managed Services, the certain fields are updated in the Phone and Line devices to the target site's default settings.

Within `device/cucm/Phone`, the following models and fields are updated:

- Phone
  - Device Pool Name
  - Location Name

Within `device/cucm/Line`, the following models and fields are updated:

- Line
- Call Forward All
  - Calling Search Space
  - Route Partition Name
  - Share Line AppearanceCssName

16.1.17. Delete Phones

Use this procedure to delete one or more phones, or phone settings. When phones are deleted, the following occurs:

- The Remote Destination is removed first, so that the VOSS-4-UC cache remains in sync with the Cisco Unified Communications Manager.
- The Phone is deleted.

  Note: Lines are not affected.

Procedure

1. Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site, you can see all the fields described in this procedure. If you are logged on as the site administrator, you can see a subset of the fields that are available on the interface.
2. Choose a site from the hierarchy breadcrumb.
3. Choose **Subscriber Management > Phones**.
4. Choose one of the following methods to delete phones or phone settings:
   - Choose an individual phone to be deleted by selecting its check box in the far left column, then clicking **Delete**. From the popup window, click **Yes** to confirm the deleted phone.
   - Delete multiple phones at once by selecting the relevant check boxes, then clicking **Delete**. From the popup window, click **Yes** to confirm the deleted phones.
   - Remove phone settings as required by removing them from the relevant tab of a selected phone. Click **Save**.

When the delete action is complete, the phone disappears from the list.

16.2. Intercom Lines

16.2.1. Introduction

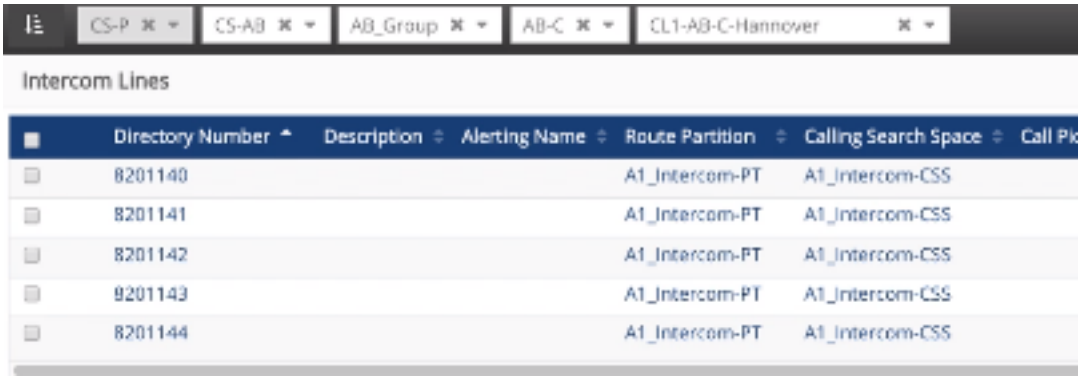
The Intercom Lines feature allows for the management of Intercom lines at a site level independently of the management of lines at a site.

Intercom Lines are associated from Phones or Subscribers - they can then be set up and then associated to phones and subscriber phones simply by first selecting the Intercom Route Partition.

16.2.2. Managing Intercom Lines

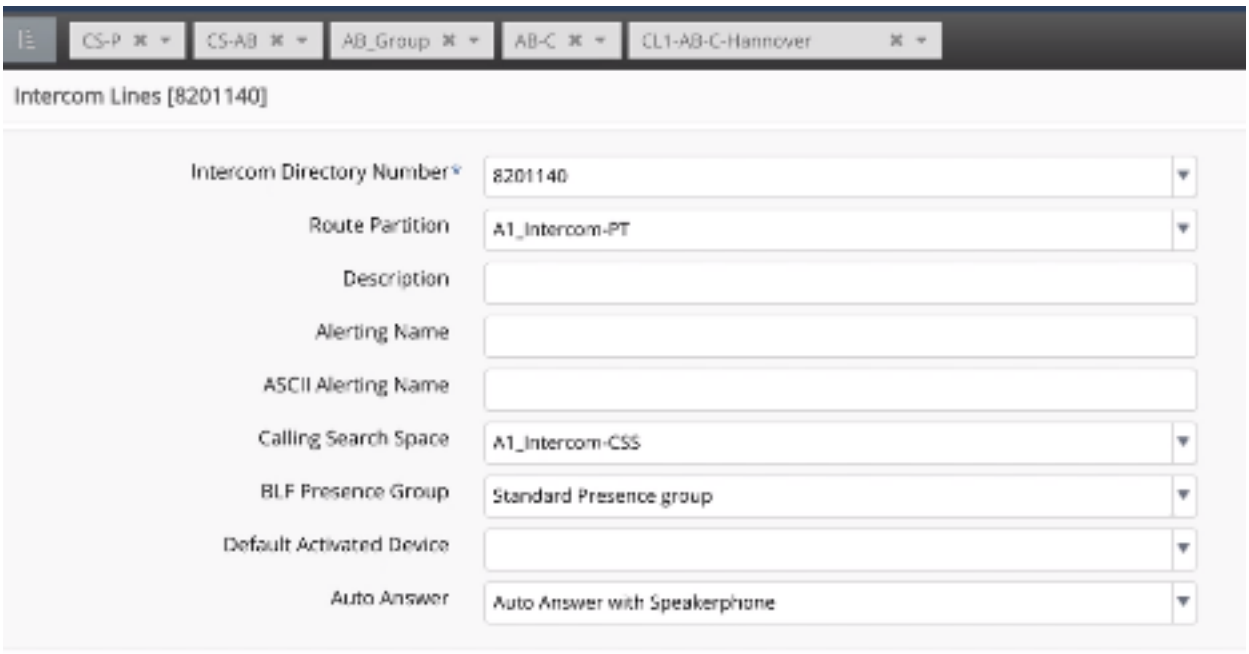
When the feature is set up, administrators will navigate to a site and then have access to a **Intercom Lines** menu under the **Subscriber Management** menu for the site.

A list view of Intercom lines are shown, where these can be added, deleted and modified.



The Intercom lines detail form is more simplified than the Lines form, showing only the relevant fields.

Note: Intercom lines should be not be managed from the **Lines** menu.



When adding or modifying these:

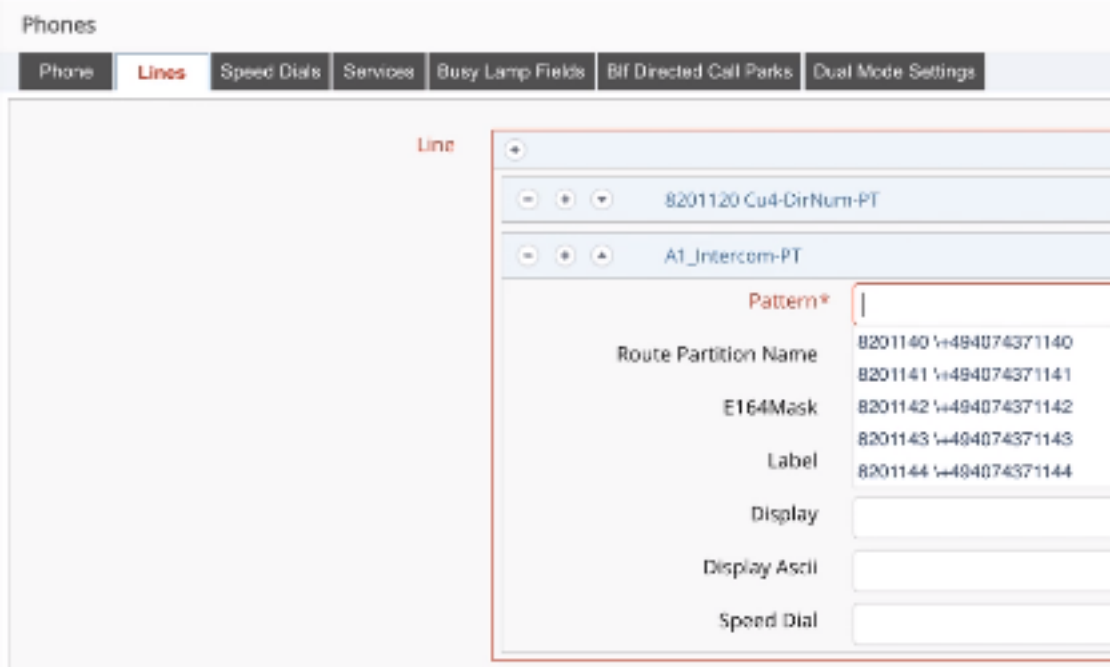
- The **Route Partition** drop-down only shows Intercom partitions.
- The **Calling Search Space** drop-down only shows Intercom calling search spaces.
- For **Default Activated Device**, select the supported device from the drop-down list.
- The **Auto Answer** drop-down only shows supported options.
- If the **Description** field is left blank, it takes a default value “Intercom Line”.

16.2.3. Associating Intercom Lines to Phones

Navigate to a site hierarchy and choose **Phones** under the **Subscriber Management** menu for the site.

To associate an Intercom line on the **Lines** tab of the **Phone** form, first specify an Intercom partition for the **Route Partition Name**.

The simplified Line input form is presented, showing only the supported Intercom line fields to be configured.



- The **Pattern** drop-down *only* shows existing Intercom lines. No new lines can be added.

Intercom and non-Intercom lines can both be associated to a single phone.

Associated Intercom lines will also show as “used” in the list view of the **Directory Number Inventory** menu under **Dial Plan Management** and its **Description** in the list will also show as “Intercom Line”.

Deleting the phone on the **Phones** list view will then also show the Intercom line as not in use.

16.2.4. Intercom Lines in Subscriber Management

Navigate to a site hierarchy and choose **Subscribers** under the **Subscriber Management** menu for the site.

When adding a phone to a subscriber, to associate an Intercom line to the phone on the **Phones** tab, also first specify an Intercom partition for the **Route Partition Name**.

The simplified Intercom Line input form shows only the supported Intercom line fields to be configured.

- The **Pattern** drop-down *only* shows existing Intercom lines, including those in use.

No new lines can be added as a part of Subscriber management - they are added on the **Intercom Lines** menu.

Associated Intercom lines will also show as “used” in the list view of the **Directory Number Inventory** menu under **Dial Plan Management** and its **Description** in the list will also show as “Intercom Line”.

Deleting the phone on the **Phones** list view will then also show the Intercom line as not in use.

16.3. Quick Add Subscriber

16.3.1. Quick Add Subscriber: Overview

Quick Add Subscriber provides a single page where you can:

- Add users to Unified Communications Manager
- Provision a Voice service for Unified Communications Manager users. See *Provision the Voice Service* for more details.
- Add users to Voicemail and WebEx accounts
- Provision users with services, such as Single Number Reach, Webex Teams, Extension Mobility, and Jabber Devices (Mobile Identity)
- Add lines for Unified Communications Manager users
- Associate a Device Pool directly from the interface to a subscriber's newly associated devices or services other than the Device Pool provided in the Site Defaults Doc (SDD) or reference Configuration Template (CFT) in the Quick Add Group (QAG). See *Quick Add Subscriber Device Pool* for more details.
- Associate Calling Search Space (CSS) values to a subscriber's newly associated lines, devices or services other than the CSS's provided in the Site Defaults Doc (SDD) or reference Configuration Template (CFT) in the Quick Add Group (QAG), by selecting a Class of Service (CoS) directly from the interface. See *Quick Add Subscriber Class of Service* for more details.

Quick Add Subscriber supports many user types, including:

- LDAP users
- Unified Communications Manager integrated users
- LDAP-integrated users on Unified Communications Manager
- Manually created users

If the Default Self-service Language is set on the SDD, Users will be assigned the corresponding Self-service language.

Quick Add Group is a collection of templates that configure the subscriber features. Quick Add Group is required to use Quick Add Subscriber.

Note: To add subscribers using Quick Add Subscriber, a default user template called "voicemailtemplate" must exist on the Unified CM. It is possible, through Dial Plan management, to change this default by editing the Default CUC User Template value in the Site Defaults reference.

For self-provisioned phones to show as being associated with a Subscriber, perform a Cisco Unified Communications Manager Data Sync after setting up a self-provisioned phone.

Any modifications of the added subscriber and associated services are done from the respective service menu items.

The input form on the user interface shows a number of check boxes to enable user services such as Voicemail, WebEx, Single Number Reach, Webex Teams (*Webex Teams Quick Add*), etc. If the Entitlement profile selected on the Quick Add Subscriber form does not include a particular service, then the check boxes for that service is not available. For example, if the selected Entitlement profile for the Subscriber does not

include Voice services, then the check boxes for Voice, Jabber, and Self Service ID will not show on the form. The choice of Entitlement profile will filter the available options in the **Phone Type** drop-down to show only the enabled devices in the Entitlement profile.

For the Voicemail service, controls will also not be available if the site's Site Defaults Doc has no default value on the CUC Defaults tab for the Default CUC Subscriber Template. This default value (voicemailusertemplate) should already exist on the Unified CM and is automatically populated on an HCS system when a VoiceMail Pilot is created. A Cisco Unity Connection device must also be configured at the related NDL (Network Device List) at site level.

While the GUI hides controls if services are not available, API and Bulk Load operations have Provisioning Workflow checks for the presence of the Default CUC User Template in the Site Defaults Doc and a configured WebEx Server in the NDL before the selected services can be added.

If no Unified CM has been configured at the hierarchy that the Subscriber belongs, then Quick Add Subscriber bulk load transactions and API calls will show a warning message: No Call Manager has been configured.

Webex Teams Quick Add

If you select the **Webex Teams** check box, the **Webex Teams User Template** drop-down is exposed. From this, you can select the **Webex Teams User Template** to use for the user. This selection overrides the default user template referenced in the Quick Add User Group associated to the user. If a **Webex Teams User Template** is not selected from the drop-down, selection falls back to the **Webex Teams User Template** referenced in the associated Quick Add User Group. If you want customized values, clone the **Webex Teams User Template** (**Customizations > Configuration Templates**) and edit as required.

16.3.2. Quick Add Subscriber Device Pool

A Device Pool contains system, device, and location-related information, and is mandatory when adding a Subscriber using Quick Add Subscriber. A Device Pool can be referenced by:

- Site Defaults Doc (SDD)
- Reference Configuration Template (CFT) referenced in the Quick Add Subscriber Group (QAG)
- Admin GUI (if exposed)

Site Defaults Doc

The Device Pool referenced in the SDD makes sure that a Subscriber's devices are always associated to a Device Pool. If there is no Device Pool referenced in either the QAG or Admin GUI drop-down (see below) the value defaults to the SDD.

Quick Add Subscriber Group (QAG)

The Device Pool referenced by a Configuration Template (CFT) in the QAG takes precedence over the Device Pool referenced in either the SDD or the Admin GUI drop-down (if exposed). See *Quick Add Subscriber Group* for details.

Admin GUI

An Administrator can expose a Device Pool drop-down on the QAS page on the Admin GUI by editing or cloning the Field Display Policy. See *Expose Device Pools and Class of Service in Quick Add Subscriber*. The Device Pool drop-down allows an Administrator to overwrite the value in the SDD by selecting a custom Device Pool from the drop-down list. The options available in the list are the site-level Device Pools if they are available, otherwise it displays all Device Pools available at Customer level (NDLR aware).

Note: When exposing the Device Pool drop-down, the Administrator **must** remove the value in the Device Pool field of the CFT referenced in the QAG, that is, the field must be blank. This is done to make sure that the value in the CFT does not overwrite the custom value in the drop-down.

The CFTs and their target models for which the Device Pool name can be made blank to allow the GUI to drive the Device Pool selection include:

- Phone templates (device/cucm/Phone)
- Jabber device templates (device/cucm/Phone)
- Remote Destination Profile templates (device/cucm/RemoteDestinationProfile)

16.3.3. Quick Add Subscriber Class of Service

A Class of Service (CoS) allows the user to specify a Calling Search Space (CSS) for devices and lines, respectively. A CSS, in turn, is mandatory for lines and devices when adding a Subscriber using Quick Add Subscriber. A Calling Search Space can be referenced by:

- Site Defaults Doc (SDD)
- Reference Configuration Template (CFT) referenced in the Quick Add Subscriber Group (QAG)
- Admin GUI via the Class of Service field (if exposed)

Site Defaults Doc

The Calling Search Space values referenced in the SDD ensure that a Subscriber's lines and devices always have a Calling Search Space associated to it. If there are no Calling Search Space values referenced in either the QAG or via the Class of Service field in the Admin GUI drop-down (see below) the value defaults to the SDD.

Quick Add Subscriber Group (QAG)

The Calling Search Space values referenced by a Configuration Template (CFT) in the QAG take precedence over the Calling Search Space values referenced in either the SDD or the Class of Service via the Admin GUI drop-down (if exposed). See *Quick Add Subscriber Group* for details.

Admin GUI

An Administrator can expose a Class of Service drop-down on the QAS page on the Admin GUI by editing or cloning the Field Display Policy. See *Expose Device Pools and Class of Service in Quick Add Subscriber*. The Class of Service drop-down allows an Administrator to overwrite the Calling Search Space values in the SDD by selecting a custom Class of Service from the drop-down list. The Class of Service, in turn, contains a custom Calling Search Space for Lines and Devices respectively. The options available in the list are the customer level Class of Service instances, as created by the relevant administrator.

Note: When exposing the Class of Service drop-down, the Administrator **must** remove the values in the Calling Search Space fields of the CFT's referenced in the QAG, that is, the field must be blank. This is done to make sure that the value in the CFT does not overwrite the custom Calling Search Space value as defined in the selected Class of Service.

The CFTs and their target models for which the Calling Search Space name can be made blank to allow the GUI to drive the Calling Search Space values include:

- Line templates (device/cucm/Line)
- Phone templates (device/cucm/Phone)

- Jabber device templates (device/cucm/Phone)
- Remote Destination Profile templates (device/cucm/RemoteDestinationProfile)

16.3.4. Expose Device Pools and Class of Service in Quick Add Subscriber

Administrators with access to Field Display Policies (FDP) can expose the **Device Pools** field and **Class of Service (CoS)** field on the Quick Add Subscriber (QAS) interface at a specific hierarchy.

1. As an administrator with access to Field Display Policies (FDP), choose **Customizations > Field Display Policies**.
2. Filter the **Target Model Type** on **view/QuickSubscriber**.
3. Depending on which hierarchy or hierarchies the **Device Pools** or **Class of Service** field should be exposed in QAS:
   a. If the FDP exists at the correct hierarchy, open it.
   b. If the FDP does not exist at the required hierarchy, clone one of the available FDP's on a higher hierarchy to the required hierarchy (use **Actions > Clone**).
4. Open the FDP and go to the first group's **Available** list in the **Fields** block. Select **device_pool** or **class_of_service**.
5. Click on the **Select** button to move the **device_pool** or **class_of_service** label from the **Available** list to the **Selected** list.
6. Use the **Move up** and **Move down** buttons to move the label to the desired position relative the the other field labels.
7. Ensure that the cloned FDP name is "default", and click **Save**.

If an administrator is at the hierarchy where the cloned FDP is created or at a lower hierarchy, and then navigates to **Subscriber Management > Quick Add Subscriber**, a drop-down field with the title: **Device Pools** or **Class of Service** is exposed.

16.3.5. Configuration

To create or configure users, enable users with services, or associate users with devices, configure the following items on the system.

1. Server Configurations

   Configure the following servers in VOSS-4-UC:

   - Cisco Unified Communications Manager (Unified CM) Server - Adding a Unified CM server. This server is required to:
     – Sync manually provisioned users or LDAP-integrated users in Unified CM to VOSS-4-UC.
     – Sync any of these users' existing associated Phones, Directory Numbers, Extension Mobility Profiles in Unified CM to VOSS-4-UC.
     – Create Subscribers (push users to Unified CM)
     – Push users' associated Phones, Directory Numbers, Extension Mobility Profiles, to Unified CM.

- LDAP Server. This server is required if you want to configure LDAP-synced users in VOSS-4-UC. If you do not want to configure LDAP-synced users, this server is optional.
- Cisco Unity Connection Server. This server is only required if you want to add Cisco Unity Connection voicemail users that are configured in VOSS-4-UC.

2. Dial Plan Deployment

   Configure a Dial Plan at both the Customer and Site hierarchies.

3. Voicemail Service

   Deploy Voicemail Service with a pilot number created and associated to a site under **Services > Voicemail** in VOSS-4-UC. This item is required to create a "Default CUC Subscriber Template" under **Site Defaults > CUC Defaults**. The template is required to create Cisco Unity Connection Voicemail users.

4. WebEx Service

   Configure a WebxEx Server in VOSS-4-UC to deploy any WebEx users provisioned through QAS. Set a password for WebEx users in Site Defaults.

16.3.6. Quick Add Subscriber Group

Quick Add Subscriber Groups allow administrators to group feature and configuration templates for use with the Quick Add Subscriber and Add Subscriber Wizard functions. This grouping helps to quickly and easily configure subscribers.

For example, if you want to add 100 back-office users and 50 sales users:

- The back-office users all use the 7965 phone with SCCP protocol and no services.
- The sales users all use the 8865 phone with SCCP protocol and Single Number Reach service.

To quickly configure these two groups, create two Configuration Templates:

- One for the 7965 phone with no services for the back-office users.
- One for the 8865 phone with the Single Number Reach service for the sales users.

You also create two Quick Add Groups:

- One for the back-office users which reference the back-office user Configuration Template.
- One for the sales users which reference the sales users Configuration Template.

When adding subscribers with the Quick Add Subscriber and Add Subscriber Wizard functions, choose the appropriate Quick Add Group for the user you are provisioning.

All subscriber services use configuration templates that belong to a Quick Add Group.

16.3.7. Quick Add Subscriber Group Default Model

Default Group Model for Quick Add Subscriber and Add Subscriber Wizard Functions

Title	Field Name	Configuration Template Name
Group Name *	group_name	N/A
CUCM User Template *	default_cucm_user_template	Default CUCM User Template
Phone Template	default_cucm_phone_template	Default CUCM Phone Template
Extension Mobility Template	default_cucm_device_profile_te mplate	Default CUCM Extension Mobility Template
Line Template	default_cucm_line_template	Default CUCM Line Template
Remote Destination Template	default_cucm_rd_template	Default CUCM Remote Destination Template
Remote Destination Profile Template	default_cucm_rdp_template	Default CUCM Remote Destination Profile Template
Webex User Template	default_webex_user_template	Default Webex User Template
Jabber Android Template	default_cucm_jabber_andro id_template	Default CUCM Jabber Android Template
Jabber CSF Template	default_cucm_jabber_csf_template	Default CUCM Jabber CS Template
Jabber iPad Template	default_cucm_jabber_ipad_template	Default CUCM Jabber iPad Template
Jabber iPhone Template	default_cucm_jabber_ipho ne_template	Default CUCM Jabber iPhone Template
Carrier Integrated Mobile Device Template	default_cucm_jabber_cim_template	Default Carrier Integrated Mobile Device Template
CTI Remote Device Template	default_cucm_jabber_ctird_template	Default CTI Remote Device Template
CUC User Template	default_cuc_user_template	Default CUC User Template
CUC User Password Template	default_cuc_user_password_template	Default CUC User Password Template
CUC User PIN Template	default_cuc_user_pin_template	Default CUC User PIN Template
Default Webex Teams User Template	default_spark_user_template	Default Spark User Template
Default Webex Teams User CTI Device Template	default_spark_user_cti_dev ice_template	Default Spark CTI Remote Device Template

Fields marked with * are mandatory.

16.3.8. Quick Add Subscriber Conditions

For details to provision services to users, follow these instructions:

- *Provision the Voice Service*
- *Provision the Extension Mobility Service*
- *Provision the Voicemail Service*
- *Provision the WebEx Service*

- *Provision the Single Number Reach Service*
- *Provision the Jabber or Dual Mode Device Service*
- *Provision the Contact Center Agent*
- *Enable Self Provisioning*

When creating users with the Quick Add Subscriber function, consider these conditions:

- A checkbox called **Send welcome email** is displayed when you type in a user email address *only if* the following configuration has been made and is enabled:
  - An SMTP server has been set up (*SMTP Server*)
  - The **Allow email to be sent to user after Quick Add Subscriber** on **Email** tab of the **Global Settings** is set to **Yes** for the relevant hierarchy. (*Global Settings*)

  A welcome email is then sent to the subscriber email address using the configured "Quick Add Subscriber" HTML email template that applies to the hierarchy. (*Email*)
- From the Quick Add Subscriber Group menu, create a custom group or use the default group.
- You can edit existing users on Cisco Unified Communications Manager through Quick Add Subscriber only if the users exist at the Site level.

  A checkbox called **Include users at higher hierarchy** can be displayed by means of a custom Field Display Policy (field name: `lookUpForUser`, hidden by default), so that the **User** dropdown list will also show users above the current site hierarchy. This setting is also available for bulk load sheets and API calls.
- A checkbox called **Fail Transaction if user not found** can be displayed by means of a custom Field Display Policy (field name: `failIfNotFound`, hidden by default) to prevent adding users not on Cisco Unified Communications Manager. By default, the transaction will not fail. The option is used for the case where users have not been synced from LDAP to Cisco Unified Communications Manager. This setting is also available for bulk load sheets and API calls.
- LDAP synced or LDAP integrated at Cisco Unified Communications Manager user fields are always read-only and cannot be edited.
- You can associate a Line with multiple phones.
- You can associate a Phone with multiple Lines.
- If you choose to add a Phone for the user, the **Phone Name** drop-down list will show available phones at the user's site, according to the Phone Type as specified in the Site Defaults for the site.

  The phones available from the drop-down list are those in the associated Quick Add Subscriber Group at the Customer level, which have synced from Unified CM, as well as the phones that are available at the specific site level.

  You can also add a new phone if required by entering a valid name in the **Phone Name** field. The Phone Name must consist of a prefix, for instance SEP, followed by a MAC address, which is 12 hexadecimal characters. If you enter the Phone Name incorrectly, for example too few or too many characters, then subsequent associated transactions will fail.
- Associate an Entitlement Profile with the Subscriber.
- You can create multiple devices for a user. Therefore, the **Voice** check box is always visible. When the **Voice** check box is selected, four optional fields are exposed: **Phone Type**, **Phone Protocol**, **Phone Button Template**, and **Phone Security Profile**.

- Values set in the **Phone Type**, **Phone Protocol**, **Phone Button Template**, and **Phone Security Profile** fields will override any existing values in QAG or CFT, as well as the SDD or any other backend CFTs (CFTs that can not be edited).

  If a specific phone type is not allowed in an entitlement profile, that phone type will not be displayed in the Phone Type drop-down list for a Subscriber associated to that entitlement profile.

  If a field is blank, the existing values in QAG, CFT, SDD or other backend CFTs will be used.

  If a Phone Template is not specified in QAG, or if the specified Phone Template has blank values for the phone fields, then the phone field values are pulled from the SDD.

  You can override the default Phone Button Template value by entering a custom value in the **Phone Button Template** field. The entered value will be applied on Unified CM if the Unified CM allows it for that phone type.

Note: To reduce the likelihood of conflicting QAS settings when completing the optional fields mentioned above, we strongly recommend setting the required fields in the order as displayed on the Quick Add Subscriber screen:

1. Entitlement Profile
2. Quick Add Group
3. Voice (Phone Type, Phone Protocol, Phone Button Template and Phone Security Profile).

- You can set only one Extension Mobility profile for a user. Therefore, the **Extension Mobility** check box is not visible after you create an Extension Mobility profile.
- You can set only one WebEx account for a user.
- See *Contact Center Agent Quick Add*.
- You can associate multiple Jabber and Dual Mode devices to a user.
- Jabber and Dual Mode devices get the first line assigned to them that is specified in the QAS form.
- You can create a Directory Number in Unified Communications Manager in two ways:
  - By creating a Voicemail Line in QAS.
  - By creating a Line in QAS.

  When you create a Voicemail or Voicemail Line using Quick Add Subscriber, the Directory Number Used field is set to “true” under **Subscriber Management > Directory Number Inventory**.
- A Directory Number created without any device associations (for example, a Voicemail Line) is tagged under **Subscriber Management > Lines** as ‘DN created without device from QAS.’
- When the **Enable Self Provisioning** check box is checked, phone lines are added using the Universal Line Template (ULT) referenced in the Self Provisioning User Profile chosen from the **Self Provisioning User Profile** drop-down list which is exposed upon selecting the check box.

  If a User is added with lines but no devices, then selecting the **Enable Self Provisioning** check box automatically sets the **CUCM User Primary Extension** to the QAS line pattern and ULT route partition. If a user is added with devices and lines, then selecting this check box also automatically sets the CUCM User Primary Extension to the QAS line pattern and ULT route partition.

  Choose the required User Profile from the **Self Provisioning User Profile** drop-down list. The available User Profiles are those under **User Management > Self Provisioning > User Profile**. A User Profile must be selected when a user is enabled for Self Provisioning. A default User Profile (as shown under **Site Management > Site-Defaults**) is selected. Change this default if required.

Contact Center Agent Quick Add

Contact Center Management

The Quick Add Subscriber feature supports the easy creation of an UCCX agent.

The **Contact Center Agent** check box becomes visible if:

- the associated Entitlement Profile has Contact Center enabled - *Entitlement Profiles Fields*
- a Contact Center Server is available at the hierarchy - *Contact Center Servers*
- the selected user is not already associated with an Agent

If the check box is enabled:

- A **Contact Center Agent Profile** drop down list is available to select an agent profile.

  Note: The **Contact Center Agent Profile** needs to be created before adding the Contact Center Agent from the Quick Add Subscriber feature.

  The agent profile will determine the team, resource group and skills assigned to the newly created agent. See: *Agent Profiles*.

- The **Agent Extension** can be selected.

  The extension will be a list of specified Lines, in other words, the administrator must specify the Line to be created or reused before checking the **Contact Center** check box.

- The **Agent Device Type** can be selected: either Extension Mobility or Phone:
  - If Extension Mobility is selected, the **Extension Mobility** check box is automatically enabled.
  - If Phone is selected, the administrator must first enable **Voice** and specify a Phone to be created or reused before checking the **Contact Center** check box.

An IPCC extension is automatically managed for the Unified CM user associated with the Contact Center Agent.

16.4. Extension Mobility

16.4.1. Extension Mobility

Extension Mobility (EM) profiles, often referred to as roaming profiles, enable a user to log onto a phone in another location and the phone automatically adopts the profile for that user. An EM profile is required for users who move between locations on a regular basis, or for users in an organization or location, who have been assigned an extension mobility profile rather than a permanent phone.

VOSS-4-UC provides three ways to create, manage and associate extension mobility profiles:

- when adding a subcriber using the add Subscriber workflow - see *Add Subscribers* (**Extension Mobility** tab).
- when adding a subscriber using Quick Add Subsciber - see under Quick Add Subscriber: Overview
- when adding a standalone Extension Mobility - see *Standalone Extension Mobility*.

16.4.2. Standalone Extension Mobility

Standalone Extension Mobility (EM) allows administrators to create and manage all EM profiles at the specified organization level. This is done on the **Extension Mobility** list view (default menu **Subscriber Management > Extension Mobility**).

Managing Extension Mobility

When adding or editing EM profiles you can personalize the EM profile for each user.

Consider the following:

- Extension Mobility Details, such as:
  - Name*. Must be unique and can't be the same as a device name on Unified CM since both are device types. This field is not applicable when editing an EM profile.
- Lines
  - Line settings can only be changed for the original line, not the clones.
  - All line settings changed for a line, automatically apply for the clones of that line, if any.
- Speed Dials. Enables you to manage the speed dial numbers associated with the EM profile.
- Services. EM profiles can be subscribed, unsubscribed and re-subscribed to IP Phone Services such as Intercom Calls, Login/Logout or SingleWire.
- Subscribers. Allows you to associate the EM profile to one or more subscriber.

  You can also disassociate an EM profile from a subscriber by clearing the name from the **Username** drop-down and clicking **Save**.

  The **Subscriber** 'Link' on an existing EM profile links to the associated Subscriber's **Extension Mobility** form (default menu **Subscriber Management > Subscribers**).

When deleting an extension mobility profile, the following elements are automatically removed/cleared:

- Speed dials
- Busy lamp fields
- Service URL's
- IP phone service subscriptions

See also *Add Subscribers* (**Extension Mobility** tab) to add extension mobility to a subscriber during the add subscriber workflow.

16.5. Replace Phone

16.5.1. Replace Phone: Overview

Note:

- This software release currently only fully supports the replacement of an existing desk phone type with any other desk phone type.

The Replace Phone feature is typically used when you want to choose a new phone for a user or when a phone type is no longer supported.

The feature provides an easy way to replace an existing (old) phone with a different phone model, while retaining as much of the old phone's configuration as possible. It performs the following:

- copies the old configuration.
- deletes the old phone
- adds the replacement (new) phone along with the old configuration
- updates user information to reflect the change in the controlled devices

Note:

- Speeddial, Busy Lamp Field, Blf Directed Call Park, and Services settings are *not* copied from the old phone configuration. Configure these settings manually on the appropriate tab on the replacement phone **Phones** screen if required. See "Configure Phones".
- If the new phone has attributes that were not present on the old phone, you must manually set the required values if the default values are not appropriate. Alternatively, you can select an optional configuration template, which will override the configuration copied from the old phone as well as any manual settings.

If you need a customized Phone Template, a default template can be cloned, renamed and modified from **Customizations > Configuration Templates**. This customization is then available in the **Phone Button Template** drop-down of the Replace Phone feature.

See "Configuration Templates" for more details if required.

16.5.2. Using Replace Phone

The Replace Phone feature is *only available at a site hierarchy node*.

1. Log in as Site administrator or higher.
2. Choose **Subscriber Management > Replace Phone**. A pop-up window opens to navigate to the site at which the phone is to be replaced.
3. On the **Existing Phone** tab:
   a. Choose the **Device Name** of the phone that you want to replace.

      The Product, Device Protocol, Phone Button Template, and other values are shown automatically as read-only values.
4. On the **Replacement Phone** tab:

   Note: If you choose a Phone (Configuration) Template, all other fields available on the **Replacement Phone** tab are redundant. Even if certain fields are populated, the Phone Template values override them.

   a. Enter the **Device Name** of the replacement phone (mandatory).

b. Choose a **Phone Template** (optional) for the replacement phone if you want to override the attributes copied from the original phone and the manual settings below.

c. Choose the **Product** (phone model) of the replacement phone (mandatory). Note that if the existing phone was associated with an entitlement profile, then the replacement **Product** drop-down only displays phone types that are allowed by the entitlement profile.

d. Choose the **Device Protocol** (mandatory).

e. Choose a **Phone Button Template** value for the replacement phone, if one is available (optional).

f. Choose the **Security Profile** for the replacement phone (mandatory).

g. Enter a **Description** for the phone (optional).

5. Click **Save**.

16.6. EM Login/Logout

16.6.1. Extension Mobility (EM) Login or Logout

VOSS-4-UC allows a site administrator (or higher) to log a user in to or out from one or more phones configured for Extension Mobility at the Customer or Site hierarchy level.

Note: For the feature to work, the phone must be enabled for Extension Mobility **and** the user must have Extension Mobility (Device Profile).

Login User

Log a user in to a phone taking note of the following:

- The **User Name** drop-down (mandatory) contains only users who have Extension Mobility (Device Profile).
- The **Device Profile Name** drop-down is auto populated with the user's first Extension Mobility (Device Profile). If the user has more than one Extension Mobility (Device Profile), choose the profile to use from the drop-down.
- The **Phone Name** drop-down (mandatory) contains only phones that are enabled for Extension Mobility.
- A **Login Duration (in minutes)** of '0' (default setting) indicates that the user will remain logged in to the phone indefinitely. Enter, for example 180, if you want to log out the user from the phone after three hours.
- The **Status** field indicates either the currently logged in user or 'No User Logged In'.
- If you try to log a user into a phone that already has a logged in user, the **Force Login** check box is displayed. Select this check box and click **Save** to simultaneously log out the existing user and log in the new user.

Logout User

To log a user out from a phone:

1. Choose the **Phone Name** from which you want to log out the user and click **Save**.
2. The **Status** field displays either the currently logged in user or 'No User Logged In'.

Logout User from Phones

1. From the **User Name** drop-down (mandatory), choose the user you want to log out from a phone.
2. Move the phone/s from the 'Available' area to the 'Selected' area and click **Save**.

16.7. Smart Add Phone

16.7.1. Smart Add Phone: Overview

The Smart Add Phone feature provides an easy way to add a phone *only to a site hierarchy node* by selecting the Phone Template that matches the required Phone Product. This selected Phone Template then also adds associated default attribute values. Optionally, you can also choose to add one or more lines and a non-default Phone Button Template for the phone.

When a phone is added using the Smart Add Phone feature, the phone details that were added by the phone template can be seen and modified if needed by selecting the phone from **Subscriber Management > Phones**.

If you need a customized Phone Template, the default template can be cloned, renamed and modified from **Customizations > Configuration Templates**. This customization is then available in the **Phone Template** drop-down of the Smart Add Phone feature.

The line defaults are obtained from the Site Defaults doc for the site. The Default CUCM Line Partition must be set as the partition for the site.

Note: A cloned, custom phone template requires further customization in order to customize the line settings when it is used with the Smart Add Phone feature. For details, refer to the topic on Custom Line Settings for Smart Add Phone Configuration Template in the Advanced Configuration Guide.

16.7.2. Using Smart Add Phone

The Smart Add Phone feature is *only available at a site hierarchy node*.

1. Log in as an administrator.
2. Choose **Subscriber Management > Smart Add Phone**. A pop-up window opens to navigate to the site at which the phone is to be added.
3. Choose the **Phone Template** value that matches the phone to add. The Phone Product and Protocol values are input automatically and become read-only.
4. Optionally choose a non-default **Phone Button Template** value for the phone, if one is available.

   You can override the default **Phone Button Template** value by entering a custom value in the **Phone Button Template** field. The entered value will be applied on Unified CM if the Unified CM allows it for that phone type.

5. Based on the selected phone template, the **Device Name** prefix is added for the phone. Complete the device name.
6. The **INI Enabled** field shows if the Internal Number Inventory is enabled for the site or not and the **Default Line Partition** field indicates which default line partition has been set in the Site Defaults doc. Optionally add one or more lines to associate to the phone.

   The Lines input is enabled if the default Route Partition value for the site has been set in the site's Site Defaults Doc.

   - If the **INI Enabled** is **YES**, then choose a number from the drop-down list of numbers from the Internal Number Inventory. Numbers that are marked as used, are also shown. Lines that are selected, have additional properties set according to the Site Defaults Doc for the site.
   - If the **INI Enabled** field is **NO**, then the list of numbers are those Directory Numbers on Unified CM with the Route Partition matching the site. You can choose a number from the drop-down or add a custom number that is not in the drop-down list, in other words, you can type in a number. Lines that are added have additional properties set according to the Site Defaults Doc for the site.
7. Click **Save**.

Choose **Subscriber Management > Phones** to see and modify the phone that is added using the Smart Add Phone feature. Added lines are shown on the **Lines** tab of the **Phones** input form.

16.8. Reset UC Passwords

16.8.1. Reset UC Passwords Overview

VOSS-4-UC maintains details of user credentials A VOSS-4-UC user can also be a corresponding user on a number of devices. In particular, users can have password (and PIN) credentials for:

- VOSS-4-UC user
- Unified CM (also PIN)
- Cisco Unity Connection (also PIN)
- LDAP user on Unified CM
- LDAP user on Cisco Unity Connection
- WebEx user

The Reset UC Passwords feature allows you to select a username for a user on Unified CM at a selected hierarchy and then, given the configured services for the user, you can select a check box to reset the user's password and/or PIN for the services.

The feature can be used by an administrator at the provider, customer and site hierarchy. It will, given a selected username, also enable options to select other devices for password modification and also displays notices or warning messages to indicate available devices and exclusions.

For example, the password of a Unified CM user that is also an LDAP user, cannot be modified. Such a user is also not a VOSS-4-UC user. In other instances, the VOSS-4-UC password is also reset when a user's device password is reset.

If a user is an LDAP user on either Unified CM or Cisco Unity Connection and they are selected, then only the PIN for the device will be reset.

16.8.2. Resetting UC Passwords

1. Log in as the provider, customer or site administrator and navigate to the hierarchy at which the Unified CM is available.
2. Choose **Subscriber Management > Reset UC Passwords**.
3. Choose the username on Unified CM from the User drop-down list.
4. Check boxes will show for the selected user according to the associated devices. The devices can be:
   - Cisco Unity Connection
   - WebEx
   - CUCM (Unified CM)
5. Select the check boxes for the devices on which the user's password or PIN needs to be changed. Note that a PIN can only be reset for CUCM or CUC, not WebEx or VOSS-4-UC, because these have no PIN functionality.

   Read the displayed Password or Pin notices and warnings. The messages show the conditions as to when passwords and PINs will be reset.

   Note that the content of these messages must be inspected as the check boxes are selected or or cleared, because the conditions change according to the status of the check boxes.

   If no check boxes are selected, then only the VOSS-4-UC password can be changed. If the user is an LDAP user on either Unified CM or Cisco Unity Connection, then only the PIN for the device can be changed.
6. Click **Save**.

16.9. Subscriber Workflows

16.9.1. Creating Quick Add Subscriber Groups

Procedure

1. Log in as provider, reseller, customer, or site administrator.
2. Choose **Subscriber Management > Quick Add Subscriber Groups**.
3. Click **Add**.
4. In the **Group Name** field, enter a group name. This is a required field.
5. From the **Template** drop-downs, choose the required templates.

   For example, take the following steps to create back-office QAS users with phone type 6911 using SCCP protocol (voice account):

   a. From the Default CUCM **Phone Template** drop-down, choose **Backoffice Phone 6911 SCCP**.

   b. From the Default CUCM **Line Template** drop-down, choose **Default CUCM Line Template**. This associates a line with the phone.

c. You can also use custom configuration templates to assign to a Quick Add Subscriber Group.

Note:

The custom configuration template must be at the same level in the hierarchy as the group.

6. Click **Save**.

16.9.2. Delete a Quick Add Subscriber Group

The default Quick Add Subscriber (QAS) Group resides at the sys hierarchy node.

Note: A QAS Group is required for the QAS function to work.

Procedure

1. Log in and browse to **Subscriber Management > Quick Add Subscriber Groups**.
2. Select the check box next to the Quick Add Subscriber Group you want to delete.
3. Click **Delete**.
4. Click **Yes** from the confirmation popup window to delete the QAS group.

16.9.3. Create Subscribers with Existing Users

Existing Users exist at the Site Level under **User Management > Users**, but are not yet pushed to Cisco Unified Communications Manager.

Procedure

1. Create a custom Quick Add Group or use the default Quick Add Group.
2. Choose **Subscriber Management > Quick Add Subscriber**. Choose a user from the **Username** drop-down list.

   The user data fields, such as **First Name** and **Last Name**, display the existing values for the user from **User Management > Users**.
3. From the **Quick Add Group** drop-down, choose a quick add group to assign to the user.

   The default value in the Quick Add Group list is “default”.
4. If necessary, edit the user information in the **First Name**, **Last Name**, and **Email Address** fields.
5. If necessary, provision the user with services using the **Voice**, **Extension Mobility**, **Voicemail**, **WebEx**, **Single Number Reach**, **Jabber Device**, and **Self-Service Id** fields.
6. Click **Save**.

16.9.4. Create Subscribers with New Users

New users do not yet exist in VOSS-4-UC and Cisco Unified Communications Manager.

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**.
2. Choose a user from the **Username** drop-down list.
3. In the **First Name** field, enter the user's first name.

   The user's first name is optional but is required if you want to provision the user with a WebEx account.
4. In the **Last Name** field, enter the user's last name.

   The user's last name is required.
5. Choose a group to assign to the user from the **Quick Add Group** drop-down list.

   The default value in the Quick Add Group list is "default".
6. If required, provision the user with services using the **Voice**, **Extension Mobility**, **Voicemail**, **WebEx**, **Single Number Reach**, **Jabber Device**, and **Self Service Id** fields.
7. Click **Save**.

16.9.5. Updating Subscribers

Subscribers are users that already exist under User Management > Users and in Cisco Unified Communications Manager.

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**.
2. Choose a user from the **Username** drop-down list, .
3. The user data fields show the user information found under **User Management > Users**.

   Any associated devices or subscribed services for the user appear under the **Existing Services** tab.
4. From the **Quick Add Group** drop-down, select a Quick Add Group to assign to the user.

   The default value in the Quick Add Group field is "default".
5. If required, edit the user fields and provision new services to the user.
6. Click **Save**.

16.9.6. Provisioning Services to Users

To provision services to users, follow these instructions:

- *Provision the Voice Service*
- *Provision the Extension Mobility Service*
- *Provision the Voicemail Service*
- *Provision the WebEx Service*
- *Provision the Webex Teams Service*
- *Provision the Single Number Reach Service*
- *Provision the Jabber or Dual Mode Device Service*

- *Enable Self Provisioning*

16.9.7. Provision the Voice Service

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**, and choose a user from the **Username** drop-down list.
2. Select the **Voice** check box. The optional Phone details, for example **Phone Type**, **Phone Protocol**, **Phone Button Template**, and **Phone Security Profile** fields are exposed, and the mandatory **Lines** and **Phones** fields highlight.
3. Choose the required options from the **Phone Type**, **Phone Protocol**, **Phone Button Template** and **Phone Security Profile** drop-down lists. The displayed default values depend on the selected Quick Add Group (QAG).

   Tip:

   Make sure that the selected template, for example **Phone Type**, exists in the Quick Add Group, and is also allowed by the Entitlement Profile. The selected Entitlement Profile will filter the available options in the **Phone Type** drop-down to show only the enabled devices in the Entitlement Profile.
4. In the **Lines** field, click +. The **Directory Number** drop-down appears.
5. From the **Directory Number** drop-down, choose a line.

   The line must be one of the Directory Numbers found under **Subscriber Management > Directory Number Inventory**.
6. In the **Phones** field, click +. The **Phone Name** drop-down appears.
7. From the **Phone Name** drop-down, choose a phone.
8. You can add more than one phone in the **Phones** field. To add another phone, click + again and choose another phone from the drop-down.
9. Click **Save**.

16.9.8. Provision the Extension Mobility Service

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**, and choose a user from the **Username** drop-down list.
2. Select the **Extension Mobility** check box.
3. Click **Save**.
4. Choose **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down list.
5. Choose the **Existing Services** tab, and make sure that the Extension Mobility profile name appears in the **Extension Mobility Profiles** field.

16.9.9. Provision the Voicemail Service

Procedure

1. Choose **Subscriber Management > Subscribers**. From the **Subscribers** list, click on the name of the subscriber to be provisioned with voicemail.
2. Choose the **Voicemail** tab.
3. In the **Voicemail Account** field, click +. The **Voicemail Line** drop-down appears.
4. Choose a line from the **Voicemail Line** drop-down and click **OK**.
5. Choose **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down list.
6. Choose the **Existing Services** tab.
7. Make sure that the voicemail line appears in the **Voicemail Extension** field.

16.9.10. Provision the WebEx Service

Procedure

1. Choose **Subscriber Management > Subscribers**. From the **Subscribers** list, click the name of the subscriber to be provisioned with WebEx service.
2. Choose the **WebEx** tab.
3. In the **Web Ex User** field, click +. The WebEx configuration fields appear.
4. Enter information in the **First Name**, **Last Name**, **Email**, **Password**, and **Repeat Password** fields. Choose **WebEx privileges** in the **Privilege** section.
5. Click **Save**.
6. Choose **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down list, .
7. Choose the **Existing Services** tab.
8. Make sure that “ACTIVATED” appears in the **WebEx** field.

16.9.11. Provision the Single Number Reach Service

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**, and choose the user for whom you want to provision Single Number Reach from the **Username** drop-down list.
2. Choose the **Single Number Reach** tab. The SNR Mobile Number field appears.
3. In the SNR Mobile Number field, optionally enter the mobile number. Do not add any spaces or special characters to the number.

   The SNR Mobile Number can be the same as the user’s Mobile Number shown in **User Management > Users**.

4. Click **Save**.
5. Choose **Subscriber Management > Quick Add Subscriber**, and choose the same user from the **Username** drop-down list.
6. Choose the **Existing Services** tab.
7. Make sure that the Single Number Reach displays the **Single Number Reach** profile name.

   The Single Number Reach profile name is the user name followed by "-RDP". For example: jsmith-RDP.

16.9.12. Provision the Contact Center Agent

If the Subscriber is assigned an Entitlement Profile that has the Contact Center service enabled, then the subscriber can be provisioned as a Contact Center Agent. A **Contact Center** tab is then available on the subscriber input form to manage Contact Center Agent properties.

Procedure

1. Choose **Subscriber Management > Subscribers**. From the **Subscribers** list, click the name of the subscriber to be provisioned as a Contact Center Agent.
2. Choose the **Contact Center** tab.

16.9.13. Provision the Webex Teams Service

Webex Teams Feature Reference

Webex Teams can only be provisioned for a subscriber if the **Webex Teams** check box has been selected in the Entitlement Profile associated to the subscriber.

Procedure

1. Choose **Subscriber Management > Subscribers**. From the Subscribers list, click the name of the subscriber to be provisioned with Webex Teams.
2. Choose the **Webex Teams** tab.
3. In the **Webex Teams User** field, click +. The Webex Teams configuration fields appear.

   Note: The **Login Enabled** and **Invite Pending** check boxes are read-only fields, and indicate the status of the user, that is whether the Webex Teams account has been activated or not.

   Options available in the **Services** and **Roles** sections are dependent on the Webex Teams Server to which the Webex Teams Service is synced (see below for a complete list).

   ---

4. In the **Services** section, select the required check boxes:

   Message

   - Webex Teams Messaging. Allows a user to exchange messages and share files with another person or a group of people.

   Meeting

- Webex Teams 25 Party Meetings. Allows a user to host up to 25-party meetings in Webex Teams cloud spaces.
- Webex Enterprise Edition 200. Webex Enterprise Edition.
- Webex Collaboration Meeting Rooms. Allows users to come together for one meeting experience irrespective of the devices and software they use – whether that's video conferencing services like WebEx or other systems like Polycom.

Hybrid Calendar Services

- Microsoft Exchange/Office 365. Enable for users who have mailboxes in on-premises Exchange or Office 365.
- Google Calendar. Enable for users using Google Calendar.

Hybrid Call Services

- Aware. Makes Webex Teams "aware" of all calls across your existing unified communications system. Hybrid Call Services Connect (see field below) is dependent on Hybrid Call Services Aware.
- Connect. Deployed on top of Hybrid Call Services Aware (see above field) and amongst other things, connects Webex Teams with VOSS-4-UC so that they work together. Enabled = Remote Device created.

  Note that with Hybrid Call Service Aware and Hybrid Call Service Connect together, users can make the same calls from either their desk phones or the Webex Teams app as well as hear incoming calls ring both their desk phones and the Webex Teams app and answer the call on either.

5. In the **Roles** section, configure the required roles by selecting the required check boxes:
   - No administrator privileges
   - Full administrator privileges. Access to all of the portal's features, including: assign roles, company policy and templates, device management licenses and upgrades, etc.
   - Read-only administrator privileges. Can view only whatever privileges are available to the full administrator.
   - Support Administrator. Access to user information and support logs.
   - User and Device Administrator
   - Device Administrator
6. Click **OK** to provision Webex Teams for the subscriber.
7. Make sure that "Enabled" appears in the Webex Teams column of the relevant subscriber on the **Subscribers** screen.

Webex Teams can also be provisioned for a subscriber using Quick Add Subscriber:

1. Choose **Subscriber Management > Quick Add Subscriber**.
2. From the **Username** drop-down list, choose the name of the subscriber to be provisioned with Webex Teams.
3. Choose the **Webex Teams** check box to enable Webex Teams for the subscriber.
4. From the **Webex Teams User Template** drop-down list, choose the template you want to assign to the user.
5. Click **Save** to provision Webex Teams for the subscriber.

6. Make sure that “Enabled” appears in the **Webex Teams** column of the relevant subscriber on the **Subscribers** screen.

16.9.14. Provision the Jabber or Dual Mode Device Service

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**. From the **Username** drop-down, select a user.
2. Select the **Jabber/Dual-Mode Device** check box. The **Jabber and Dual-Mode Devices** field appears.
3. Click + next to **Jabber and Dual-Mode Devices** to expose the **Jabber/Dual Mode Agent** drop-down and **Device Name** field.
4. Choose a device type from the **Jabber/Dual Mode Agent** drop-down. The **Device Name** field is automatically generated in the following format:

   <device type prefix><username><random number>, where:

   - <device type prefix> - always three characters, either BOT, CSF, TAB, TCT, CIM, or CTI.
   - <username> - 8 characters maximum. If a username contains ‘_’ and ‘.’ characters, these characters are removed from the automatically generated username. Automatically generated usernames can be edited if required.
   - <random number> - dependent on length of username, to make up a total of 11 characters along with the username.

   See examples in table below.

   Example Device Type and Device Name Combinations

For this type of device	Device Name (automatically generated)
Android (Cisco Dual Mode for Android)	For example: BOTJOHND003938
CSF (Cisco Unified Client Services Framework)	For example: CSFROBWOR77891
iPad (Cisco Jabber for Tablet)	For example: TABRQUENT18947
iPhone (Cisco Dual Mode for iPhone)	For example: TCTPDEVILLI156
Carrier Integrated Mobile	Format (regex): “[a-zA-Z0-9]{1,15}” For example: CIMJOHNSMI
CTI Remote Device	Format (regex): “[a-zA-Z0-9]{1,15}” For example: CTI-JOHNSMI

   For the following Agents, also select the **Mobile Identity** check box to enable Mobile Identity if required:

   - Android
   - iPhone
   - Carrier Integrated Mobile

5. Click **Save**.
6. Choose **Subscriber Management > Quick Add Subscriber**. From the **Username** list, choose the same user.

7. Choose the **Existing Services** tab.
8. Make sure that the **Phones** field displays the Jabber device.

For each device type, a Configuration Template that is associated with the Subscriber's Quick Add Group is used to provision the device. For defaults, see: *Quick Add Subscriber Group Default Model*.

Note: If a CSF Jabber device type is selected, all lines are associated to the CSF Jabber device by default.

16.9.15. Enable Self Provisioning

Procedure

1. Choose **Subscriber Management > Quick Add Subscriber**. From the **Username** drop-down list, select a user.
2. Select the **Enable Self Provisioning** check box. The **Self Provisioning User Profile** drop-down appears.
3. From the **Self Provisioning User Profile** drop-down, choose a Self Provisioning User Profile. These were previously created under **User Management > Self Provisioning > User Profile**.
4. In the **Lines** field, click +. The **Directory Number** drop-down appears.
5. Choose a line from the **Directory Number** drop-down.
6. Click **Save**.
7. Choose **Subscriber Management > Subscribers** and choose the same user from the Subscribers list view.
8. Make sure that the **Self Service** and **User Profile** fields display the same settings as those set in Quick Add Subscriber.

16.9.16. Workflow for Deleting Subscribers

You can delete and unprovision subscribers in two ways:

- Use the **Subscriber Management > Subscribers** menu path.
- Use the **User Management > Manage Users > Remove Users from CUCM** menu path.

Note: Using the Subscriber Management menu path is the preferred method for deleting and unprovisioning subscribers.

Deleting a subscriber works differently based on:

- The Subscriber Type
- The subscriber's Device Associations

Subscribers are typically of these types:

- **Non-LDAP Synchronized Users**
  - Users created in VOSS-4-UC and pushed to Cisco Unified Communications Manager.

  - Users provisioned in Cisco Unified CM and synchronized to VOSS-4-UC.

- **LDAP Integrated at VOSS-4-UC Users**

  Users that are LDAP integrated at Cisco Unified CM and synchronized to VOSS-4-UC.

- **LDAP Synchronized Users**

  Users that are directly synchronized from an LDAP Server to VOSS-4-UC.

Subscribers can have these associations:

- Associated devices, such as Phones, Extension Mobility, Single Number Reach, Voicemail, and WebEx.
- No device associations.

When you delete a user using **Subscriber Management > Subscribers**, the system performs these tasks, depending on the user type and device associations.

User Type	With Devices	Without Devices
Non-LDAP Synchronized Users LDAP Integrated at Cisco Unified CM Users	Deletes all devices: • Phones: device/cucdm/Phone • Single Number Reach: device/cucm/RemoteDestinationProfile • Extension Mobility: device/cucdm/DeviceProfile • Voicemail: device/cuc/User • WebEx: device/WebEx/User Deletes the Provisioning Status.	Deletes the Provisioning Status.
LDAP Synchronized Users	Deletes all devices: • Phones: device/cucdm/Phone • Single Number Reach: device/cucm/RemoteDestinationProfile • Extension Mobility: device/cucdm/DeviceProfile • Voicemail: device/cuc/User • WebEx: device/webex/User Deletes the user from Cisco Unified CM: device/cucm/User Removes the Cisco Unity Call Manager from the Provisioning Status.	Deletes the user from Cisco Unified CM: device/cucm/User Removes the Cisco Unity Call Manager from the Provisioning Status.

When you delete a user using **User Management > Manage Users > Remove Users from CUCM**, the system performs the following tasks, depending on the user type and device associations.

User Type	With Devices	Without Devices
Non-LDAP Synchronized Users LDAP Integrated at Cisco Unified CM Users	The user is not deleted from Cisco Unified Communications Manager. These associations for the user are not deleted from Cisco Unified CM: • Phones: device/cucdm/Phone • Single Number Reach: device/cucm/RemoteDestinationProfile • Extension Mobility: device/cucdm/DeviceProfile • Voicemail: device/cuc/User • WebEx: device/webex/User A log message appears under User Management > Log Messages. The message describes why the user was not deleted and lists the user's associated devices.	Removes the user from the Cisco Unified CM: (device/cucm/User). Removes the Cisco Unified CM server from the Provisioning Status.
LDAP Synchronized Users	The user is not deleted from Cisco Unified CM. These associations for the user are not deleted from Cisco Unified CM: • Phones: device/cucdm/Phone • Single Number Reach: device/cucm/RemoteDestinatinProfile • Extension Mobility: device/cucdm/DeviceProfile • Voicemail: device/cuc/User • WebEx: device/webex/User A log message appears under User Management > Log Messages. The message describes why the user was not deleted and lists the user's associated devices.	Removes the user from the Cisco Unified CM: (device/cucm/User). Removes the Cisco Unified CM server from the Provisioning Status.

16.9.17. Delete a Subscriber from Subscriber Management

Follow these steps to delete and unprovision Subscribers.

Procedure

1. Choose **Subscriber Management > Subscribers**.
2. Choose the subscriber you want to remove.
3. Click **Delete**.
4. Click **Yes** to confirm.

16.9.18. Delete a Subscriber from User Management

Follow this step to delete users from Cisco Unified Communications Manager.

Procedure

1. Choose **User Management > Manage Users > Remove Users** from CUCM.

16.10. Line Reports

16.10.1. Create Line Reports for a Site

Use this procedure to create a report of all lines configured at a site.

You can use this information to determine which lines you must move before deleting the site. The report shows:

- The hierarchy node of the line's corresponding DN inventory
- Whether the line is shared within the site
- A list of all the phones that reference the line
- The owner and hierarchy node of each phone that references the line

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer for which you want to create a site line report.
3. Choose **Administration Tools > Reports > Create Line Report**.
4. From the **Site Hierarchy** drop-down, choose the site for which you want to create the line report.
5. Click **Save**.

A line report for each line in the selected site is generated.

What to Do Next

View Line Reports

16.10.2. View Line Reports

Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the customer for which you want to view line reports.
3. Choose **Administration Tools > Reports > Line Reports**.

   A list of line reports is displayed containing this information:

Column	Description
Pattern	Directory Number of the line.
Partition	The route partition of the line. The pattern combined with the partition defines the uniqueness of the line in CUCM.
Line Hierarchy	Hierarchy where the CUCM line with this pattern and partition is defined.
DN Inventory Hierarchy	Hierarchy where the DN inventory for the pattern is defined. If empty, no DN inventory exists for this pattern.
Device Count	Number of Phones, Device Profiles, and Remote Destination Profiles remote across all sites that are referencing this line.
Used Across Sites	Indicates whether at least one phone which exists in a different site references this line.
Shared Within Site	Indicates whether this line is shared between multiple phones within the site where the line exists.
Timestamp	Time when the report was generated.
Hierarchy	Hierarchy of the customer for which the report was generated.

4. To see additional information about Phones, Device Profiles, and Remote Destination Profiles related to a line, click the required line report. The **Line Reports** screen displays this information about Phones, Device Profiles, and Remote Destination Profiles:

   Phones

Column	Description
End User	The user ID of the CUCM user who owns this phone.
Phone Name	Device name of the phone which references the line.
Hierarchy	Hierarchy where the phone exists which references the line.

   Device Profiles

Column	Description
End User	The user ID of the CUCM user who owns this Device Profile.
Device Profile Name	Name of the Device Profile which references the line.
Hierarchy	Hierarchy where the Device Profile exists which references the line.

   Remote Destination Profiles

Column	Description
End User	The user ID of the CUCM user who owns this Remote Destination Profile.
Remote Destination Profile Name	Name of the Remote Destination Profile which references the line.
Hierarchy	Hierarchy where the Remote Destination Profile exists which references the line.

What to Do Next

To avoid letting too many line reports accumulate, delete them individually or select the check boxes on the **Line Reports** list view and click **Delete** to delete multiple reports.

16.11. Customization Reports

16.11.1. Audit Template Customizations

You can run the template customization audit tool on a selected hierarchy node to identify template definitions and instances that were not delivered in the standard template packages during an installation or upgrade.

The audit report includes custom model schema definitions as well as data, domain, and view instances created on the hierarchy node as a result of workflow execution.

Use the report to verify that there are no unexpected instances at the specified hierarchy node.

Procedure

1. Log in as a customer administrator or higher.
2. Set the hierarchy path to the level from which you want to run your audit.

   From a given hierarchy node, you can audit customized templates at the node, and at nodes directly above or below the node in the hierarchy tree.
3. Choose **Administration Tools > Reports > Audit Template Customization**.
4. Choose the hierarchy node for which you want to audit customized templates.
5. Click **Save**.

What to Do Next

View the audit report. See “View Template Customization Audit Reports”.

16.11.2. View Template Customization Audit Reports

Procedure

1. Log in as provider, reseller, customer, or higher level administrator.
2. Choose **Administration Tools > Reports > Template Customization Reports**. A list of template customization audit reports is displayed.
3. Click a report to view the details. The message field shows how many customized templates were found at the hierarchy node. The details fields lists the model type and instance of each customized template.

16.11.3. Example Template Customization Audit Reports

The purpose of a Template Customization Audit Reports is to provide a record of changes as a result of workflow execution at a particular hierarchy, in particular:

- data, relation, and view instances of standard models that include for example Configuration Templates, Field Display Policies, Macros.
- custom model schema definitions that may have been created at the site (for example, instances of `data/DataModel`) as a result of a custom adaptation.

Consider an example customization report that was created at a Site hierarchy called: `LOC001`.

After the report is created from the **Administration Tools > Reports > Audit Template Customization** menu, it shows as an item in the list of reports on the **Administration Tools > Reports > Template Customization Reports** menu.

The report can be identified by checking the creation Timestamp and Message columns of the list. The message would contain the number of templates and the phrase that shows the Site hierarchy, for example:

```
544 customized templates were found at sys.hcs.CS-P.CS-NB.AAAGlobal.LOC001
```

The Details list in the report shows entries of the format:

```
Model Type: data/User, \
Instance: bkey(["QAS0003", "hcs.CS-P.CS-NB.AAAGlobal.LOC001"]), \
pkid(5949dd115da9aa9559aa2386)

Model Type: data/ConfigurationTemplate, \
Instance: bkey(["Reference CUCM User Template", \
                "device/cucm/User", \
                "hcs.CS-P.CS-NB.AAAGlobal.LOC001"]), \
pkid(5949dcd15da9aa9559aa1b2d)

Model Type: data/Macro, \
Instance: bkey(["CUSTOMER_INI_ENABLED", \
                "hcs.CS-P.CS-NB.AAAGlobal.LOC001"]), \
 pkid(5949db2a5da9aa9559aa01d9)
```

From the list details, it is possible to see the model instances created at the site - defined by type, business key and pkid.

This provides administrators with information when inspecting data at a hierachy for troubleshooting or for reference when contacting support operators.

16.12. Voicemail

16.12.1. Voicemail: Overview

VOSS-4-UC Provider solution supports voicemail as described below.

Optionally, VOSS-4-UC Provider also supports a Unity SIP Integration feature that can be used in place of your existing voicemail service. A list of menus items is available to carry out the Unity SIP Integration tasks in both Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection (CUC). Refer to “Appendix: Optional Features - Unity SIP Integration” for details.

The Voicemail interface (default menu **Subscriber Management > Voicemail**) allows an Administrator to add, modify or delete Cisco Unity Connection (CUC) Voicemail users and their associated Voicemail services from a single tabbed form.

The users and associated services added through VOSS-4-UC are also added to Cisco Unity Connection Voicemail system.

Complete the required fields on the tabs and click **Save**. The following can be added or edited using the Voicemail interface:

- CUC Account. See also *Unified Messaging Account* (only one per subscriber can be added in VOSS-4-UC).
  - If you select an existing subscriber the email address is auto-populated.
- Alternate Extensions. Alternate extension numbers available to the CUC Voicemail user. See also *Add Alternate Extension*.
- Message Actions. Actions to determine how incoming Voicemail, Email, Fax and Receipt messages are handled. If the selected message action involves relaying the message, you must enter a valid email address in the **Relay Address** field.
- Credentials. Password and PIN configuration.
- Notification Devices. Devices used to notify the CUC user of Voicemails sent to the user. **SMS** notification is only available if an SMPP Provider has been added on the relevant Voicemail server. See also *Add Additional Notification Devices*.
- Caller Input. These associate the caller input keys to specific actions. You can choose an action to associate with each key by choosing it from a drop-down list. See also *Manage Voicemail Caller Input Keys*.

16.12.2. Voicemail Workflows

A Voicemail account can only be added if:

- The administrator has navigated to the relevant Provider, Customer, Site level.
- A CUC Server (VM Server) has already been provisioned at the Provider or Customer level.
- A Network Device List (NDL) and NDLR points have already been created.

When adding a new Voicemail account, the following workflow is executed:

1. A CUC account is added with the details input by the user.
2. Alternate extensions are added with the details input by the user (if applicable).
3. Message actions are initially added with defaults, but can be updated with details input by the user if the Subscriber has been added, or upon modification.
4. Credentials (password and PIN) are added with the details input by the user. The password and PIN can either be locked by the administrator, or the user can be prompted to change the credentials upon first login.
5. Notification Devices are added. The system automatically provisions default notification devices, however additional notification devices can also be added when adding a Voicemail account.
6. Caller Input keys are updated or added as configured by the user.

You can modify either an existing Voicemail account service information (details that were added to a Voicemail account during the Add Voicemail process), or you can modify a Voicemail account by adding

new Voicemail services (those that were not added to the Voicemail account during the initial Add Voicemail process). For example, you can add additional alternate extensions and/or notification devices. After adding a Voicemail service to a subscriber, any lines that are used by any of the devices associated to the subscriber must be updated to reflect the proper call forward and Voicemail profile settings to enable the Call Forwarding to Voicemail and Voicemail buttons.

When modifying a Voicemail account, the workflow and processes are executed as with the Add workflow.

- Modular Add and Delete workflows can be carried out. For example, if more than one alternate extension or notification device is added to the Voicemail account, a pop-up form is available on the appropriate **Alternate Extensions** tab or **Notification devices** tab. Alternatively, for one-to-many or zero-to-many item instances such as an alternate extension, it can be deleted. These Add and Delete operations carry out a secondary workflow on the Voicemail instance.

When deleting a Voicemail account, the following should be noted about the workflow:

1. All elements associated with the Voicemail account are deleted.
2. Modular Delete workflows can be carried out as a part of a Modify workflow.

16.12.3. Unified Messaging Account

Overview

Unified Messaging (Single Inbox) is a Cisco Unity Connection service that enables users to have a single inbox in their e-mail client that is used for their e-mail as well as their Voicemail.

Note:

- VOSS-4-UC only supports either the Exchange or Office 365 Unified Messaging Service, MeetingPlace is **not** supported.
- Only **one** Unified Messaging Account (Single Inbox) per Subscriber can be added by VOSS-4-UC. However, if an existing Cisco Unity Connection subscriber is imported into VOSS-4-UC already has more than one account, then all associated services are imported, and will be available in VOSS-4-UC.
- Administrators must manually sync VOSS-4-UC with Cisco Unity Connection to obtain the required Unified Messaging Services. A manual sync must also be done whenever changes are made to the Cisco Unity Connection server.
- VOSS-4-UC does not automatically integrate Cisco Unity Connection Servers with Microsoft Exchange, the details for that process can be found here: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html

---

The following Cisco Unity Connection settings, set to 'True' (On), are included in Unified Messaging:

- EmailAddressUseCorp - Use Corporate Email Address
- EnableMailboxSynchCapability - Synchronize Connection and Exchange Mailboxes (Single Inbox)

The following two models were added to the Model Type List **CUCXN Overbuild Resources** for Unified Messaging:

- device/cuc/ExternalService
- device/cuc/ExternalServiceAccount (the actual Cisco Unity Connection User's model which contains their Unified Messaging Account)

VOSS-4-UC also added a new Model Type list **CUCXN Unified Messaging Services**, and added the same two Models: device/cuc/ExternalService and device/cuc/ExternalServiceAccount

Procedure

1. Choose **Subscriber Management > Voicemail**.
2. Click on the subscriber for whom you want to add the unified messaging service.
3. On the **CUC Account** tab, click **Unified Messaging Account +** and choose the **Unified Messaging Service** from the drop-down list.
4. Click **Save** when complete.

16.12.4. Add Alternate Extension

Procedure

1. Log in and navigate to the customer level hierarchy.
2. Choose **Subscriber Management > Voicemail**.
3. From the **CUC Account** tab, enter the account information.
4. From the **Alternate Extensions** tab, select the + next to **Alternate Extensions**.
5. Enter the user **Number** and choose the **Phone Type** from the drop-down, then enter the **Name** and choose the **Partition Name** from the drop-down.
6. Click **Save**.
7. Log into Cisco Unity Connection.
8. Choose the User you have been updating.
9. Choose **Edit > Alternate Extensions**.

   The Alternate Extension will be in place if configured from VOSS-4-UC.
10. From **Alternate Extension** choose the Partition from the drop-down and click **Save**.

16.12.5. Add Additional Notification Devices

Procedure

1. Log in and navigate to the Customer Level Hierarchy.
2. Choose **Subscriber Management > Voicemail**.
3. Choose the required subscriber to whom you want to add the notification devices.
4. Click the **Notification Devices** tab.
5. Add notification devices, such as **SMTP**, **Phone**, **Pager**, **SMS** or **HTML** by clicking the '+' next to the notification device, selecting the **Active** check box, and entering the required fields. Repeat for other notification devices if required.
6. Click **Save** when complete.

The selected additional notification devices will be added to the subscriber.

16.12.6. Manage Voicemail Caller Input Keys

You can edit caller input keys for an existing Voicemail user.

1. Log in as site administrator or higher.
2. Make sure that the hierarchy path is set to the correct node.
3. Choose **Subscriber Management > Voicemail**
4. Click on the Voicemail user you want to edit or click **Add**. For the **Add** transaction only, a **CUC Account**, including **Voicemail Account Name** must be created and saved before the **Caller Input** tab is active.
5. From the **Caller Input** tab, configure the default caller input keys:
   a. Click on the required key (*, #, or 0 to 9).
   b. Choose the action for the key from the drop-down list, see *Caller Input*.

   Additional fields are exposed when choosing certain options. For example, when you choose the **User with Mailbox** call action, the **User with Mailbox** and **Transfer** / **Greeting** fields are exposed.
6. Click **Save** when complete to save the caller input settings.

16.13. Conferencing

16.13.1. Conferencing: Overview

Site administrators manage the conferencing credentials of users if a WebEx server is available at the site level. The WebEx server on which users are administered can be identified with the Network Device Reference of the site, or else (according to the common reference resolution process) with the first such server in the current or higher up hierarchy level.

The default Conferencing input form that provides the interface to WebEx users displays the minimum of WebEx user properties that are mandatory. The Field Display Policies and Configuration Templates for this Conferencing input form can be modified according to the suggested customization procedure for Policies and Templates.

If conferencing was added for a Subscriber user when the Subscriber was added, the WebExId is defaulted to the userid. Note that the WebEx user properties that are shown on the Subscriber form may not correspond with those shown on the Conferencing input form. If the Conferencing feature is to be added for an existing subscriber, make sure that the WebExId is the same as the userid.

For Conference Workflows to function, make sure that the following is done at the Customer:

- A WebEx server is added.
- The WebEx server is added to a Network Device List (NDL).
- The required site references the relevant NDL.

16.13.2. Conference Workflows

User details can be added if a valid server is available.

When adding Conferencing from this input form, the mandatory fields are entered on the WebEx server.

Conferencing details can also be added as part of Subscriber Management. If the Web Ex Id is a VOSS-4-UC 10.6(x) or later version, and Unified CM username of a Subscriber, the WebEx details are displayed on its Subscriber Management screen WebEx tab.

Modify Conferencing details on the selected item, or also add and delete details from the Subscriber Management form.

Deleting a Conference item will remove the details from the WebEx tab of Subscriber Management if the user is a Subscriber.

16.14. Webex Teams Users

16.14.1. Webex Teams: Overview

Webex Teams is a Cloud-Based Business Collaboration Service, which allows employees to message, meet, and call instantly in order to strengthen relationships and increase productivity.

Webex Teams combines mobile devices and other communications tools to provide instant communications and live meetings to ensure a professional and effective collaboration experience.

Webex Teams main functionality includes:

- **Messaging**. Business messaging allows users to prepare, share, and repeat content. It facilitates one-on-one or team messaging facilities in virtual rooms.
- **Meeting**. Connect teams and meet customers easily with the added benefits of messaging and content sharing before, during, and after the meeting.
- **Call**. The service enables voice and video communications via mobile, desktop, and room-based devices. Connect your existing PSTN1 services to Webex Teams to enjoy one-touch directory dialing and join meetings from anywhere on any device. Mobile users get features such as single number reach, single voicemail service, video services, and the ability to seamlessly move between devices during a call.

Note: VOSS-4-UC does not support organizations with multiple License Subscriptions, in other words where there is a single organization with more than one entitlement for a specific license, such as “Messaging”.

Webex Teams Feature Reference

- Webex Teams Services:
  - *Webex Teams Feature Workflow*
  - *Create Webex Teams Service*
- Webex Teams Users:
  - *Provision the Webex Teams Service*
  - *Add Webex Teams User*
  - *Delete Webex Teams User*
  - *Webex Teams Licenses*
  - *Webex Teams*

16.14.2. Add Webex Teams User

Webex Teams Feature Reference

Use this procedure to add a Webex Teams User in VOSS-4-UC.

1. Log in as provider, reseller, customer, or site administrator.
2. Choose **Subscriber Management > Webex Teams Users**. The **Webex Teams Users** screen is displayed showing all Webex Teams Users (synced, or added in VOSS-4-UC).
3. Click **Add** on the button bar.
4. Choose the required site from the **Hierarchy** drop-down to which you want to add the Webex Teams user and click **OK**.
5. Enter the following information on the **Webex Teams Users** input form:
6. On the **Account Details** tab complete, at minimum, the mandatory fields:
   - First Name
   - Last Name
   - Email Address*. This is a mandatory field. Also used to match users being moved during the overbuild process.
   - Login Enabled. Read only field. Check box selected = Only visible if the user has activated their Webex Teams account by accepting an email inviting them to join Webex Teams.
   - Invite Pending. Read only field. Check box selected = User has not yet responded to an email inviting them to join Webex Teams. Only visible once this form has been completed (steps 7 and 8), saved (Step 9) and then refreshed.
7. On the **Services** tab, choose the required enabled **Services** for the user by selecting the check boxes:

   Message

   - Webex Teams Messaging. Allows a user to exchange messages and share files with another person or a group of people.

   Meeting

   - Webex Teams 25 Party Meetings. Allows a user to host up to 25-party meetings in Webex Teams cloud spaces.
   - Webex Enterprise Edition 200. Webex Enterprise Edition.
   - Webex Collaboration Meeting Rooms. Allows users to come together for one meeting experience irrespective of the devices and software they use – whether that's video conferencing services like WebEx or other systems like Polycom.

   Hybrid Calendar Services

   - Microsoft Exchange/Office 365. Select for users who have mailboxes in on-premises Exchange or Office 365.
   - Google Calendar. Enable for users using Google Calendar.

   Hybrid Call Services

   - Aware. Makes Webex Teams "aware" of all calls across your existing unified communications system. Hybrid Call Services Connect (see field below) is dependent on Hybrid Call Services Aware.

- Connect. Deployed on top of Hybrid Call Services Aware (see above field) and amongst other things, connects Webex Teams with VOSS-4-UC so that they work together. Enabled = Remote Device created.

  Note that with Hybrid Call Service Aware and Hybrid Call Service Connect together, users can make the same calls from either their desk phones or the Webex Teams app as well as hear incoming calls ring both their desk phones and the Webex Teams app and answer the call on either.

8. On the **Roles** tab, choose the **Roles** for the user by selecting the check boxes:
   - No administrator privileges
   - Full administrator privileges. Access to all of the portal's features, including: assign roles, company policy and templates, device management licenses and upgrades, etc.
   - Read-only administrator privileges. Can view only whatever privileges are available to the full administrator.
   - Support Administrator privileges. Access to user information and support logs.
   - User and Device Administrator
   - Device Administrator
9. Click **Save** on the button bar when complete to add the Webex Teams User.

16.14.3. Delete Webex Teams User

Webex Teams Feature Reference

Use this procedure to delete a Webex Teams user (synced, or added via VOSS-4-UC).

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy to the Customer or Site level.
3. Choose **Subscriber Management > Webex Teams Users**.
4. Select one or more check boxes next to the Webex Teams Users you want to delete, and then click **Delete**.
5. Click **Yes** to continue to delete or **No** to abort the process.

16.14.4. Webex Teams Licenses

Webex Teams Feature Reference

This provides a condensed view of the Webex Teams Licenses consumed and available at the selected hierarchy level.

Click **Subscriber Management > Webex Teams Licenses** to open the **Webex Teams Licenses** list view. The list view provides the following information:

- Name (of the license)
- Total Units (total number of licenses available)
- Consumed Units (the numeber of licenses still available)
- Location (where the licenses are available and used)

16.15. Reassign Services

16.15.1. Reassign Services: Overview

Reassign Services simplifies and automates the transfer of existing Subscriber services from a Source User to a Target User.

This utility is for example useful when an employee left the company and a new employee now starts the same role. Therefore, instead removing the old subscriber and configuring a new subscriber with the same settings and standards, the services and settings can be moved from the old subscriber to the new subscriber.

These services can include:

- Phone(s), which can be dual-mode with associated Remote Destination and/or Mobile Identity
- Device Profile(s)
- Remote Destination Profile(s) with associated Remote Destinations
- Voicemail User with related services including Alternate Extension and Message Handler (Action).

Note: Webex (Meetings and Teams) and UCCX services are not currently supported by this feature.

Custom settings can be applied to these services during the reassignment. A **Reassign Services Profile** setting is available to choose the configuration templates that will be used to update services during reassignment. These allow you to customize most settings on any of the above devices, including Line Alerting Name, Line Label, DisplayASCII values, and so on.

Example templates are provided that contain macro variables for fields that are likely to differ between subscribers. The field values then resolve with input from existing target user details. In this way the templates are not limited by for example a Site and Phone Model.

When reassigning services from existing source users to existing target users, the latter are moved to the *same site* as the source user, if these differ.

An option is also available to create a new target user as part of the Reassign Services process, instead of selecting an existing user without services. This user will be created at the same site as the source user.

Other features included are:

- Change User Details (modified Reassign Services) that updates the services of an existing subscriber using custom templates referenced in a Reassign Services Profile.

Topics:

- *Reassign Services*
- *Update User Details*
- *Reassign Services Profile*

16.15.2. Reassign Services

The Reassign Service feature directs you to the Customer hierarchy (if you are not already there) because it supports target users that are on a different site as the source user.

Field Name	Comment
Reassign Service Profile	This field will pre-populate with the first profile. You can select a different profile if required. If no profile option is available, then a reassign service profile needs to be added in the system.
Source User	Choose the subscriber to be reassigned. This provides a list of usernames of Subscribers in the system. It will list local or CUCM-LDAP Synced Subscribers only (not VOSS-LDAP Synced). Once a subscriber is selected, the **Source User Services** tab is updated to show services currently assigned and that will be reassigned to the target user. This is a good way to validate that all the services are shown or that there are not services that you do not want reassigned.
Source User Hierarchy	Once a subscriber is selected the **Source User Hierarchy** will be populated - this is a read-only informational field.
Add A New Target User	Select this option if you need to add a new local user to the system as the target user. Once selected, the form updates to reflect this choice.
Target User	To reassign to an existing user: select the username from the drop-down. This will show local or CUCM-LDAP synced users at the customer level or lower. Once a user is selected, the **Target User Services** tab is updated to reflect any services currently assigned to the user. If the user has any entries on this tab then the transaction will be blocked. So this provides an option to check before submitting. To create a new target user: enter the username for the new user to be created. The user will be added to the same hierarchy as the source user.
Target User Hierarchy	Shown only if add new target user is not selected - read-only informational field. Shows the hierarchy of the selected target user. Can be different to the source user and the feature will move the target user to the same hierarchy as the selected source user.
First Name	First Name of the Target user. Will be read only if the target user is a LDAP synced user.
Last Name	Last Name of the Target user. Will be read only if the target user is a LDAP synced user.
Email Address	Email Address of the Target user. Will be read only if the target user is a LDAP synced user.
Password	Visible if the target user is not a LDAP synced user. Enter the password for the target user.
Pin	Enter the PIN for the target user (used for device profile and voicemail).

Notes:

- The feature requires that source user services should all be at the same site hierarchy.
- Target user and hierarchy:
  - New target user - will be added to the hierarchy of the source user.
  - Existing target user - If the target user is in a different hierarchy to the source user, the target user will be moved to the same hierarchy as the source user as part of the reassign of services.

Note: It is not possible to reassign services to a user who is on a different Unified CM Cluster than the source user. The target user dropdown will currently not show users on a different cluster.

- The **Source User Services** tab will populate once a source user has been selected. This shows the services currently assigned to that user and the services that will be reassigned. This is a good way to validate the services that will be reassigned and to check if there are any services missing or that should not be reassigned. This can then be corrected as needed before reassigning the services.
- The **Target User Services** tabs will populate once a target user is populated. This is a good way to validate that the target user does not currently have any services assigned, as this will cause the transaction to fail with an error message indicating the target user has services. This can be resolved by choosing a different target user or by removing the services currently configured for the target user.
- Based on the setting in the reassign profile, the source user will either be left in the system (without any services) or removed from the system entirely.

Most of the services are updated to be associated to the target user and have settings updated according to the Configuration Templates (CFTs) in the reassign profiles.

There are some considerations:

- Single Number Reach (SNR) - Any existing remote destinations configured for the source user are deleted. The Remote Destination Profile (RDP) is then associated to the target user and updated per the CFT in the reassign services profile.
- Voicemail - the existing voicemail service for the source user is deleted to ensure a clean voicemail service. The voicemail service is then rebuilt for the target user based on the CFT in the reassign service profile. This means that any personalized settings, messages, greetings, and so on are cleared.
- Shared lines - Shared lines associated to the source user will only be updated if the shared line is the source user's primary extension.

The feature includes the optional ability to update shared line appearances of the source user's lines on other users' phones to reflect the destination user's details. For example:

- Bob.Smith has a phone with the following:
  - Line1: 55210 - Label: Bob Smith 55210
- Mary Smith has a phone with the following:
  - Line 1: 55220 - Label: Mary Smith 55220
  - Line 2: 55210 (shared line appear of Bob) - Label: Bob Smith 55210

In this case, when Bob's service is reassigned to a new user, Mary's Line 2 appearance will need to be updated to reflect the new user (e.g display name, label, etc.). This is supported for line appearances on Phones, Device Profiles, and Remote Destination Profiles. See the reassign services profiles section for more details on the controls.

16.15.3. Update User Details

The **Update User Details** menu shows a simplified form of Reassign Services where only one source user is selected, and that user's services are updated using custom Configuration Templates referenced in a Reassign Services Profile. The input fields allow for an easy update of basic details such as First Name, Last Name, Email, Password and PIN.

The **Reassign Services Profile** drop-down list is available to select a profile to be used to also update the user's services details.

Similar to Reassign Services, selecting a Username auto-populates the Hierarchy of the selected user and the **Current User Services** tab shows which services will be updated.

16.15.4. Reassign Services Profile

The **Reassign Services Profile** input form allows for a set of configuration settings and additional settings to apply when the Reassign Services functionality is used. The configuration templates (CFTs) that are selected in the profile determine how many of the detailed settings of the various services are updated as part of the reassign. This is essentially to allow you to re-align settings to your baseline service deployment logic and update any settings that incorporate the user's name - for example descriptions, alerting/display names, labels, and so on.

If no CFT is defined for a service, it is still moved to the new user. However, existing settings will be left in place. There are a few cases where the feature will make updates to specific service settings regardless of the CFT (i.e. when these settings are required to associate the user and service - owner of a phone, associated devices on the UCM user, etc). If the source user does not have a given service (e.g voicemail) then any CFT in the profile is ignored as the feature does not add new services that did not exist on the source user.

There is a set of example CFTs in the system by default - prefixed `RS` - that provides some examples of common settings and logic that might be used.

This profile and templates for configuration settings can be maintained per hierarchy as needed. The context for the reassign services feature is fairly similar to Quick Add Subscriber and this is to allow the reuse of macros/logic from your quick add group CFTs in the reassign services profiles. In many cases you could even use the same CFT to ease maintaining multiple sets of CFTs that define the baseline user and service configuration.

Note: At least one Reassign Services Profile must be created in order to use the feature.

Field	Description
Profile Name	Name for the Profile - recommended to make it meaningful to the user's that will be using the feature if you need more than one profile.
Profile Description	Description for the profile
Remove Source User	If selected the feature will fully remove the source user after moving all the services. If not selected then the base user and subscriber will be left when the feature completes however no services will be enabled.
User CFT	This CFT defines VOSS User settings to apply to the target user - e.g. role
CUCM User CFT	This CFT defines the UCM User settings to apply for the target user - e.g Department, Service Profile, etc.
Line CFT	This CFT defines the UCM Line settings to apply for the target user - e.g. Description, Alerting Name, Pickup Group, Call Forwarding, etc
Phone CFT	This CFT defines the Phone settings to apply to the devices being moved - e.g. Line Label, display name, device pool, CSS, etc. This same CFT applies to all phones (hardphones, soft-clients, etc) so typically relate to line appearance settings or other non-phone type specific settings. ownerID, mobility user (for soft clients) as set via the workflow irrespective of the CFT.
Device Profile CFT	This CFT defines the Device Profile (extension mobility) service for the user - e.g Line label, display name, etc. As with the Phone this is typically for line appearance settings on the device profile.
Remote Destination Profile CFT	This CFT defines the Remote Destination Profile (Single Number Reach - SNR) settings to apply to the service being moved - e.g line label, display name, CSSs, etc. Again typically for updating line appearance settings but can also edit other base RDP settings.
CUC User CFT	This CFT defines the CUC User (Voicemail) settings to apply when setting up voicemail for the user.
Add CUC User Alternate Extension	This setting determines if the feature will add a voicemail alternate extension for the user if voicemail exists on the source user. This can be used to add a standard alternate extension (e.g short extension version of the user's number) if needed as part of your standard deployment.

Field	Description
CUC Alternate Extension CFT	This setting is visible if the add alternate extension setting above is true. This CFT determines the settings for the alternate extension that will be added. This is where you would define the alternate extension to be added as standard.
Update CUC User Message Handler (Action)	This setting determines if the feature will configure the message handler settings for voicemail (form of single inbox).
CUC Message Handler (Action) CFT	This setting is visible if the message handler setting above is true. This CFT determines the settings that will be configured for the message handler. So this will need to include the email address for example of the user as well as the message actions.
Update shared lines (for unassociated Phones, Device profiles, RDP)	This setting determines if the feature will update line appearances of the source user's lines on other user's devices. This can be used to update the display names or labels for instance on those remote devices to reflect the new user's details. These CFTs only apply to line appearance settings on those devices (not general phone settings) and only for the line appearances that are shared with the source user. Other line appearances on the devices will not be updated. For example, the other user's phone had 3 lines, only 1 of which was shared with the source user. Only that 1 line appearance will be updated and the other 2 will be left untouched.
Shared Line (unassociated Phone) CFT	This setting is visible if the Update Shared Line setting is true. This CFT determines the settings on the other users' Phones that have the line appearance.
Shared Line (unassociated Profile) CFT	This setting is visible if the Update Shared Line setting is true. This CFT determines the settings on the other users' Device Profiles that have the line appearance.
Shared Line (unassociated RDP) CFT	This setting is visible if the Update Shared Line setting is true. This CFT determines the settings on the other users' RDP that have the line appearance.

Typically, Configuration Templates similar to your current Quick Add Subscriber templates can be used. Example Configuration Templates are also available for each drop-down, with naming convention `RS Example <service> CFT`. The templates shown on the **Configuration Templates** menu can be cloned, renamed and modified per hierarchy as required.

Configuration examples:

- Template Name: `RS Example CUCMPhone CFT`

  Field: **Line** > **Display Ascii**

  Value:

```
((input.firstName == fn.null ))
<{{input.lastName}}>
<{{input.firstName}} {{input.lastName}}>
```

- Template Name: `RS Example CUCMLine CFT`

  Field: **ASCII Alerting Name**

  Value:

```
{{fn.sub_string input.lastName, 0, 30}}
```

Additional optional settings available:

- **Add CUC User Alternate Extension**:

  If checked, a drop-down is enabled to select a template that updates the alternate extension.

  Example template: `RS Example CUCAlternateExtension CFT`

  Field: **DisplayName**

  Value:

```
{{ input.firstName }} {{ input.lastName }} Alt
```

- **Update CUC User Message Handler (Action)**:

  If checked, a drop-down is enabled to select a template that updates the email address for single inbox.

  Example template: `RS Example CUCMessageHandler CFT`

  Field: **RelayAddres**

  Value: if no input email address is available, a dummy address is added

- **Update shared lines (for unassociated Phones, Device profiles, RDP)**:

  If checked, a drop-down is enabled to select a template so that for any shared line instances from the source user, line label details can optionally be updated with those of the target user. The **Line CFT** template updates do not apply to shared lines.

16.16. PLAR (Hotdial)

16.16.1. PLAR (Hotdial): Overview

The Private Line Automatic Ringdown (PLAR) feature, also called Hotdial, automates the Unified CM configuration required to set up PLAR for a phone. The PLAR feature provides an administrator with a single interface and workflow for the management of the following elements of Unified CM:

- RoutePartition
- CSS
- TransPattern
- Phone
- Line
- SIP Dial Rule

The feature further provides an administrator with:

- A simplified user interface to select a Phone that must be enabled for PLAR, a destination number, and the destination CSS.
- The orchestration of a workflow to create the necessary Unified CM partition, CSS, Translation Pattern, and so on, and to apply these to the relevant Phone and Number.

To configure an existing phone for Hotdial, the user selects a pre-existing device and indicates that the device is a Hotdial device.

As soon as a PLAR configured phone goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a pre-configured destination number. The phone cannot dial any other number except the Hotdial destination that gets configured for PLAR.

The PLAR configuration can be added or deleted, but not modified.

16.16.2. PLAR (Hotdial) Workflows

When adding a new Hotdial Phone (PLAR configuration), the following workflow is executed:

1. A Unified CM route partition is created with:
    a. Name set to the Hotdial Phone selected, prefixed with “HotdialPT-“. For example: “HotdialPT-SEP000000000000”.
2. A Unified CM CSS is created with:
    a. Name set to the Hotdial Phone selected, prefixed with “HotdialCSS-“. For example: “HotdialPT-CSS000000000000”.
    b. The Partition created above is made a member of the CSS.
3. A Unified CM translation pattern is created with:
    a. Partition name is set to the Partition added, prefixed with “HotdialPT-“, for example: “HotdialPT-SEP000000000000”.
    b. Calling Search Space Name set to the selected Destination Dialing CSS.
    c. Called Party Transformation Mask is set to the selected Hotdial Destination Pattern.
    d. Route Option is set to Route this pattern.
    e. Urgent Priority is enabled.
4. The Unified CM phone selected is updated as follows:
    a. For SIP Phones only, a SIP Dial rule is created and the phone is set to use the SIP Dial Rule.
    b. CSS name is set to the “HotdialCSS-” added for the Phone.
    c. Hotline Device is set to true if the phone is marked as a Hotline Device by the user on the input form.

VOSS-4-UC automatically resets the phone when required.

When deleting PLAR (Hotdial) for a Phone (deleting the PLAR configuration), the following workflow is executed:

1. Update Phone CSS to the original CSS.
2. Delete the Hotdial Translation pattern.
3. Delete the Hotdial CSS.
4. Delete the Hotdial Route Partition.
5. For SIP Phones only, the device is updated to use a Dial Rule of “None”, and the Dial Rule is deleted.

16.17. Hunt Groups

16.17.1. Hunt Group Management

Hunt groups can be configured at the customer or site level.

The purpose of hunt group management is to provide business context for the lines selected as members of line groups and to provide you with a single consolidated view of the following hunting elements.

- Hunt Pilot
- Hunt List
- Line Groups

Note: When selecting a Call Pickup Group from the drop-down list, the available Call Pickup groups to choose from will be:

- those at the hierarchy of the current Hunt Group if there are any available
- those at a hierarchy level above the current if none are available at the current level

---

You must select the lines that belong to line groups or any existing line groups that must be added to the hunt list members.

For hunt groups configured at the customer level:

- You are prompted for an NDL that identifies the Cisco Unified CM where the hunt group is defined.
- You can define a unique hunt pilot pattern for the hunt group. The hunt pilot pattern is added to the customer-level DN inventory and is marked as in-use and unavailable.
- You can include lines defined at the customer level and at any site within the customer.

Searches can be performed on any of the details of the hunt pilot.

A hunt group is a combination of the hunt pilot, hunt list, and line groups that are automatically linked together using unique identifiers for the following:

- The hunt pilot's hunt list is set to the name of the hunt list. The hunt list name must be configured first in order for it to appear in the hunt pilot tab.
- The hunt list's line group members are set to the name of the associated line groups.

Certain default values for hunt groups are populated by the site defaults menu item, which can be viewed and edited (depending on your log-in level). See the **Default CUCM Hunt Pilot Partition** field on the **General Defaults** tab under the **Modify Site Defaults** topic in this manual.

Hunt groups can be:

- Added - You can specify the parameters of the hunt pilot and the hunt list, and select one or more new or pre-existing line groups from a drop-down or free text field. If your administrator has enabled the number inventory feature, you can select the **Hunt Pilot Pattern** from a drop-down list of available numbers. If the feature is disabled, the **Hunt Pilot Pattern** field is a free text field or a drop-down containing only selected available numbers. To allow the successful use of call forwarding in a hunt pilot, the defaults for Max Callers In Queue (32) and Max Wait Time In Queue (900) are cleared. To use queuing instead of call forwarding, set these values other than the default, for example to 33 and 901.

- Modified - You can modify the parameters of the hunt pilot or hunt list. Examples include adding or deleting line groups, or adding or deleting line group members.
- Deleted - You can delete a hunt group.

16.17.2. Add a Hunt Group

Use this procedure to add a hunt group in VOSS-4-UC and Cisco Unified Call Manager (CUCM).

1. Log in as site administrator or higher.
2. Browse to the hierarchy level (if necessary) to which you want to add the hunt group.
3. Click **Subscriber Management > Hunt Groups**. The **Hunt Groups** list is displayed.
4. Click **Add**.
5. Complete, at minimum, the required fields on each tab (see below).
6. Click **Save**

Hunt Pilot

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

- **Hunt Pilot Pattern** - Enter, or select from the drop-down list, the hunt pilot 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 +. Make sure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique.
- **Route Partition** - If you want to use a partition to restrict access to the hunt pilot, choose the desired partition from the drop-down list. If you do not want to restrict access to the hunt pilot, do not choose a partition, i.e leave the field blank.
- **Numbering Plan** - Choose from the drop-down list.
- **Route Filter** - If your hunt pilot includes the '@' wildcard, you may choose a route filter from the drop-down list. 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.
- **Hunt List** - The hunt list name must be configured first on the **Hunt List** tab in order for it to appear on this tab. See **Hunt List** below for details.
- **Call Pickup Group** - Choose the number that can be dialed to answer calls to this directory number (in the specified partition).
- **Alerting Name** - Enter an alerting name for the hunt pilot in UNICODE format. This name gets displayed on phones that the hunt pilot dials when it receives an incoming call, along with calling party information. The phone users can use this information to answer the call accordingly. This name also gets displayed on the calling phone. If you do not enter a name, the hunt pilot DN displays on the phones.
- **Provide Outside Dial Plan** - Select this check box for each hunt pilot that routes the call off the local network and provides outside dial tone to the calling device. Leave the check box clear if you want to route the call in the network.

- **Maximum Hunt Timer** - Specifies the maximum time for hunting without queuing. **Do not specify the same value** for the **Maximum Hunt Timer** field and the **RNA Reversion Timeout** field on the associated line group.
- Enter/complete the required fields under the **Forward Hunt No Answer**, **Forward Hunt Busy**, **Queuing** and **Park Monitoring** areas of the page, such as:
  - **Use Forward Settings of Device that Forwarded to Hunt Pilot** check box. When selected, the call forward settings of the line group member are used.
  - **CFNA and CFB Destination** - indicates the directory number to which calls are forwarded.
  - **CSS CFNA and CSS CFB** - This setting applies to all devices that are using this directory number. Drop-down displays all the CSSs in the system. Default = Default line CSS of the site.

Hunt List

A Hunt List lists a set of Line groups in a specific order. A hunt list then associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls. A hunt list comprises a collection of directory numbers as defined by line groups.

A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.

- **Name** - The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Make sure each hunt list name is unique to the route plan.

  Best practice is to use concise and descriptive names for your hunt lists. The CompanynameLocationCalltype format provides enough detail and is short enough so you can easily identify a hunt list.
- **Cisco Unified Communications Manager Group** - Choose a CUCM group from the drop-down list. The hunt list registers to the first node in the CUCM group.

  If you choose a CUCM group that has only one node that is configured, you receive a warning. To avoid this issue, choose a group that is configured with more than one node.
- **Enable this Hunt List** - Select this check box to enable your hunt list immediately when you click **Save**. No system reset is required.
- **For Voice Mail Usage** - If this hunt list is to be used for voicemail, select this check box. If you select this check box, the route list control process keeps a count of the setups that are being served to the hunt list, and will not allow more setups than the number of available devices. As a result, each device in the hunt list is treated as if it has a Busy Trigger and related Maximum Number of Calls of one.

Line Groups

A line group allows you to designate the order in which directory numbers are chosen. CUCM distributes a call to idle or available members of a line group based on a call distribution algorithm and on the Ring No Answer (RNA) Reversion Timeout setting.

Note: Although you can configure an empty line group with no members (directory numbers), CUCM does not support this configuration for routing calls. If the line group contains no members, the hunt list stops hunting when the call gets routed to the empty line group. To avoid this, make sure that you configure at least one member in the line group.

You must define one or more directory number before configuring a line group. After you configure or update a line group, you can add or remove members from that line group.

- **Line Group Name** - This field is a drop-down list, which allows you to choose an existing line group. The drop-down list displays all existing line groups available at the site.

  This field can also be used as a free text field. To create a new line group, enter a name in this field.

  The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Make sure that each line group name is unique to the route plan.

  Best practice is to use concise and descriptive names for your line groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a line group.
- **RNA Reversion Timeout** - Enter a time, in seconds, after which CUCM will distribute a call to the next available or idle member of this line group or to the next line group if the call is not answered and if the first hunt option, Try next member; then, try next group in Hunt List, is chosen. The RNA Reversion Timeout applies at the line-group level to all members.
- **Hunt Options No Answer** - Choose a hunt option for CUCM to use if a call is distributed to a member of a line group that does not answer. This option gets applied at the member level. Choose from the options in the drop-down list.
- **Automatically Logout Hunt Member on No Answer** - If this check box is selected, line members will be logged off the hunt list automatically. Line members can log back in using the “HLOG” softkey or PLK.
- **Hunt Options Busy** - Choose a hunt option for CUCM to use if a call is distributed to a member of a line group that is busy. Choose from the options in the drop-down list.
- **Hunt Options Not Available** - Choose a hunt option for CUCM to use if a call is distributed to a member of a line group that is not available. The Not Available condition occurs when none of the phones that are associated with the DN in question is registered. Not Available also occurs when extension mobility is in use and the DN/user is not logged in. Choose from the options in the drop-down list.
- **Member** - Configure Line Group Members as required by choosing a **Directory Number** and **Partition** from the drop-down list.

16.17.3. Hunt Group Management Workflows

When adding a new hunt group, the following workflow is executed:

- A hunt list is added with the details input by the user.
- A hunt pilot is added with the details input by the user.
- One or more line groups are created with the specified directory numbers as members.

When modifying a hunt group, the following workflow is executed (depending on what was modified):

- The line group details are modified.
- Added line groups are added.

  A removed line group is deleted *only* if it is the last instance. If a shared line group is removed, it is deleted from the specified hunt group *only*, but is still included in other hunt groups that are also using it.

If the hunt group uses existing line groups, then the existing line groups are updated when the hunt group is modified.

- The hunt list is modified.
- The hunt pilot is modified.

When deleting a hunt group, the following workflow is executed:

- The line groups that are members of the hunt list are deleted (if they are not used by any other hunt group in the system).

  If a shared line group is removed, it is deleted from the specified hunt group *only*, but is still included in other hunt groups that are also using it.
- The hunt pilot is deleted.
- The hunt list is deleted.

16.18. Call Pickup Groups

16.18.1. Call Pickup Groups: Overview

Certain default values for call pickup groups are populated by the site defaults menu item, which can be viewed and edited (depending on your log in level). Choose **Dialplan Management > Site Defaults** and click on the required site name in the list view.

The Call Pickup Groups feature provides an administrator with the following:

- A single interface on which to create call pickup groups, and to select one or more lines as members of a pickup group.
- The ability to add Unified CM call pickup groups and to modify the call forward and call pickup settings of each Unified CM directory number for membership to a newly added call pickup group. When adding a call pickup group, if your administrator has enabled the number inventory feature, the Pattern can be selected from a drop-down list of available numbers. If the feature is disabled, the **Pattern** field is a free text field or a drop-down containing only selected available numbers.
- The ability to add lines to an existing call pickup group by selecting the pattern (directory number). When adding a member line, if your administrator has enabled the number inventory feature, the Pattern can be selected from a drop-down list of available numbers. If the feature is disabled, the **Pattern** field is a free text field or a drop-down containing only selected available numbers. The **Route Partition Name** field is populated automatically based on the selected Pattern.
- The ability to delete a pre-existing call pickup group, and to delete one or more lines from an existing call pickup group.

The first member of the associated pickup group name is set the newly created pickup group, and associated pickup groups can be added as part of the workflow.

16.18.2. Add a Call Pickup Group

Use this procedure to add a call pickup group in VOSS-4-UC.

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

2. Set the hierarchy to the Customer or Site level.
3. Choose the Network Device List only if you have set the hierarchy to Customer level. For Site level this step is not required.
4. Choose **Subscriber Management > Call Pickup Groups**.
5. Click **Add** on the button bar to open the **Call Pickup Groups** input form.
6. On the **Call Pickup Group** tab, enter the **Name** and a **Description**.
7. From the **Call Pickup Group Number** drop-down, choose the pickup group pilot number.
8. From the **Route Partition Name** drop-down, choose the required route partition.
9. From the **Pickup Notification** drop-down, choose the method (**No Alert**, **Audio Alert**, **Visual Alert** or **Audio and Visual Alert**, and then enter the required **Pickup Notification Timer** period (in seconds).
10. If the Call Pickup Group is associated with other pickup groups, click the + next to **Call Pickup Groups** to expose the **Pickup Group Name**. This allows users to pick up incoming calls in a group that is associated with their own group.

    Note that the first member is automatically added, so there is no need to specify the first member as itself in an Add request.

    a. For included **Pickup Group Names**, ensure that the **Priority** always starts at 1. When more than one included group exists, the group with Priority 1 has the highest the priority of answering calls for the associated group. Integer values are added in order of priority.

    b. The associated Directory Name and Partition is automatically selected, based on the Call Pickup Group Name.

    c. Set any required Pickup Notification settings.
11. On the **Member Lines** tab, click the **+** (Add) button next to **Line** to expose the Line section.
12. Choose a **Directory Number** from the drop-down. The **Route Partition** Name is automatically selected, choose a different **Route Partition** if necessary. Call Pickup Group members will only be successfully added if their directory number exists in a valid route partition. Directory numbers in a 'null' route partition, appear as selectable members, but saving them results in an error.
13. Repeat steps 11 and 12 to add more members to the **Call Pickup Group**.
14. Click **Save** on the button bar when complete to save the **Call Pickup Group**.

Note: If you are using partitions with the call pickup numbers, ensure that the directory numbers that are assigned to the call pickup group have a Calling Search Space that includes the appropriate partitions. We recommend using `CU{macro}-PreISR-PT` partition for the call pickup groups added at the customer hierarchy.

The selected Call Pickup Groups drop-down lists the call pickup groups created at the customer and the site level. Select the required call pickup group from both the customer and the site level.

Adding a Call Pickup Group at customer level with members across child sites, succeeds without error, and the configuration is pushed to the associated Unified CM. However, when viewing the Call Pickup Group configuration after it was added, the added members will not be seen. Added members are only seen if the Call Pickup Group and its members are at the same hierarchy level.

Verify the individual Member Line association with the Call Pickup Groups by navigating to **Subscriber Management > Lines**. The Call Pickup Group under Lines displays associated Call Pickup Group.

16.18.3. Delete a Call Pickup Group

Use this procedure to delete a call pickup group in VOSS-4-UC.

1. Log in as provider, reseller, customer, or site administrator.
2. Set the hierarchy to the Customer or Site level.
3. Choose **Subscriber Management > Call Pickup Groups**.
4. Choose the call pickup group, and then click **Delete**.

16.19. Contact Center

16.19.1. Contact Center Management

The Cisco Unified Contact Center Express (UCCX) feature in VOSS-4-UC allows administrators to manage Agents and related configuration from a single pane of glass.

In addition to managing these configuration elements directly, the VOSS-4-UC Day 2 features also provide seamless UCCX management.

As a part of Contact Center management, VOSS-4-UC provides a number of interfaces. The associated Contact Center device models that will also be synced to the Contact Center server (UCCX device) upon a data sync.

- UCCX Server Management:
  - *Contact Center Servers*
- Day 2 Integration:
  - When a UCCX device has been added to a hierarchy and Entitlement Profiles have been added that have Contact Center entitlement enabled, subscribers can be configured as Contact Center Agents.

    Further management can be carried out in VOSS-4-UC, including VOSS-4-UC Overbuild (*Objects that are Moved During the Overbuild*).
  - *Contact Center Agent Quick Add*
  - *Contact Center Subscriber*
- Direct Management:
  - **Agents** (`device/uccx/Agent`): see *Agents*.
  - **Skills**: these are associated with competency levels - see *Skills*.
  - **Teams** (`device/uccx/Team`): see *Teams*.
  - **Resource Group** (`device/uccx/ResourceGroup`): see *Resource Groups*.
  - **Contact Service Queues** (`device/uccx/ContactServiceQueue`): see *Contact Service Queues*.
- Agent Device association with Unified CM Application users

  Administrators can specify the agent's controlled device via:
  - Quick Add Subscriber

  - Subscriber
  - Direct Agent management

  The device is associated with the list of Unified CM application users specified as part of the UCCX server configuration.

  Care is taken to keep this association in sync when Phones and Extension Mobility profiles are deleted or replaced.

- VOSS-4-UC also provides a number of interfaces to simplify Contact Center management:
  - **Agent Profiles**: see *Agent Profiles*.
  - **Re-skilling**: VOSS-4-UC provides functionality so that skills and their competency levels can easily be managed in bulk (add, remove) by means of a set of side-by-side transfer boxes that are available for:
    - Agents
    - Teams
    - Resource Groups

    See: *Re-skill Contact Center Agents*

Agents

Agents that have been synced in or added when adding subscribers at a specific customer or site hierarchy are listed here.

The detail view of an Agent opened from the list also shows the Agent's devices and tagged lines.

Synced agents from UCCX that have not been moved to a site may show the agent to be at the Customer hierarchy level.

It is possible to manage agents directly. An agent can also be added: choose **User ID** from the drop down.

The following agent properties can easily be managed from a single interface:

- **Alias**: agent alias on the device - note there are restrictions on allowable characters in the alias.
- **Type**: agent type: Agent or Supervisor
- **Team**: agents who are not assigned to a specific team, belong to the Default team.
- **Resource Group**: not mandatory; groups can be created
- **Automatically Available**: A check box enabled by default. If enabled, the agent is automatically in an available or ready state after finishing a call and disconnecting.
- **Skills**: not mandatory; skills can be defined.
- **Controlled Device**: select the agent's device type: either Extension Mobility or Phone. If Phone is selected, the phone needs to be selected from **Phone Name**.

Teams

Contact Center Agent Team names, their primary and secondary supervisors, team members and team availability to Contact Service Queues can be defined and managed by a a set of side-by-side transfer boxes on the user interface.

It is possible to manage Teams at a customer level. When creating a new team at the customer level, the user must select a Network Device List.

Resource Groups

A list of Resource Groups can be defined that will comprise of one or more Agent Profiles. When creating these directly in VOSS-4-UC, they should therefore be defined *before* Agent Profiles are created.

When the Agent Profiles are created or maintained, the Resource Groups are referenced.

Also, when a Contact Service Queue can be configured to use Resource Groups.

Skills

A list of skills can be defined and competency levels are assigned to a selected skill when it is applied to an Agent, Agent Profile or a Skill Group in a Contact Service Queue.

Contact Service Queues

Incoming contact center calls are placed in the queue and sent to a specific agent in accordance with the specific queue configuration.

The Contact Service Queues (CSQs) interface allows for the properties of the configuration to be defined, for example associating Resource Groups or Skills.

If a Chat or Email Contact Service Queues exist on UCCX, data from these are included when a Contact Center server is imported.

Agent Profiles

An Agent Profile comprises of a:

- Team
- Resource Group: profiles can be grouped together as Resource Groups.
- Skill

These should therefore be defined *before* creating an Agent Profile.

Note: Agent Profiles should be created *before* creating an Agent using Quick Add Subscriber.

Re-skill Contact Center Agents

As a part of Contact Center agent management, re-skill menu items are available with access to user interface controls such as side-by-side transfer boxes or drop down lists.

These controls provide functionality to easily re-skill a selected number of contact center agents:

- By Agent: for selected skills and their selected competency levels, these can be added or removed for one or more agents.
- By Team: for a selected team, skills and their selected competency levels can be added or removed - thereby updating the team skills. (not for Business Admin Portal)
- By Resource Group: for a selected resource group, skills and their selected competency levels can be added or removed - thereby updating the resource group. (not for Business Admin Portal)

Example Setup Journey

1. Configure Unified CM and UCCX server integration (this is done directly on the UC apps).
2. Create a new UCCX server at the relevant customer hierarchy level:
    a. Use UCCX admin user credentials
    b. Pick the list of Unified CM application users to be used for agent device association.
3. Update the Network Device List (NDL):
    a. The relevant Unified CM and UCCX servers must be referenced in the NDL.
    b. This NDL must be set for each site hierarchy where agents will be managed.
4. Sync the existing configuration from the UCCX server.

    This can be done either directly from the UCCX server page or via the **Data Sync** menu.
5. Create Agent Profiles under the **Contact Center** menu (usually under **Subscriber Management**).
6. Create a new Agent:
    a. Using Quick Add Subscriber
    b. Using Subscriber feature
    c. Directly using the Agent feature under the **Contact Center** menu (usually under **Subscriber Management**).

17 Self Service Administration

17.1. Self Service Administration: Overview

In addition to the administration and configuration of various components of the Self Service interface, an administrator also enables end user access to Self Service.

The items below provide an overview of this administration and configuration.

17.2. Self Service Feature Display Policy

The Self Service Feature Display Policy is used by an administrator to determine which features or services are available to the Self Service User on the Self Service Interface. These are typically available on both the Button Bar and Dashboard.

On the **Phones**, **Personal Phones** and **Voicemail** tabs, there are two similar check boxes (one associated with entitlement, the other not). For example, on the **Voicemail** tab, the first check box is labelled **User can enable Voicemail (Add a Voicemail Account)** and the second check box is labelled **User can enable Voicemail only if the user is entitled to Voicemail**.

If the Entitlement Feature is used, that is an Entitlement Profile is associated to the subscriber on the **Entitlement Profile** drop-down on the **Subscriber Management > Subscribers** screen, then select the second check box. If an Entitlement Profile is not associated to the subscriber, then select the first check box, as the second check box is no longer applicable.

In a similar way, select the appropriate check boxes on the the **Phones** and **Personal Phones** tabs.

Availability of features/services is configured using the following tabs on the **Self Service Feature Display Policy** screen:

- **Base**

  Shows/hides the **My Availability** and **Speed Dials**/**Busy Lamp Fields** areas and associated functionality. This controls the ability to add and manage speed dials and busy lamps.

  The **Enable (CFWD Only) Minimal Mode** check box controls the user self-service user interface. If enabled, the user is presented with a minimal interface suitable for mobile devices with *only* the functionality to set call forwarding. For details on the minimal interface, refer to the topic on Minimal Mode in the Self-service Guide.

- **Phones**

  Shows/hides the **Your Company Phones** area and associated functionality. This controls the ability to add smart devices, as well as to manage company phones and associated lines.

- **Personal Phones**

  Shows/hides the complete **Your Personal Phones** area and associated functionality, or hides selected functionality only, such as setting up ring schedules or advanced timer options. Also controls the ability to enable own personal phone management (add remote destination profile).

- **My Information**

  Shows/hides one or more of the **My Information**, **My Credentials**, and **Webex Self Service** areas and the associated functionality.

- **Voicemail**

  Shows/hides one or more of the **Voicemail Settings**, **Alternate Numbers and Notification Devices**, and **Caller Input** areas, as well as the associated functionality. Also controls the ability to add own Voicemail account if required.

- **Call Forward**

  Shows/hides the complete **Call Forwarding** area and associated functionality, or selected advanced call forwarding functionality only, such forward calls to settings.

See *Self Service Feature Display Policy Field Reference* for field descriptions.

See also topics under:

- “Entitlement Management” - for more details about the Entitlement feature.
- “General Subscriber Management Tasks” - for more details about associating an Entitlement Profile to a subscriber.

17.3. Self Service Feature Display Policy Field Reference

Title	Field Name	Description
Base	base	Configure Base features.
Name*	name	The name of the Feature Group.
My Availability	my_availability	Turn my availability on/off.
Automatically update Presence Status from calendar	update_presence_from _calendar	Allow users to manage the setting that automatically updates their presence status based on their calendar. The user must have ‘IM and Presence’ enabled, and Self Service ‘My Availability’ settings must be in ‘Show’ state.
Speed Dials	speed_dials	Turn speed dials on/off.
Enable (CFWD Only) Minimal Mode	enable_minimal_mode	Display Call Forward settings only minimal mode.

Title	Field Name	Description
Phones	phones	Configure Phone features.
User can add own smart devices	own_phone_add	User can add own smart devices. Default: false.
User can add own smart devices only if the user's Entitlement Profile includes 'Voice'	own_phone_add_if _entitled	Default : false.
Limit the user's total number of phones the number allowed by the user's Entitlement Profile	own_phone_add_limit _entitlement	Default : false.
Device Configuration Templates for User Phone Add	device_type_list.[n]	See below.
Phone Management	phone_management	Turn phone management on/off.
Phone Line Management	phone_line_management	Turn phone line management on/off.

Device Configuration Templates for User Phone Add	device_type_list.[n]	Smart Device configuration.
Device Name	devicetype	Choose from the drop-down list; either: iPhone, iPad, or Android Phone or Tablet.
Device Name Prefix	device_name_prefix	Automatically populated depending on the device name selected above; either TCT, TAB, or BOT.
Configuration Template	config_template	Select from the drop-down list. We recommend that you select the default configuration template for each device.

Title	Field Name	Description
Personal Phones	personal_phones	Configure Personal Phone features.
User can enable Personal Phone Management (add Remote Destination Profile)	user_add_rdp	Default: false
User can enable Personal Phone Management / SNR only if entitled to SNR	user_add_rdp_if_entitled	Default: false
Device Configuration Template for End User Remote Destination Profile Add	rdp_config_template	Choose from the drop-down list. Default = Default CUCM RDP Template.
Personal Phone Management	personal_phone_management	Turn personal phone management on/off.
Mobile Id Management	mobileid_management	Turn mobile id management on/off.
Ring Schedules	ring_schedules	Turn ring schedules on/off.
Advanced Timer Options	advanced_timer_options	Turn advanced timer options on/off.
Line Association	line_association	Turn line association on/off.

Title	Field Name	Description
My Information	my_information	Configure My Information features.
User Data	user_data	Turn user data on/off.
User Language	user_language	Turn user language on/off.
Password	password	Turn password on/off.
Pin	pin	Turn pin on/off.
Minimum Pin Length	pin_min_length	Minimum length of Pin (0 to 64 characters).
Link to Webex self service portal	webex_link	Toggle whether end user portal users can see a link to their Webex self service portal. The user must have an associated webex account in order to have the link.

Title	Field Name	Description
Voicemail	voicemail	Configure Voicemail features.
User can enable Voicemail (Add a Voicemail Account)	user_add_vm_account	Default: false
User can enable Voicemail only if the user is entitled to Voicemail	user_add_vm_account_if _entitled	Default: false
Device Configuration Template for End User Voicemail Account Add	voicemail_config_template	Choose from the drop-down list. Default = Default CUC User Template.
Voicemail Basic	voicemail_basic	Turn basic Voicemail on/off.
Voicemail Devices	voicemail_devices	Turn Voicemail devices on/off.
Phone Notification Device	phone_notification_device	Show/Hide Phone Notification Device management from end user.
SMS Notification Device	sms_notification_device	Show/Hide SMS Notification Device management from end user.
Voicemail Alternate Extensions	alternate_extensions	Show/Hide Voice Mail Alternate Extension management from end user.
Configuration Template for end user Alternate Extensions for Voicemail	cucaltext_config_template	Choose from the drop-down list. Default = cucalt-cft.
Configuration Template for end user add Phone Notification Devices	cucphonedevice_config_template	Choose from the drop-down list. Default = cucphone-cft.
Configuration Template for end user add SMS Notification Devices	cucsmsdevice_config_template	Choose from the drop-down list. Default = cucsms-cft.
Voicemail Caller Input	voicemail_callerinput	Turn Voicemail caller input on/off.

Title	Field Name	Description
Call Forward	call_forward	Configure Call Forward features.
Call Forward Basic	call_fwd_basic	Turn basic call forwarding on/off.
Advanced Call Forward	call_fwd_adv	Turn advanced call forwarding on/off.

17.4. End User Access and Authentication

A user can log into the Self-Service GUI if a System User entry exists for the user. A System User entry is created automatically when a user is added as a subscriber. Refer to the topics under “Subscriber Management”.

You can grant a user access to Self-Service by creating a user, with a **Self-Service** role, directly in the System user interface. Such a user is not able to view devices or any services associated with the devices, nor can a manually added user view personal information such as first name, last name, address, department, and so on. Refer to *Create and Update a User*.

Self-Service authentication is controlled by the administration interface using the same three authentication methods: Standard, LDAP, and SSO.

Consolidated password and PIN management for end users is available as follows, based on the self-service authentication method configured for the end user:

- Standard VOSS-4-UC authentication: end users can change their password and PIN from the Self Service interface.
- LDAP and SSO authentication: end users cannot change their password and PIN from the Self Service interface.

To ensure the best user experience, it is recommended that all applications (Self-Service and the Unified Communications applications) use the same authentication method.

17.5. GUI Themes and Branding

The Self Service GUI interface can be branded by configuring Cascading Style Sheets, images and logos. The same theme upload and download interface used for the Admin GUI is used.

The theme itself differs between the Admin and Self Service interface (based on the user role).

The login page theme is also loaded from the URL:

```
https://<host>/selfservice/#/login?theme=<mytheme>
```

Refer to the topic “Download and Update a Theme”.

17.6. Self-Service Login Banner

The Self-Service login banner corresponds with the administrator interface banner.

For details on banner configuration and specifications, refer to the topic on “Login Banner” in the “Advanced Configuration Guide”.

17.7. Personal Phones (Remote Destinations)

You must allocate a remote destination profile (RDP) to end users for them to manage their own personal phones and simultaneous ring settings.

If no RDP is associated to the end user, the Personal Phones management interface in the Self Service application is hidden.

Multiple RDP’s per end user is not supported. The Personal Phones management interface in Self Service is also hidden if an end user has more than one RDP associated. Refer to the topics under “Subscriber Workflows”.

17.8. Dual Mode Phones - Mobile ID

If users have a dual mode device associated, they can manage the phone number and simultaneous ring settings for the device.

If no dual mode device is associated, the relevant settings are hidden in the Self Service interface. Refer to the “Subscriber Workflows” topic.

17.9. Voicemail for Self-Service

Voicemail settings are only visible in the Self Service interface if the user has a Voicemail box. Refer to the “Subscriber Workflows” topic.

17.10. Links Page

The contents of a user’s Links page in the Self Service interface can be managed.

You can create one or more links to for example, Voicemail, WebEx, or downloadable content such as a User Guide.

Links on the page are associated to a user role and are managed using the Administration GUI Self Service Links interface.

Refer to “Create a Self Service Link”.

18 Services

18.1. Voice Mail

18.1.1. 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.

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.
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.

18.1.2. 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

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**.

18.1.3. 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.

18.1.4. Delete Voice Mail Service

Procedure

1. Log in as the Provider Administrator.

2. Choose **Services > Voice Mail > Voice Mail Service**.
3. From the list of Voice Mail Services, choose the service to be deleted by selecting the check box in the leftmost column.
4. Click **Delete** to delete the Voice Mail Service.
5. From the popup window, click **Yes** to confirm the deletion.

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

18.1.5. 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.
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

18.1.6. 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.

18.1.7. 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.

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.

18.1.8. Delete a Voice Mail Pilot Number

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 > Pilot Numbers**.
3. From the list of Pilot Numbers, choose the number to be deleted, by selecting the check box in the leftmost column.
4. Click **Delete** to delete the Voice Mail Pilot Number.
5. From the popup window, click **Yes** to confirm the deletion.

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

18.2. Contact Center Service

18.2.1. Set Up Contact Center Using Cisco Unified Communications Manager

Contact Center provisioning configures Cisco Unified Communications Manager to communicate with Contact Center.

Configure Services > Contact Center > Servers to enable Cisco Unified Communications Manager to communicate with Contact Center when transferring a call from agent to agent and routing a call back to the Customer Voice Portal (CVP).

Configure Services > Contact Center > Service to allow internal service calls to be routed to the CUBE (ENT) for Contact Center to process.

18.2.2. Prerequisites: Overview

1. Once you have VOSS-4-UC configured and have added a Provider, add a Customer (under Provider or Reseller). Log in as a Provider Admin.
2. Contact Center configuration is only supported for dedicated Unified Communications Applications for a Customer. When adding a Provider, clear Shared UC Apps.

3. After successfully adding a Customer, choose the Customer hierarchy at the above context level and then add the Cisco Unified Communications Manager(s) to that customer from **Device Management > Cisco Unified Communications Manager > Servers**.
4. Complete a Cisco Unified Communications Manager import before proceeding further.
5. VOSS-4-UC supports multiple Cisco Unified Communications Manager clusters at a Customer hierarchy. You can decide which cluster to use for Contact Center and IP telephony.
6. SIP Trunk Security Profiles must be created manually in each Cisco Unified Communications Manager and synced to VOSS-4-UC.
7. For the Contact Center customers, Built-in-Bridge must be enabled for the phones. By default, it is disabled at system level.
8. SIP Trunk Profiles must be created manually in each Cisco Unified Communications Manager and synced to VOSS-4-UC.

18.2.3. Built-in-Bridge

Built-in-Bridge (BIB) is not enabled by default for the phones. It is disabled at the system level as it is not used by all the customer by default. It is used only by the customers having Contact Center.

The provider has to perform the following procedures to enable BIB for the customers having contact center.

Note: Create a new Field Display Policies at the customer level and add Built-in Bridge to the list.

- *Configure the Built-in-Bridge*
- *Enable or Disable the Built-in-Bridge*

18.2.4. Configure the Built-in-Bridge

Procedure

1. Log in to VOSS-4-UC as provider administrator.
2. Choose **Customizations > Field Display Policies**.
3. Make sure that hierarchy is set to the appropriate Customer.
4. Click **SubscriberPhoneMenuItemProvider**.
5. Choose **Action > Clone**.
6. In the **Name** field, enter **SubscriberPhoneMenuItemProvider**.
7. From the **Target Model Type** drop-down, choose **relation/SubscriberPhone**.
8. Click '+' next to **Groups** to expand the Groups section, and in the **Title** field enter **Phone**.
9. From the **Available** list, choose **builtInBridgeStatus** and click **Select**.
10. Click **Save**.

18.2.5. Enable or Disable the Built-in-Bridge

Before You Begin

Ensure that you configure Built-in-Bridge. See, Configure the Built-in-Bridge.

Procedure

1. Log in to VOSS-4-UC as provider administrator.
2. Make sure that hierarchy is set to the appropriate Customer.
3. Choose **Subscriber Management > Phones** and select the appropriate phone.
4. On the **Phone** tab:
   - From the **Built in Bridge** drop-down in the **Vendor Config** section, choose **On** to enable BIB.
   - From the **Built in Bridge** drop-down in the **Vendor Config** section, choose **Off** to disable BIB.
5. Click **Save**.

18.2.6. How to Set Up a Contact Center Server

Procedure

1. Log in as provider administrator at the customer hierarchy.
2. Choose **Services > Contact Center > Servers** menu to add a Contact Center server.
3. Click on **Add** button to add a new Contact Center server, complete the fields, and click **Save** to save the Contact Center server.

Field	Description
Contact Center Server Name	Unique server name. This field is mandatory.
Description	Server description.
Cisco Unified Communications Manager	The Cluster you want to use for Contact Center Server. This field is mandatory.
Transfer Conference Pattern	Transfer conference pattern used when transferring calls between agents. This field is mandatory.
Network VRU	Pattern used to route calls to a CVP. This field is mandatory.
SIP Trunks	This field is mandatory. See fields below:
Trunk Destination Type	CVP or CUBE (ENT) or CUSP SIP Trunk. This field is mandatory. Note: Both CVP and CUBE (ENT) trunks must be added for this Contact Center Server to be added successfully.
Trunk Destination Address	The destination address of the CVP or CUBE (ENT) or CUSP SIP Trunk. This field is mandatory. Multiple destination addresses & ports can be added for each trunk type.
Trunk Destination Port	The destination port of the CVP or CUBE (ENT) or CUSP SIP Trunk, if no value provided system takes 5060 as default.
Trunk Security Profile	The SIP trunk Security Profile that needs to be used by each trunk. This field is mandatory.
SIP Profile	The SIP trunk profile that needs to be used by each trunk. This field is mandatory.

For 500/1000/4000/12K/SCC - You must provide information for a CVP and a CUBE (ENT) SIP Trunk. For Small Contact Center, both the CVP and CUBE (ENT) trunks should have the same IP address with a different Trunk Security Profile selected in the **Trunk Security Profile** drop-down for each trunk.

For CUSP - You must provide information for a CUSP SIP Trunk. Only one trunk type can be added.

Note: For CUSP, use only one SIP trunk. For CVP or CUBE (ENT), use two SIP trunks.

1. Device Pool will create automatically as a part of Contact Center server with the name “Cu<CUSTOMER_ID>-CC<CC_SERVER_ID>-DP” with the default Call Manager Group & Region.
2. Call Manager Group & Region can be changed in the Cisco Unified Communications Manager as desired.
3. Two application users creates with names pguser & pguser2 - both are created with default password “cisco”.

Note:

- Planning to change the pguser & pguser2 names to tie with the Customer ID in future releases.
- For all the phone line CSS of a site, add Cu<CUSTOMER_ID>-CC<CC_SERVER_ID>-Xfer4CCServer-PT to the Class of Service member list as a partition with the next available index.
- The admin needs to add Default Region as related regions for each site region created for a site.
- Reset the trunk by clicking the **Reset** button in the Trunk page after updating the SIP profile.

18.2.7. Edit Contact Center Servers

Procedure

1. Log in to VOSS-4-UC as provider or reseller Administrator.
2. Choose the Customer hierarchy level.
3. Choose **Services > Contact Center > Servers**.
4. Click the Contact Center server that you want to edit and modify the required fields.

   Note:

   You cannot change the Contact Center server name.
5. Click **Save**.

18.2.8. Delete Contact Center Servers

Before You Begin

Delete the Contact Center service and parameters associated with Contact Center server.

Procedure

1. Log in to VOSS-4-UC as provider or reseller administrator.
2. Choose the Customer hierarchy level.
3. Choose **Services > Contact Center > Servers**.
4. Select the check box in the leftmost column next to the Contact Center server that you want delete.
5. Click **Delete**.
6. From the popup window, click **Yes** to confirm the deletion.

18.2.9. How to Set Up a Contact Center Service

Procedure

1. Log in as provider administrator at the customer hierarchy.
2. Choose **Services > Contact Center > Services** menu to add a Contact Center Service.
3. Click **Add** to add a new Contact Center Service, complete the fields, and then click **Save**.

Note:

- Customer & Site Dial Plan is required to add a Contact Center Service.
- Only ONE instance of Contact Center Server can be created for a Cisco Unified Communications Manager cluster.

- Only ONE instance of Contact Center Service can be created for a Contact Center Server.
- For CUSP only ONE trunk of type CUSP needs to be added.
- For deleting a server, ensure the service is deleted first.

18.2.10. Edit Contact Center Services

Procedure

1. Log in to VOSS-4-UC as provider or reseller administrator.
2. Choose the customer hierarchy level.
3. Choose **Services > Contact Center > Services**.
4. Click the Contact Center service that you want to edit, and modify the required fields.

   Note:

   You cannot change Contact Center Service Name.
5. Click **Save**.

18.2.11. Delete Contact Center Services

Procedure

1. Log in to the VOSS-4-UC as provider or reseller administrator.
2. Choose the customer hierarchy level.
3. Choose **Services > Contact Center > Services**.
4. Select the check box in the leftmost column next to the contact center service that you want to delete.
5. Click **Delete**.
6. From the popup window, click **Yes** to confirm the deletion.

18.2.12. Conditions / Restrictions: Overview

- Only one instance of Contact Center Server can be created for a Cisco Unified Communications Manager cluster.
- Only one instance of Contact Center Service can be created for Contact Center Server.
- For CUSP, only one trunk of type CUSP needs to be added in **Services > Contact Center > Servers**.
- For deleting a server, please make sure the service is deleted first.

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

Ensure that before you begin deleting Contact Center Server you have deleted all the agent lines for that Contact Center Server.

- The monitoring application PCA is added through HCM-F only for monitoring the Contact Center components. But, for other components such as CUCM, IM and Presence, and Unity Connection, PCA is added (selected) through VOSS-4-UC.

18.2.13. Configure CTI Port

Procedure

1. Choose **Subscriber Management > Phones**.
2. Click **Add** to create a new CTI port.
3. Choose the **Hierarchy Provider > Reseller > Customer > Site**.
4. Click the **Phone** tab, and from the **Product** drop-down choose **CTI Port**.
5. In the **Device Name** field, enter a unique name for the Local CTI Port pool name. For example, use the following format for the device name (LCPxxxxFyyyy):
   - LCP identifies the CTI Port as a local device.
   - xxxx is the peripheral ID for the Unified Communications Manager PIM.
   - yyyy is the local CTI Port.
6. In the **Description** field, enter a description for the Local CTI Port.
7. From the **Device Pool Name** drop-down, choose the appropriate device pool.
8. On the **Lines** tab.
9. Click '+' next to **Line** to add a new line.
10. From the **Pattern** drop-down, choose a unique directory number for the CTI port.
11. Click **Save**.

    Make sure that you leave all the fields with default values in this page.
12. Choose **Subscriber Management > Phones**.
13. Click **Add** to create a new CTI port.
14. Choose the **Hierarchy Provider > Reseller > Customer > Site**.
15. Click the **Phone** tab, and from the **Product** drop-down, choose **CTI Port**.
16. In the **Device Name** field, enter a unique name for the Local CTI Port pool name. For example, use the following format for the device name (RCPxxxxFyyyy):
    - RCP identifies the CTI Port as a Network device.
    - xxxx is the peripheral ID for the Unified Communications Manager PIM.
    - yyyy is the Network CTI Port.
18. In the **Description** field, enter a description for the Local CTI Port.
19. From the **Device Pool Name** drop-down, choose the appropriate device pool.
20. On the **Lines** tab.
21. Click '+' next to **Line** to add a new line.
22. From the **Pattern** drop-down, choose a unique directory number for the CTI port.

23. Click **Save**.

    Make sure that you leave all the fields with default values in this page.

18.2.14. Tag CTI Port as Contact Center Agent Line

Procedure

1. Choose **Subscriber Management > Agent Lines**.
2. Choose **Hierarchy Provider > Reseller > Customer > Site**.
3. Click **Add** to create a new CTI port.
4. From the **Device Type** drop-down, choose **Phone**.
5. From the **Device Name** drop-down, choose a port from the list of device names.
6. From the **Line** drop-down, choose the Line.
7. From the **Application User** drop-down, choose **pguser**.
8. Click **Save**.
9. Repeat the steps for both LCP and RCP ports.

18.3. Configure Cisco Media Sense

18.3.1. Set Up Trunk

Procedure

1. In VOSS-4-UC, choose **Device Management > CUCM > SIP Trunks**.
2. Click **Add**.
3. In the **Device Information** tab, from the **CUCM** drop-down, choose a CUCM.
4. In the **Device Name** field, enter the device name.

   This is a mandatory field when you add a trunk, but a read-only field when you modify a trunk.
5. In the **Description** field, enter a description.
6. In the **SIP Info** tab, click '+' next to **Destination** to add the trunk destination.
7. Enter the Ipv4 Address of Media Sense Server, Port, and Sort Order.
8. Click **Save**.

18.3.2. Set Up Route Group

Procedure

1. In VOSS-4-UC, choose **Device Management > CUCM > Route Groups**.

2. Click **Add**.
3. From the **CUCM** drop-down, choose a CUCM.
4. In the **Route Group Name** field, enter the route group name.
5. From the **Distribution Algorithm** drop-down, choose **Circular** or **Top Down**.
6. Click '+' next to **Members** to add Trunk details.
7. From the **Device Name** drop-down, choose the Trunk and enter the selection order.
8. Click **Save**.

18.3.3. Set Up Route List

Procedure

1. In VOSS-4-UC, choose **Device Management > CUCM > Route Lists**.
2. Click **Add**.
3. From the **CUCM** drop-down, choose the required CUCM.
4. Enter the Route List Name, Description, and Call Manager Group Name.
5. Select (default option) or clear the **Route List Enabled** check box to enable or disable the route list. If disabled, the route list, calls in progress do not get affected, but the route list does not accept additional calls.
6. Select the **Run on Every Node** check box if you want the route list to be active on every node.
7. Click '+' next to **Route Group Items** to add a route group.
8. From the **Route Group** drop-down, choose the route group.
9. Click **Save**.

18.3.4. Set Up Route Patterns

Procedure

1. In VOSS-4-UC, select **Device Management > CUCM > Route Patterns**.
2. Click **Add**.
3. On the **Pattern Definition** tab, from the **CUCM** drop-down, choose the CUCM and then enter the **Route Pattern** name and description.
4. From the **Route Partition** drop-down, choose the required route partition.
5. In the **Destination (Only Choose Route List or Gateway)** section of the page, choose either a **Route List** or **Gateway/Trunk** from the respective drop-down.
6. Click **Save**.

18.3.5. Configure Device

Procedure

1. In VOSS-4-UC, choose **Subscriber Management > Phones**.
2. Choose audio forking phone configured.
3. On the **Phone** tab, in the **Vendor Config** section of the screen, from the **Built In Bridge** drop-down, change the setting to **On**.
4. On the **Lines** tab, click '+' next to **Line** and click the required line to access the line details.
5. From the **Recording Profile Name** drop-down, choose the recording profile created using CUCM.

   If using a recording service provider, choose **Automatic Call Recording Enabled** from the **Recording Flag** drop-down, as per the recording service provider recommendations. If not using a recording service provider, choose **Call Recording Disabled**.
6. Click **Save**.

18.4. Set up Cisco Remote Silent Monitoring

18.4.1. Create Unified CM Group

Procedure

1. Choose the Customer in the hierarchy.
2. Choose **Device Management > CUCM > Unified CM Groups** and click **Add**.
3. From the **Network Device List** drop-down, choose the appropriate NDL to add a new Region, and then click **OK**.
4. In the **Name** field, enter **RSMSimPhone** for the Unified CM group name.
5. Select the **Auto-registration Cisco Unified Communications Manager Group** check box if required. Only use this when setting **TFTP Default** to true, which will result in setting all other Unified CM groups to false.
6. Click '+' next to **Unified CM Group Items** to add Unified CM Group Items.
7. From the **Call Manager Name** drop-down, choose the required CUCM and then enter the priority.
8. Click **Save**.

18.4.2. Create Region

Procedure

1. Choose the Customer in the hierarchy.
2. Choose **Device Management > CUCM > Regions**.
3. Choose the appropriate NDL from the drop-down list to add a new Region, and then click **OK**.

4. From the **CUCM** drop-down, choose the CUCM.
5. In the **Name** field, enter **AR_ RSMSimPhone** as the region name.
6. Click '+' next to **Related Regions**, to add a related region, and then complete the following fields:
   - Choose the appropriate **Region Name** from the drop-down.
   - Choose the **Audio Bandwidth** value as **64 kbps (G.711)** from the drop-down.
   - Choose the appropriate **Video Bandwidth** from the drop-down.
   - Choose the appropriate **Immersive Video Bandwidth** from the drop-down.
7. Click **Save**.

18.4.3. Create Device Pool

Procedure

1. Choose the customer in the hierarchy.
2. Choose **Device Management > CUCM > Device Pools**.
3. Choose the appropriate NDL from the drop-down list to create a new device pool, and then click **OK**.
4. On the **Device Pool Settings** tab, in the **Device Pool Name** field, enter the device pool name as **RSMSimPhone_DP**.
5. From the **Cisco Unified CM Group** drop-down, choose **RSMSimPhone**.
6. On the **Roaming Sensitive Settings** tab, from the **Date/Time Group** drop-down, choose the appropriate date/time group.
7. From the **Region** drop-down, choose **AR_ RSMSimPhone**.
8. From the **SRST Reference** drop-down, choose **Disable**.

18.4.4. Create Phones

Procedure

1. Choose **Subscriber Management > Phones**, and then click **Add**.
2. From the **Hierarchy** drop-dow, choose the site and click **OK**.
3. On the **Phone** tab in the **Device Name** field, enter the device name and add SEP before the mac address. For example, if the mac address is 000000000AB1 the device name must be SEP000000000AB1.
4. From the **Product** drop-down, choose the product type as **Cisco 7941**.
5. (Optional) In the **Description** field, enter the phone description.
6. From the **Device Protocol** drop-down, choose **SIP**.
7. From the **Device Pool Name** drop-down, choose **RSMSimPhone_DP**.
8. From the **Lines** tab, click '+' next to **Line** and from the **Pattern** drop-down, choose the directory number.
9. From the **Monitoring CSS Name** drop-down, set the Monitoring Calling Search Space as the CSS that is configured in the Calling Search Space field in the **Lines** page.

10. In the **Busy Trigger** field, enter a busy trigger value as **1**, and in the **Max Num Calls** field, enter the maximum number of calls value as **2**.

18.5. Configure Intelligent Proximity for Mobile Voice

18.5.1. Configure Intelligent Proximity for Mobile Voice in VOSS-4-UC

Before You Begin

Ensure that you have the latest COP files for your Cisco IP phone, or device package downloaded and installed in Cisco Unified Communications Manager (Unified CM):

- In your browser, open https://software.cisco.com/download/navigator.html?mdfid.
- In the Product Search window, enter Unified Communications Manager Version 10.5.
- Choose Software Type Unified Communications Manager/CallManager Device Packages.
- Download and install the file cmterm-devicepack 10.5.2 12020-1cop.sgn in Unified CM.

Each phone that you register to Unified CM contains phone-specific settings. These settings appear in Unified CM at the bottom of the Phone Configuration window under the Product Specific Configuration Layout heading. The settings vary by phone model, and are tailored to each phone model. The phone has default settings, but in the Unified CM Phone Configuration window, you can override the settings and configure new values.

Use this high-level procedure to perform these tasks:

- Ensure that all the required settings are enabled on Cisco Unified CM.
- Import the settings into VOSS-4-UC so they appear on the Phone Management page for each registered phone.
- Ensure that the settings are correct in VOSS-4-UC.
- Pair the mobile phone or tablet with the Cisco IP endpoint.

Procedure

1. In Cisco Unified CM, choose these settings on the **Device** page:
   - Proximity Mode - Choose ‘On’
   - Call Control - Choose ‘Enabled’
   - Proximity Content Share From Clients - Choose ‘Enabled’
   - Proximity Content Share To Clients - Choose ‘Enabled’
2. Import phone features (or refresh existing phone features) using the Import/Refresh feature in VOSS-4-UC. This step imports each phone type’s features as listed on the Product Specific Configuration Layout page in **Devices > Phones** in Unified CM into VOSS-4-UC. VOSS-4-UC imports the settings and only shows settings that were available and imported the last time the command was run. Perform this step any time there is a change on the Unified CM, such as adding new phone types or templates. However, we recommend that you perform this step every time. To import or refresh phone features, perform these steps:
   a. Log in to VOSS-4-UC as provider or reseller administrator.

b. Choose **Device Management > Advanced > Perform Publisher Actions**.

c. From the **Action** drop-down, choose **Import**.

d. From the **App Type** drop-down, choose **CUCM Device**.

e. In the Clusters box, click the cluster to be configured for the Intelligent Proximity feature in the **Available** window. Click Select to move the cluster to the **Selected** window.

f. Click **Save**.

3. Verify that the Bluetooth settings are enabled.

a. Log in to VOSS-4-UC as customer administrator and choose a valid site from the hierarchy node.

b. Choose **Subscriber Management > Phones**.

c. Choose the endpoint to pair with the mobile phone or tablet.

d. On the **Advanced Information** tab, make sure that these fields are set correctly if they appear for the selected endpoint type:

- **Bluetooth** drop-down - **Enabled**.
- **Allow Bluetooth Contacts Import** drop-down - **Enabled**.
- **Allow Bluetooth Mobile Handsfree Mode** drop-down - **Enabled**.

4. Pair the mobile phone or tablet with the Cisco endpoint (device such as a desk phone). For more information, see 'Intelligent Proximity for Mobile Devices' in http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/8811_8841_8851_8861/10_5/ english/userguide/P881_BK_C9A41445_00_cisco-ip-phone-8811-8841.pdf.

a. At the Cisco IP endpoint, make sure that Bluetooth and Handsfree 2-way audio are enabled.

b. Add the mobile device. Once the mobile device is discovered, you can pair the two and also store mobile contacts on the Cisco IP endpoint.

c. A security code may appear on both the endpoint and mobile device. Accept the security code on both the Cisco IP endpoint and mobile device before the pairing can be completed.

18.6. Webex Teams

18.6.1. Webex Teams Feature Workflow

Webex Teams Feature Reference

Note: Only steps 1 and 2 below are mandatory for Webex Teams to function in VOSS-4-UC. The other steps are dependent on your particular requirements.

A typical Webex Teams workflow is:

1. Create Webex Teams Service (see *Create Webex Teams Service*).
2. Make sure that the **Webex Teams** check box is selected at the required hierarchy level under both **Entitlement > Catalogs** (see *Create an Entitlement Catalog*) and **Entitlement > Profiles** (see *Create an Entitlement Profile*).

3. Sync existing Webex Teams users for the customer by clicking **Action > Sync Webex Teams Users** on the **Customer Access** form. A sync can also be run by executing **SyncSpark[Customer]** from **Administration Tools > Data Sync**.
4. Add a Webex Teams user in VOSS-4-UC (see *Add Webex Teams User*).
5. Add Webex Teams users using **Subscriber Management > Subscribers**.
6. If you want to add a Webex Teams user using Quick Add Subscriber (QAS), choose the **Webex Teams User Template** to use for the user. This selection overrides the default user template referenced in the **Quick Add Subscriber Groups** associated to the user. If a **Webex Teams User Template** is not selected from the drop-down, selection falls back to the **Webex Teams User Template** referenced in the associated **Quick Add Subscriber Groups**. If you want customized values, clone the **Webex Teams User Template** (**Customizations > Configuration Templates**), and edit as required.
7. Add Webex Teams users using **Subscriber Management > Quick Add Subscriber** (see *Webex Teams Quick Add*)
8. Provision Webex Teams for an existing user (see *Provision the Webex Teams Service*).

18.6.2. Create Webex Teams Service

Webex Teams Feature Reference

Before You Begin

For VOSS-4-UC to connect to the Webex Teams Cloud API you need:

- a Webex Teams Organization Account Number
- an Access and Refresh token

Both are obtained from the Cisco Webex page.

Procedure

See procedure below for clarity if required:

1. Log in as provider or reseller administrator.
2. Make sure that the hierarchy path is set to the correct customer node.
3. Choose **Services > Webex Teams > Access Token** to open the **Webex Teams Account** form on a separate tab, i.e it opens the following URL:

   ```
   https://us-central1-webex-teams-auth-token.cloudfunctions.net/
   webex_teams_oauth
   ```

4. Click the **GET TOKENS** link.
5. Enter a valid Email address in the **Email address** field on the **Cisco Webex** page and click **Next**. An Email address and password are only required the first time you login to the Cisco Webex site.
6. Enter a valid password in the **Password** field on the **Cisco Webex** page, and click **Sign In**. The following codes/tokens are generated and displayed on the form:
   - **Organization ID**
   - **Access Token** (14 days)

- **Refresh Access Token** (90 days)

Note:

- VOSS-4-UC automatically refreshes the access tokens every 7 days. To manually refresh the access tokens, click **GET TOKENS** on the **Webex Teams Account** form or **Action > Refresh Access Token** on the **Customer Access** form.
- The Refresh Token is valid for 90 days. The number of valid days remaining for the access token is displayed in the **Refresh Token Expires in** counter on the **Webex Teams Access Token Management for VOSS4UC** page.
- Refer to https://developer.webex.com/docs/integrations for more details on access token management.

7. Click on each **Copy** button in turn to copy the item, return to the VOSS-4-UC tab, and paste in the appropriate field on the **Customer Access** form. Note that the access tokens must also be pasted into the 'Repeat' fields.
8. Complete at minimum the other mandatory fields on the **Customer Access** form:
   - The **Webex Teams Customer Name** field is populated automatically using the Customer Name.
   - Enter the **HTTP Proxy String**. Only if a proxy server is required to connect to the Webex Teams cloud, e.g. `http://[ip address]:port`.
   - Enter the **HTTPS Proxy String**. Only if a proxy server is required to connect to the Webex Teams cloud, e.g. `https://[ip address]:port`.
9. Click **Save** to add the Webex Teams Service.

What to Do Next

Sync the Webex Teams Users for the customer by clicking **Action > Sync Webex Teams Users** on the **Customer Access** form.

Webex Teams Users can also be synced from **Administration Tools > Data Sync**, and then running the SyncSpark[Customer] data.

18.7. Call Handler (Auto Attendant)

18.7.1. Call Handler (Auto Attendant)

Auto Attendant is an overarching service that caters for the provisioning, configuration and management of Call Handlers, Greetings, Schedules and related dialplan components in Cisco Unity Connection and Cisco Unified Communications Manager.

A Call Handler transfers telephone calls to the extension of a user or department without the intervention of a receptionist or operator. This is achieved via a system of voice menus that the person initiating the call interacts with via their telephone keypad or via voice commands.

In some Call Handler systems, there are message-only information menus and voice menus that are used so that an organization can provide business information such as hours, directions to their premises, information

about job opportunities, and answer other frequently-asked questions. After the message has played, the caller can be forwarded to the receptionist or they can return to the main menu.

Call Handlers can be created at either Customer or Site Level. If created at Customer level, a Network Device List (NDL) must be selected to instruct the workflow which UC Application Servers to provision. If created at Site level, the NDL associated to the site is chosen automatically.

Call Handler (Auto Attendant) Feature Reference

- *Add Call Handler (Auto Attendant)*
- *Modify a Call Handler (Auto Attendant)*
- *Call Handler Field Descriptions*
- *Manage Greeting Files*
- *Call Handler (Auto Attendant) Schedule*
- *Create a Call Handler (Auto Attendant) Schedule*
- *Modify a Call Handler (Auto Attendant) Schedule*

See also:

- *Add a Language Filter*
- *Add a TimeZone Filter*

18.7.2. Add Call Handler (Auto Attendant)

Before You Begin

Make sure that the relevant Cisco Unity Connection Call Handler template has been synced from Cisco Unity Connection.

Note: Not all the configuration parameters needed to provision the Call Handler are exposed in the user interface. Many settings and values are derived from Configuration Templates, i.e. **Provide Outside Dial Tone = False**, and **Call Classification = OnNet** are hard coded in the **AddCucmRoutePatternForCallhandlerCFT** configuration template. If you want to change these, or other values, clone the configuration template from **Customizations > Configuration Templates** to the desired hierarchy level, and edit the fields as required.

Procedure

1. Log in as provider, reseller or customer administrator.
2. Make sure that the hierarchy path is set to the required Customer or Site node.
3. Choose **Services > Auto Attendant > Call Handler**.
4. Click **Add** to add a Call Handler.
5. From the **Hierarchy** drop-down, choose the Site to which you want to add the Call Handler (if not already done).

6. From the **Network Device List** drop-down, choose the required network device list (NDL). This is a mandatory field. This field is only applicable at the customer node, and the value is derived automatically at the site node.
7. Enter a **Name** for the Call Handler. This is a mandatory field.
8. Optionally enter a number from the **Pilot** drop-down that you want to associate the Call Handler. The drop-down list displays a list of directory numbers that are available at the selected hierarchy level.
9. If a **Pilot** number is added, the **Route List** input field is shown to choose the Cisco Unified CM route list to apply to the Call Handler.

   The route lists available in the drop-down are determined by the NDL. If the NDL changes, the drop-down list auto updates to display new route lists based on the updated NDL.
10. From the **Call Handler Template** drop-down, choose the Cisco Unity Connection Call Handler Template to apply to the Call Handler.

    For detailed information about the call handler template, see the “Call Handler Templates” section of the “Call Management” chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x.
11. Click **Save** to add the Call Handler to VOSS-4-UC and Cisco Unity Connection.
12. Optionally, edit the Call Handler settings, see *Modify a Call Handler (Auto Attendant)*.

Adding a Call Handler through VOSS-4-UC, also adds a Route Pattern on the Cisco Unified CM designated in the NDL. The pattern is the value of the pilot selected. The rest of the pilot configuration (including partition), is driven through a configuration template that can be cloned and modified. A Direct Routing Rule is also created on the Cisco Unity Connection designated in the NDL, during this step. This rule will accept inbound calls into Cisco Unity Connection, and route them to the relevant Call Handler.

18.7.3. Modify a Call Handler (Auto Attendant)

1. Log in as provider, reseller or customer administrator.
2. Make sure that the hierarchy path is set to the correct hierarch level.
3. Choose **Services > Auto Attendant > Call Handler**.
4. Click the Call Handler that you want to modify.
5. From the **Call Handler Basics** tab, edit the settings from the following drop-downs if required: **Pilot**, **Time Zone**, **Schedule**, **Phone System**, **Language**, **Partition Name** and **Call Handler Owner**.
   - If the **Pilot** is updated, the **Route List** input field needs to be completed.
   - Choosing an ‘owner’ from the **Owner** drop-down list in the **Call Handler Owner** section of the screen, associates a Unity Connection user to the owner of this call handler.
6. From the **Transfer Rules** tab, enable or disable the required transfer rules. Note that the **Standard** transfer rule can not be disabled.

   By default the **Transfer Call To** action is set to **Greeting**. If the action is changed to **Extension or URI**, additional controls are exposed that allow you to enter an extension number or URI as well as the transfer type (Release to Switch or Supervise Transfer).
7. From the **Caller Input** and **Greetings** tabs respectively, edit the default caller input and greeting settings.

Additional fields are exposed when choosing certain options. For example, when you choose the **User with Mailbox** call action on the **Caller Input** tab, the **User with Mailbox** and **Transfer** / **Greeting** fields are exposed.

Refer to "System Call Handlers" in the "Cisco Unity Connection System Administration Guide" for more information about the Call Handler feature.

8. From the **Record**/**Playback** tab, configure the greeting that you want to record and playback on the chosen extension. This interface allows administrators to trigger a call to a physical device, which allows for recording or playback of a greeting. The extension to dial must be an accessible extension for the administrator (or user) to answer and record or listen to greetings.
   a. Select an extension from the drop-down, or manually type in the number of the device you want to call to record or listen to a greeting.
   b. Select the **Specific Greeting** check box if you want to record or playback a greeting for Standard, or Busy, etc. Otherwise the action will apply to the main Call Handler.
   c. The duration is the time (in seconds), that the system will allow to record a greeting, and does not apply when playing back a recording. **This is an important timer, as setting this too low, might result in incorrect configuration**.

Important: **Do not** click **Save** on this form, go to **Action > Record Greeting** or **Action > Playback Greeting** to save these settings.

---

9. On the **Upload Greeting** tab, from the **Greeting File** drop-down, choose the greeting file (.wav) to upload to the call handler, and then configure the specific greeting (if required), see *Manage Greeting Files*.

   See also: *Call Handler Field Descriptions*.

10. Click **Save** when complete to save the changes to the Call Handler in VOSS-4-UC and Cisco Unity Connection.

Note: To delete a Call Handler, click on the Call Handler you want to delete and then click **Delete** on the button bar. From the popup window, click **Yes** to confirm the deletion.

18.7.4. Call Handler Field Descriptions

Call Handler Basics (Auto Attendant only)

Title	Field Name	Description
Network Device List *	HF.target_ndl	Mandatory input-field for the **option** (if hierarchy is at Site-node, however, this value is derived automatically). The workflow (and GUIRules) will target the UC devices that is linked to this Network Device List (NDL). In the Mod use-case, this should also be derived automatically and can thus be omitted from Updates.
Cisco Unity Connection	HF.cuc_info	Informative (non-input) field. Indicates the target CUCx host/IP, which is automatically derived from the input NDL.
Cisco Unified CM	HF.cucm_info	Informative (non-input) field. Indicates the target CUCM host/IP, which is automatically derived from the input NDL.
Name *	DisplayName	The text name of the handler to be used when displaying entries in the administrative console, e.g. Cisco Unity Connection Administration. For example, the display name for the default opening greeting call handler is “Opening Greeting.”
Route List	route_list	The CUCM Route List to use. The valid options are dependent on the selected NDL/CUCM. console, e.g. Cisco Unity Connection Administration. For example, the display name for the default opening greeting call handler is “Opening Greeting.”
Pilot	DtmfAccessId	The DTMF access id (i.e., extension) for the call handler. The dialable number.
Call Handler Template	cuc_template	Select the Unity Template for Call Handler.

Transfer Rules (Auto Attendant only)

Title	Field Name	Description
Message	callerInput_tab_message	Caller Input
Callhandler Menu Entry	CallhandlerMenuEntry.[n]	
Object Id	ObjectId	The primary key for this table. A globally unique, system-generated identifier for a MenuEntry object.
Call Handler *	CallHandlerObjectId	The unique identifier of the CallHandler object to which this menu entry belongs.
Touchtone Key	TouchtoneKey	The character on the touch-tone keypad that this menu entry corresponds to (* , #, 0,1. . . 9).
Ignore Additional Input (Locked)	Locked	A flag indicating whether Cisco Unity Connection ignores additional input after callers press this key. Values: 0: Additional input accepted 1: Additional input ignored; Cisco Unity Connection performs the action assigned to the key.
Call Action	Action	The type of call action to take, e.g., hang-up, goto another object, etc.
Extension or URI	TransferNumber	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Description	DisplayName	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Transfer Type	TransferType	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Rings to Wait for	TransferRings	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Target Conversation	TargetConversation	The name of the conversation to which the caller is routed.
Target Handler Object Id	TargetHandlerObjectId	The unique identifier of the specific object to send along to the target conversation.

Caller Input

Title	Field Name	Description
Message	callerInput_tab_message	
Callhandler Menu Entry	CallhandlerMenuEntry.[n]	
Object Id	ObjectId	The primary key for this table. A globally unique, system-generated identifier for a MenuEntry object.
Call Handler *	CallHandlerObjectId	The unique identifier of the Call Handler object to which this menu entry belongs.
Touchtone Key	TouchtoneKey	The character on the touch-tone keypad that this menu entry corresponds to (* , #, 0,1. . . 9).
Ignore Additional Input (Locked)	Locked	A flag indicating whether Cisco Unity Connection ignores additional input after callers press this key. Values: 0: Additional input accepted 1: Additional input ignored; Cisco Unity Connection performs the action assigned to the key.
Call Action	Action	The type of call action to take, e.g., hang-up, goto another object, etc.
Extension or URI	TransferNumber	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Description	DisplayName	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Transfer Type	TransferType	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Rings to Wait for	TransferRings	This setting only applies if “Call Action” is set to ‘Transfer to Alternate Contact Number’.
Target Conversation	TargetConversation	The name of the conversation to which the caller is routed.
Target Handler Object Id	TargetHandlerObjectId	The unique identifier of the specific object to send along to the target conversation.

Greetings (Auto Attendant only)

Title	Field Name	Description
Message	greetings_tab_message	
Greeting	Greeting.[n]	
Greeting Type	Enabled	The type of greeting, e.g. “Standard,” “Off Hours,” “Busy,” etc.
Enabled	Enabled	If TimeExpires is set, this field is ignored.
Time Expires	TimeExpires	The date and time when the greeting rule expires. The greeting rule is considered not expired (enabled), if the value is NULL or a future date. The greeting rule is considered expired (disabled), the value is in the past.
Callers Hear	PlayWhat	The source for the greeting when this greeting is active.
Play the “Record Your Message at the tone” Prompt	PlayRecordMessage Prompt	A flag indicating whether the “Record your message at the tone?” prompt prior to recording a message.
Callers See My Personal Recording	EnablePersonal Video-Recording	It will Enable the Personal video Recording in CUCA.
Callers See Play the “Record Your Message at the Tone” Prompt	PlayRecordVideo MessagePrompt	A flag indicating whether the “Record your message at the tone?” prompt prior to Video recording a message.
Ignore Caller Input During Greeting	IgnoreDigits	A flag indicating whether Cisco Unity Connection takes action in response to touchtone keys pressed by callers during the greeting.
Allow Transfers to Numbers Not Associated with Users or Call Handlers	EnableTransfer	A flag indicating when an extension is dialed at the greeting and the extension is not available whether to transfer to another extension.
Times to Re-prompt Caller	Reprompts	The number of times to reprompt a caller. After the number of times indicated here, Cisco Unity Connection performs the after-greeting action.
Delay between Re-prompts	RepromptDelay	The amount of time (in seconds) that Cisco Unity Connection waits without receiving any input from a caller before Cisco Unity Connection prompts the caller again.

Title	Field Name	Description
After Greeting	AfterGreetingAction	The type of call action to take, for example, hang-up, goto another object, etc.
After Greeting Target Conversation	AfterGreetingTarget Conversation	The name of the conversation to which the caller is routed.
After Greeting Target Handler Object Id	AfterGreetingTarget HandlerObjectId	The unique identifier of the specific object to send along to the target conversation.
Call Handler Object Id	CallHandlerObjectId	The unique identifier of the Call Handler object to which this greeting rule belongs.
Callhandler URI	CallhandlerURI	
Greeting Stream Files URI	GreetingStreamFilesURI	
Greetings Type	GreetingType	The type of greeting, e.g. “Standard,” “Off Hours,” “Busy,” etc.
URI	URI	

Record/Playback (Auto Attendant only)

Title	Field Name	Description
Message	RecordPlayback.note	A special interface, which allows administrators to trigger a call to a physical device, which allows for recording or playback of a greeting. The extension to dial must be an accessible extension for the admin (or user) to answer and record or listen to greetings.
Call Handler Name	RecordPlayback.call_handler	Call Handler Name.
Extension	RecordPlayback.extension	Extension to Record message on.
Specific Greeting	RecordPlayback.specific_greeting	The unique identifier of the Call Handler object to which this menu entry belongs.
Greetings	RecordPlayback.greeting	Greetings.
Duration	RecordPlayback.duration	Duration to allow enough time to make recording/playback.

Upload Greeting (Auto Attendant only)

Title	Field Name	Description
Message	note	Upload a greeting to the selected Call Handler.
Greeting File	Upload.filename	Call Handler Name.
Call Handler Name	Upload.call_handler	Call Handler Name.
Specific Greeting	Upload.specific_greeting	Specific Greeting.
Greetings	Upload.greeting	Greetings.

18.8. Manage Greeting Files

18.8.1. Manage Greeting Files

This option allows you to independently upload previously created greeting (.wav) files, which can be used when adding or updating call handlers at a hierarchy level.

Note: The Unity Connection server port that is used when uploading greeting files is the port specified during Unity Connection Publisher setup - see *Set up Cisco Unity Connection*.

---

1. Click **Auto Attendant > Manage Greeting Files**.
2. Click **Add**.
3. Click **Browse** to select the required greeting file from the directory in which it was saved.
4. Enter an optional description to uniquely identify the greeting file.
5. Click **Save**.

Uploaded greeting files are available to use on the **Record/Playback** and **Upload Greeting** tabs when you modify a call handler, see *Modify a Call Handler (Auto Attendant)*.

18.9. Cisco Unity Connection Schedule

18.9.1. Call Handler (Auto Attendant) Schedule

Note: You can only manage schedules at the same hierarchy level (or lower) as your log in level. For example, if you login as a customer administrator, you can view schedules at your own customer hierarchy level, and add new schedules at (or below) your hierarchy level.

During initial installation, VOSS-4-UC imports two predefined schedules from Cisco Unity Connection. These are accessed via **Services > Auto Attendant > Schedule**:

- **All Hours**
- **Weekdays**

By default, the **All Hours** schedule is configured to be “active” 24 hours a day, 7 days a week, with no holidays. Routing rules that follow this schedule will always be active, and call handlers that use this schedule ‘as is’, will never use off hour transfer settings or play closed greetings.

The **Weekdays** schedule is configured to be active from 8 a.m. to 5 p.m. (in the time zone of the Cisco Unity Connection server) from Monday through Friday. It is also configured to observe any days and times that are set in the default Holidays schedule.

Note: By default the **Holidays** schedule is not configured for any days or times. — at a minimum you may want to add days and times to this holiday schedule when your organization will be closed.

Designating Holidays

When a Holiday setting is in effect, holiday greetings are played (if enabled), and off hours transfer rules are observed. You can set up several years of holidays at a time. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.

See also:

- *Create a Call Handler (Auto Attendant) Schedule*
- *Modify a Call Handler (Auto Attendant) Schedule*

18.9.2. Create a Call Handler (Auto Attendant) Schedule

You may want to create a new schedule for your organization.

On the **Schedule** form (modify or add), take note of the following field:

Uses Holiday Schedule - If you want your schedule to recognise days that are included as holidays in a holiday schedule, then choose a holiday schedule from the **Uses Holiday Schedule** drop-down list. Any day included in the selected holiday schedule will be recognized as a holiday.

If you want to create a new holiday schedule:

1. Select the **Is Holiday** check box.
2. Click **Holiday Details +** enter the following fields:
    - **Name**
    - **Holiday Start Date**
    - **Holiday End Date**
    - **Start Time**
    - **End Time**.
3. Add more days to the holiday as required by clicking **+** next to the entered holiday, and entering new details in the fields.
4. Click **Save** when complete.

Note: Another method to create a new schedule is to:

1. Select an existing schedule from the **Schedule** list view.
2. Clone it (**Action > Clone**) to the desired hierarchy level.
3. Edit as required.
4. Click **Save**.

18.9.3. Modify a Call Handler (Auto Attendant) Schedule

To edit a Call Handler schedule:

1. From the **Schedule** list view, click on the schedule that you want to edit.

2. Select the **Schedule Details** link name and edit the required fields (as described under *Create a Call Handler (Auto Attendant) Schedule*).
3. Click **Save** when complete.

To delete a Call Handler schedule:

1. From the **Schedule** list view, select the check box next to the schedule you want to delete. If you want to delete more than one schedule, select multiple check boxes.
2. Click **Delete** on the button bar.
3. Click **Yes** on the dialog box to delete.

18.10. Cisco Unity Connection Localization

18.10.1. Cisco Unity Connection Localization

Provider administrators or higher can manage multi-site, multi-country customers by setting geo-specific information using the Site Defaults Doc. Using this information, administrators can use custom Configuration Templates (as in the Quick Add Group for Quick Add Subscriber), to set this information on a per-site level.

Timezones and languages in VOSS-4-UC are populated with the required CUC timezones and languages. These are typically selected from the relevant drop-down lists as described under Modify Site Defaults.

Note: You must only add timezone and language codes in VOSS-4-UC that match the installed timezones and languages on the associated CUC Server. The names entered must uniquely describe the timezone and code.

See also:

- *Add a TimeZone Filter*
- *Add a Language Filter*

18.10.2. Add a TimeZone Filter

To add a custom Cisco Unity Connection timezone filter:

1. Log in as provider administrator or higher.
2. Choose **Services > Cisco Unity Connection Localization > TimeZone Filters** to see a list of time-zone filters currently in VOSS-4-UC.
3. Click **Add**.
4. Enter the following:
    a. TimeZone Code - this is a mandatory field, and must match a timezone code installed on the associated Cisco Unity Connection Server.
    b. TimeZone Name - this is a mandatory field, and must be a unique description for the timezone code above.
5. Click **Save**.

18.10.3. Add a Language Filter

To add a custom Cisco Unity Connection language filter:

1. Log in as provider administrator or higher.
2. Choose **Services > Cisco Unity Connection Localization > Language Filters** to see a list of language filters currently in VOSS-4-UC.
3. Click **Add**.
4. Enter the following:
    a. **Installed Language Code** - this is a mandatory field, and must match a language code installed on the associated Cisco Unity Connection Server.
    b. **Language Name** - this is a mandatory field, and must be a unique description for the language code above.
5. Click **Save**.

19 Overbuild

19.1. Overbuild Introduction

19.1.1. Overbuild Overview

Important: It is recommended that VOSS-4-UC training and/or VOSS Services are engaged during the initial use of the feature to help ensure optimized processes and guidance.

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

The Overbuild feature enables Provider and Reseller Administrators to integrate an existing, deployed Unified Communications (UC) system into VOSS-4-UC without reprovisioning, unless required. This option is available for single-cluster dedicated deployments only. Overbuild provides tools to help the administrator manage the data synced from existing configurations in Cisco Unified Communications Manager and Cisco Unity Connection.

Although a deployed Unified CM system does not contain such VOSS-4-UC components as a hierarchy or a subscriber, the relationship between Unified CM components makes it possible to, for example, create a VOSS-4-UC subscriber at a site hierarchy during the Overbuild process. The necessary workflows, macros and brownfield move processes are available for this purpose. You will not need to access these tools directly; they are part of the **Run Overbuild** menu interface.

The Overbuild logic can be summarized as follows:

- **Phones** - This is based on the device pool of the phone. It will be moved to a site based on the device pool matching one of the device pools set up under the site defaults for a site.
- **Phone Remote Destinations** - This will move the remote destinations to the site of the associated phone.
- **Users** - If the user has an associated phone then the user is moved to the same site as the phone.

  If the user does not have an associated phone then the user must be manually moved to the relevant site using the **Move Users** menu option under either **User Management** or **Overbuild**.

  It is recommended this happens prior to the Overbuild process so that all their related services are moved during overbuild; otherwise the Overbuild will need to be run again after moving the user to handle their related services.
- **Device Profiles** - this will move the device profile to the same site as the user associated to the device profile.

- **Remote Destination Profiles (RDP)** - this logic is the same as phones - based on the device pool of the RDP. It will be moved to a site based on the device pool matching one of the device pools setup under the site defaults for a site.
- **Remote Destinations** - this will move the RD to the same site as the associated RDP
- **Lines** - this will move the line to the same site as the phone/device profile/RDP it is associated to.
- **CUC Users** - this will move the voicemail user to the same site as the base user.
- **Webex Teams Users** - this will move existing Webex Teams Users that are synced into VOSS-4-UC to the same site as the base user (if it finds a matching email address).
- **Contact Center Agents** - this will move contact center agents to the same site as the base user (if it finds a matching Unified CM user ID).

The Overbuild process involves five broad steps:

- Perform initial manual setup and configuration on VOSS-4-UC.
  - The business information of the existing, deployed system is identified and entered into VOSS-4-UC, optionally by the bulk load process. This means hierarchy information is created with customers, sites and site codes. Some configuration data is initially generated, for example site Dial Plan (if applicable) and Site Defaults data. This data should be modified if required according to Unified CM data, so that Overbuild processing can move data to required sites.

    For example, the default, generated VOSS-4-UC Site Defaults for a site have the Site name as the Device Pool name. Since the Site Defaults are used in the Overbuild process, this name should be modified to match the Device Pool name on the imported Phones before the Overbuild process is run. VOSS-4-UC allows Provider and Reseller Administrators to modify Site Defaults in order to modify the configuration of an Overbuild process.

    Note:

    While Customers and Sites have access to the Site Defaults under the **Site Management** menu, the **Overbuild Defaults** tab is only visible to Provider and Reseller Administrators.
  - Create a shell dial plan schema group at the Customer hierarchy. The shell schema group enables Partners, Resellers, and Provider Administrators to access customers that have existing or deployed dial plans without having to use the pre-packaged type 1-4 dial plans. The shell schema groups only contain two default values: Device Pool and CUCM Group. The rest of the fields are blank for customization. This enables administrators to “over-build” VOSS-4-UC operations on top of customers’ existing dial plans.

    See “Provider HCS Dial Plan Management Support Guide”.
  - Network device connections are identified, created, associated with a Network Device List, and imported. This includes Unified CM and CUCX clusters.

    Caution:

    Whenever this data is synced in, it becomes managed by VOSS-4-UC and, as a result, would be deleted by any hierarchy delete. Delete failures can result with existing deployed dial plans. See *Delete Issues and Purges* for information on managing these issues.

    One Unified CM typically belongs to a customer and resides in a cluster, so this device import takes place at the created customer hierarchy. The device can also be associated with a Network Device List on VOSS-4-UC that is mapped to a created hierarchy.
- If the **Users** check box is selected on the **Run Overbuild** tool, users exposed under the **User Management** menu are moved to the site of their associated phones as specified in the Site Defaults Doc Device Pools.

Users without phones will not be moved and can be moved separately - see *Move Users*.

The following model instances are moved from customer level to the site level:

- `data/User`
- `data/LdapUser`
- `data/SsoUser`
- `data/NormalizedUser`
- `data/HcsUserProvisioningStatusDAT`
- `data/HCSHcmfUserDAT`
- `device/cucm/User`
- `device/hcmf/User` (only if HCM-F is installed)

- If the **Lines** check box is selected on the **Run Overbuild** tool, lines are moved to the relevant site, and marked as in use in the Directory Number (DN) inventory. If a matching DN inventory entry does not exist then one is created. DN entries are created at site by default unless the **Create Internal Number Inventory at Customer** check box is selected on the Site Defaults Doc **Overbuild Defaults** tab.
- The **Run Overbuild** tool selects which data to move based on device pool configurations. You can run the tool for all sites, or a particular site.

  Note:

  The existing system's provisioned phones that have been imported should have their Device Pools matched with Site Default Data values on each specific site.

  The imported elements are moved according to Overbuild Move Workflows, which are triggered by the **Run Overbuild** tool. These workflows identify imported network device data and move it to the site hierarchy that corresponds to the existing deployed site.
- Manually validate and modify the overbuild run by reviewing the moved items using Overview Tool. Use Device Models and/or Relations to move, update, delete, and in a few limited cases add instances of device types for the selected hierarchy.
- Perform post-move operations:
  - Move any users who were not moved during the Overbuild process - see *Move Users*.
  - Add your E.164 inventory (optional) - see *Add E.164 Inventory*.
  - Filter calling search spaces and assign a class of service (optional) - see *How to Filter Calling Search Spaces and Assign a Class of Service*.
  - Perform Self-service authentication provisioning steps for non-LDAP, LDAP, and SSO-enabled scenarios - see *User Authentication*.
  - Add additional internal number inventory for future lines - see *Add Directory Number Inventory*.

19.1.2. Overbuild Steps

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

Provider and Reseller Administrators can follow these general steps to use the Overbuild tool:

1. Provision the business hierarchy. This can be done manually in VOSS-4-UC or by bulk load (see “Bulk Administration” topics and *Bulk Loading a File*).
2. Associate a shell schema group with the customer, then add a custom dial plan under “Advanced Configuration”. (This step is optional at the site hierarchy). See “Provider HCS Dial Plan Management Support Guide”.
3. Provision Cisco UC Applications, network device lists, and network device list references. Once UC Applications are configured, the sync from Cisco Unified Communications Manager will be scheduled and executed. See “Data Sync” topics.
4. Choose the device pool and devices for the site on both the **Site Defaults > General** and **Overbuild Defaults** tabs. See *Overbuild Site Defaults: Overview*.
5. Choose **Run Overbuild** to move the imported UC Applications data into the site hierarchy that corresponds with the existing deployed site. See *Run Overbuild: Overview*.
    - Users exposed under the **User Management** menu are moved to their associated phones if the **Users** check box is selected on the **Run Overbuild** tool.

      Users are moved to their phones if the phones have the user set as the OwnerUserID, if the **Users** check box is selected on the **Run Overbuild** tool.

      Note: The User’s role is not changed when moving to Site.
    - Lines are moved and marked as in use in the Directory Number (DN) inventory if the **Lines** check box is selected on the **Run Overbuild** tool. A Site DN inventory is created.

      If the DN instance already exists, it is updated as in use. The DN inventory instance is created at the site level by default. This can be set to Customer in the SiteDefaultDoc before running OverBuild.

      Note: Adding Directory Number inventory at Customer level is only possible if the DialPlan in use is non SLC(Site Location) Based, or if no DialPlan is in use.
6. Choose **Overview Tool** to verify the number of Unified Communications elements at the selected hierarchy and below. See *Summary of the Overview Tool*.
7. Optionally, review the device model types listed with hierarchy in the Device Models or Subscriber Management menu. See *Device Models: Overview*.
8. Perform postmove operations:
    - Add your E.164 inventory (optional) - see *Add E.164 Inventory*.
    - Filter calling search spaces and assign a class of service (optional) - see *How to Filter Calling Search Spaces and Assign a Class of Service*.

19.2. Moving Model Instances

19.2.1. Moving Model Instances: Overview

If the Move operation is enabled for a model, instances can be moved from its current hierarchy level to another level. Data models, Device models and Relations can be enabled for the Move operation. For lists of objects moved during a move operation, see *Objects that are Moved During the Overbuild* for data and device models, and *Subscriber Management - Moving Items* for Subscriber Management models.

Instances can only be moved up in the hierarchy if the administrator is at a higher hierarchy. For example, for an instance at level cust1.site1 and the level cust1.site2 also exists, then the user needs to be at level cust1 to carry out a move of this instance 'sideways' to cust1.site2 by going up and back down the hierarchy levels.

The move is typically used in conjunction with data sync, which pulls the entities in, for example users, phones, dial plan, and so on. By default the entities reside at the level of the cluster, so the move feature allows them to be allocated to a different hierarchy (if needed).

19.2.2. Move Rules

From the user interface, the following move rules apply:

- On the GUI, the only option shown on the drop-down is to move an item to a lower hierarchy.
- For the core application and the Overbuild tool:
  - LDAP device models can be moved to a hierarchy that is at or below the hierarchy where the device is located, regardless of the Network Device List Reference (NDLR).
  - Non-LDAP device models can be moved to a hierarchy where the device is located.
  - Non-LDAP device models can be moved to a hierarchy where the NDLR references the associated device.
  - Other instances at a hierarchy node can only be moved to a hierarchy that is below their current hierarchy.

Once the resource is moved, metadata of all the resources at the moved hierarchy and below is updated to indicate the latest changes in the hierarchy path.

Note: For User Management local administrators and users, where the language is derived from the default hierarchy language, the default language is recalculated based on the new hierarchy tree location.

19.2.3. Subscriber Management - Moving Items

Administrators have privileges to manually move these Subscriber Management items:

- Lines
- Voicemail
- WebEx
- Webex Teams
- Hunt Groups
- Call Pickup Groups

It is recommended to use the dedicated tools to move subscribers and phones between customer and site hierarchy levels.

19.2.4. Move Subscriber Management List View Items

Procedure

1. Log in as a Customer Administrator or higher.
2. Choose the hierarchy level of the **Subscriber Management** menu item from which you want to move the items.
3. From the list view, choose the items to be moved by selecting the check boxes next to the items.
4. Click **Action > Move**. A form prompts you to choose the target hierarchy from a drop-down list.
5. Choose the target hierarchy and click **OK**.

The items are moved to the selected hierarchy, and will then be shown in their new hierarchy.

19.3. Overbuild Site Defaults

19.3.1. Overbuild Site Defaults: Overview

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

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

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

The settings on this tab work as follows:

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

  The list of defaults when the menu **Site Management > Defaults** is selected, show “true” in the Include Site for Overbuild column.
- Create Internal Number Inventory at Customer: If clear, the internal number inventory is created at site level only. If selected, the internal number inventory is created at customer level only, and will be used by all sites belonging to that customer, default = cleared.

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

- Additional Device Pools: By default, if a site is included for the Overbuild process, the Default CUCM Device Pool on the General Defaults tab has to match the Device Pool of the phones that have been imported in order for these and their related objects to be moved to the site at which the Site Defaults

Doc exists. The Run Overbuild tool uses the Device Pool in order to determine which devices and models are to be moved to the site where the site defaults are defined.

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

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

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

19.4. Run Overbuild

19.4.1. Run Overbuild: Overview

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

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

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

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

Given	Then
• 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**

  - 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

- 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.

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.

19.4.2. Objects that are Moved During the Overbuild

The overbuild processes the imported Unified CM objects for selected sites in the current customer. During overbuild, some objects are moved to the site hierarchy, while others remain at the customer hierarchy.

Objects That Are Moved to the Site Hierarchy

Unified CM models	device/cucm/Line device/cucm/Phone device/cucm/RemoteDestinationProfile device/cucm/RemoteDestination device/cucm/DeviceProfile device/cucm/User
HCMF (if installed)	device/hcmf/User
Cisco Unity Connection models	device/cuc/User device/cuc/UserPassword device/cuc/UserPin device/cuc/AlternateExtension device/cuc/SmtpDevice device/cuc/SmsDevice device/cuc/PagerDevice device/cuc/PhoneDevice device/cuc/HtmlDevice device/cuc/CallHandler device/cuc/CallhandlerMenuEntry device/cuc/CallhandlerTransferOption device/cuc/Greeting device/cuc/MessageHandler
Voicemail-related models	device/cuc/User device/cuc/UserPassword device/cuc/UserPin device/cuc/AlternateExtension device/cuc/SmtpDevice device/cuc/SmsDevice device/cuc/PagerDevice device/cuc/PhoneDevice device/cuc/HtmlDevice
Self-care models	device/cuc/Callhandler. By default, one CallHandler entry is created when a Cisco Unity Connection user is created. device/cuc/CallhandlerMenuEntry

- *Contact Center Management*

  After the initial sync, agents will be located at the customer hierarchy level. The overbuild tool will attempt to move these agents to the correct site hierarchy levels, based on matching Cisco Unified CM users. This matching is done according to the Unified CM user ID and the agent user ID.

Contact Center models	device/uccx/Team device/uccx/Skill device/uccx/ResourceGroup device/uccx/Agent

Data models affected when the user is moved during Overbuild:

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

Objects That Remain at the Customer Hierarchy

Unified CM models	device/cucm/DevicePool device/cucm/Region device/cucm/Location device/cucm/VoiceMailPilot device/cucm/VoiceMailProfile device/cucm/Css device/cucm/RoutePartition device/cucm/HuntList device/cucm/HuntPilot device/cucm/LineGroup device/cucm/CallPickupGroup device/cucm/DirectedCallPark device/cucm/CallPark device/cucm/CtiRoutePoint
Cisco Unity Connection models	operator undeliverablemessagesmailbox
CallHandler device models	Goodbye Opening Greeting Operator operator undeliverablemessagesmailbox
Call Pickup Groups	no objects moved

19.5. Overbuild Tool

19.5.1. Summary of the Overview Tool

Use the Overview Tool to validate your Run Overbuild process. Overbuild users can use individual device models to make sure that the required Unified CM elements have been moved to the right hierarchy.

Choose the **Overbuild > Overview Tool** menu option. It can be used at the Customer or Site hierarchy. The report shows the numbers of each Unified CM customer-specific data, for example phones, lines, users, etc. at the selected hierarchy and below. This is displayed in the format "current hierarchy/below." For example, "390/20" means that 390 elements are at the current hierarchy and 20 elements are at hierarchies below the current hierarchy. Change the hierarchy to inspect the overbuild overview at that hierarchy.

When you run the Overview Tool at Site level, the number on the right will always show as 0, since Site is the lowest VOSS-4-UC hierarchy level.

To verify the individual device models after running Overbuild, choose **Overbuild > Device Model > (desired model name)**. The hierarchy where each device model instance exists will be listed in the right-most column in the list view of the device model.

19.6. Run CUCDM8 Dial Plan Overbuild

19.6.1. Run CUCDM8 Dial Plan Overbuild

The Run CUCDM8 Dial Plan Overbuild process moves specific CUCDM 8 Dial Plan elements, which have been imported from Unified CM, to a specified Site based on the CUCDM 8 Location Name and Location ID.

Prerequisites

You must know the following CUCDM 8 location details:

- Location Name
- Location ID
- Location Dial Plan Country Code

Procedure

1. Log in as a provider administrator or higher.
2. Enter the CUCDM 8 **Location Name**, **ID**, and **Dial Plan Country Code** to identify the CUCDM 8 location from which you want to move the elements.
3. From the **Destination Site Name** drop-down, choose the Site to which you want to move the elements.
4. Click **Save**.

Dial Plan Elements Moved to the Site Hierarchy

Dial Plan Elements moved when running **CUCDM8 Dial Plan Overbuild** are:

Model Type	Model Field	Condition	Filter Text
device/cucm/Region	name	endswith	phone-{{ input.v8_siteid }}
device/cucm/Region	name	startswith	{{ input.v8_sitename }}
device/cucm/Line	shareLineAppearanceCssName	endswith	CSS{{ input.v8_siteid }}
device/cucm/Line	shareLineAppearanceCssName	startswith	{{ input.v8_sitename }}
device/cucm/Location	name	endswith	-{{ input.v8_siteid }}
device/cucm/Location	name	startswith	{{ input.v8_sitename }}
device/cucm/DevicePool	name	endswith	pool{{ input.v8_siteid }}
device/cucm/DevicePool	name	startswith	{{ input.v8_sitename }}
device/cucm/DevicePool	regionName	endswith	-{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Calls{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	CallsCLIR{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	-{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Enh{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Std{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Rst{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Service{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Internal{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Features{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	LclManagers{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	PT{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Site{{ input.v8_siteid }}
device/cucm/RoutePartition	name	endswith	Plus{{ input.v8_siteid }}
device/cucm/RoutePartition	name	startswith	{{ input.v8_sitename }}
device/cucm/Css	name	endswith	CSS{{ input.v8_siteid }}
device/cucm/Css	name	endswith	LBO{{ input.v8_siteid }}
device/cucm/Css	name	startswith	{{ input.v8_sitename }}
device/cucm/CtiRoutePoint	callingSearchSpaceName	endswith	CSS{{ input.v8_siteid }}
device/cucm/CtiRoutePoint	devicePoolName	endswith	{{ input.v8_siteid }}
device/cucm/CtiRoutePoint	devicePoolName	startswith	{{ input.v8_sitename }}
device/cucm/VoiceMailProfile	voiceMailPilot.cssName	endswith	CSS{{ input.v8_siteid }}
device/cucm/VoiceMailPilot	cssName	endswith	CSS{{ input.v8_siteid }}
device/cucm/VoiceMailPilot	cssName	startswith	CSS{{ input.v8_siteid }}

Continued on next page

Table 1 -- continued from previous page

Model Type	Model Field	Condition	Filter Text
device/cucm/CallPark	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	endswith	Feature{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/DirectedCallPark	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/DirectedCallPark	routePartitionName	endswith	Feature{{ input.v8_siteid }}
device/cucm/DirectedCallPark	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/CallPickupGroup	name	startswith	{{ input.v8_sitename }}
device/cucm/CallPickupGroup	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/CallPickupGroup	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/CallPickupGroup	routePartitionName	endswith	AllowCallFeatures{{ input.v8_siteid }}
device/cucm/HuntPilot	routePartitionName	endswith	Site{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	-{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	-{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Plus{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	isexactly	AllowEmerCalls{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	isexactly	AllowInternal{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Enh{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Std{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	Rst{{ input.v8_dp_countrycode }}{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	endswith	-PT{{ input.v8_siteid }}
device/cucm/TransPattern	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/RoutePattern	routePartitionName	isexactly	SNRRRPT{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	isexactly	AllowVMCalls{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	endswith	EmerCalls{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	isexactly	AllowInternal{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	endswith	-PT{{ input.v8_siteid }}
device/cucm/RoutePattern	routePartitionName	startswith	{{ input.v8_sitename }}
device/cucm/RouteList	name	endswith	-{{ input.v8_siteid }}
device/cucm/RouteGroup	name	endswith	-{{ input.v8_siteid }}
device/cucm/CallingPartyTransformationPattern	routePartitionName	endswith	PT{{ input.v8_siteid }}
device/cucm/CalledPartyTransformationPattern	routePartitionName	endswith	PT{{ input.v8_siteid }}

Continued on next page

Table 1 -- continued from previous page

Model Type	Model Field	Condition	Filter Text
device/cucm/VoiceMailProfile	description	endswith	location{{ input.v8_siteid }}
device/cucm/CallPark	routePartitionName	isexactly	AllowCallFeatures{{ input.v8_siteid }}
device/cucm/GatewaySccp Endpoints	callingSearchSpaceName	endswith	-CSS{{ input.v8_siteid }}
device/cucm/GatewayEndpointAnalogAccess	callingSearchSpaceName	endswith	-CSS{{ input.v8_siteid }}
device/cucm/H323Gateway	callingSearchSpaceName	endswith	-CSS{{ input.v8_siteid }}
device/cucm/MeetMe	routePartitionName	endswith	Site{{ input.v8_siteid }}

19.7. User Phone Association

19.7.1. User Phone Associate Tool

VOSS-4-UC uses the associated or controlled devices value on the Unified CM user (Subscriber in VOSS-4-UC) to determine which phones are associated to that Subscriber.

This User Phone Associate tool will ensure that Unified CM phones in the system with the ownerID value set, are correctly associated to the Unified CM user (Subscriber) for correct association in VOSS-4-UC.

A common situation where this might be the case is in the event of phones synced in from an existing environment for Overbuild - where the ownerID on the phones were set, but were not associated from the Unified CM User perspective. The symptom to look for is when you do not see the phones under the Subscriber view, but that you think they are owned by the user - an indication that this tool needs to be run to correct the association.

Note: When adding phones and subscribers from *within* VOSS-4-UC, the phone-user relationship is bi-directional.

Procedure

1. Navigate to the hierarchy of the Unified CM and choose it from the **CUCM** dropdown list.

   The **Number of Phones that will be checked** value that is displayed is the number of phones on the Unified CM at the hierarchy that have been synced in to VOSS-4-UC and have an ownerID set, but cannot be found to be an associated device of any subscriber at the hierarchy or lower.

2. Click **Save** to run the tool. Subscribers will be searched on VOSS-4-UC that match the ownerID and if found, their associated devices will be updated with the phone.

If the tool is now re-run for the selected Unified CM and any of the checked phones were set as associated devices, the **Number of Phones that will be checked** value will decrease accordingly.

Note: If a subscriber already has other associated devices, any new associated devices will be appended to the existing list.

19.8. Device Models

19.8.1. Device Models: Overview

With the Device Models menu item, you can view details about the devices by model in the selected hierarchy. Like the Overview Tool, this can be useful to help you see where devices have moved as a result of the Overbuild process. When you select a device model type in the menu, a table presents you data about the devices of that model type in the hierarchy: the device names or identifiers, their device pools, their hierarchies at and below the one currently selected, and other data that varies with the device model selected.

Within a device model, you can modify, delete, and export the individual devices by selecting them. Additionally, you can change settings all at once for all the devices in a device model by selecting the **Select All** check box, located at the top-left on the table header, and choosing **Action > Bulk Modify**.

Caution: We do NOT recommend that you directly edit the device models in this menu, but use the other menus in VOSS-4-UC such as the Subscriber Day 2 menus. The Device Models menu items should be used for manually moving device models that the Overbuild tool cannot move or that need additional manual moves after Run Overbuild is executed.

For CUC models, there are two system users, operator and undeliverablemessagesmailbox, which will remain at Customer level. All associated CUC device models for the two system users will remain at the Customer hierarchy and will show in the device model counts and device model lists at the Customer hierarchy.

For call handler device models, there are 5 default instances that remain at the Customer hierarchy:

- Goodbye (a CUC system default call handler)
- Opening Greeting (a CUC system default call handler)
- Operator (a CUC system default call handler)
- operator (the system user ‘operator’ call handler)
- undeliverablemessagesmailbox (the system user ‘undeliverablemessagesmailbox’ call handler)

These 5 call handlers remain at the Customer hierarchy and appear in the device model count and device model lists for call handlers at the Customer hierarchy.

These device models also allow you to add device instances. Note that adding device instances here in the Overbuild menu is not recommended.

- CUCM CtiRoutePoint
- CUCM DirectedCallPark
- CUCM Phone
- WebEx User

19.8.2. Find a User Associated with a CUC Device Model

The CUC device models use internal UUID references to the CUC user objects. As a result, most CUC device models do not have a field showing the ID of the user to which the device model is associated. The VOSS-4-UC search function can be used to find this associated user information.

Procedure

1. Choose **Overbuild > Device Models**.
2. Click the desired CUC device model in the menu. A list of the CUC device models appears.
3. Click the desired device model instance.
4. In the CUC device model output, find the field Subscriber Object ID.
5. In the search box at the top right of the VOSS-4-UC administrator GUI, type this string:

   ```
   device/cuc/User WITH object_id like 9b16c8ce-edd9-43c4-9262-c25296d3560b
   ```

   where 9b16c8ce-edd9-43c4-9262-c25296d3560b would be replaced with the output of the Subscriber Object ID.

   The equivalent VOSS-4-UC API request would be:

   ```
   https://<host-or-proxy>/api/tool/Search/?
   format=json&
   device%2Fcuc%2FUser%20
    with%20object_id%20like%20
     9b16c8ce-edd9-43c4-9262-c25296d3560b
   ```

19.9. Filter Calling Search Spaces and Assign a Class of Service

19.9.1. How to Filter Calling Search Spaces and Assign a Class of Service

For the overbuild, VOSS-4-UC does not filter the Calling Search Space (CSS) fields that are used for various lines and devices in the user interface. You can filter the CSSs so that drop-down lists contain only the CSSs that are relevant to the selected devices and lines. You can also flag a CSS as Class of Service (CoS).

Procedure

1. Enable CSS filtering.
   a. Log in to VOSS-4-UC as provider, reseller or customer administrator.
   b. Choose the customer hierarchy.
   c. Choose **Dial Plan Management > Customer > Dial Plan**.
   d. Click the dial plan.
   e. Select the **Enable CSS Filtering** check box.
   f. Click **Save**.

2. Move CSSs from the customer hierarchy to the site hierarchy.
    a. While still at the customer hierarchy, choose **Overbuild > Device Models > CUCM CSS**.
    b. Select the check box to the left of each CSS that you want to move.
    c. Click **Action > Move**.
    d. From the **Move Resources to Hierarchy** drop-down, choose the site to which you want to move the CSS.
    e. Click **OK**.
    f. Repeat steps b through e if you want to move more CSSs.
3. Identify the CSSs that you want to appear in the filtered drop-down lists for the devices, services, and lines.
    a. Choose the site hierarchy.
    b. Choose **Dial Plan Management > Site > Class of Service**.
    c. Click **Add**.
    d. From the **Class of Service Name** drop-down, choose the CoS that you want to associate with the CSS.
    e. Click **Save**.
    f. Repeat steps b through e for each CoS that you want to associate with a CSS.
4. Verify that the CSS field is filtered correctly.
    a. While still at the site hierarchy, choose **Subscriber Management > Lines**.
    b. Click **Add**.
    c. From the **Calling Search Space** drop-down, verify that the items in the list are the CSSs that you flagged as CoS.
5. (Optional) Remove the CoS flag from a CSS.
    a. Log in to VOSS-4-UC as provider, reseller or customer administrator.
    b. Choose the site hierarchy.
    c. Choose **Dial Plan Management > Site > Class of Service**.
    d. Click the required Class of Service Name.
    e. Click **Action > Exclude from CoS**.

    Note:

    Ensure that you exclude the CSS from the CoS when you want to remove the CoS flag. If you delete the CoS instead, the CSS is deleted from Unified CM.

20 Self Provisioning

20.1. Self-Provisioning Overview

The Cisco Unified Communications Manager Self-Provisioning feature allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user.

The following process is used to self-provision a phone:

1. The user or admin connects the phone to the network.
2. The phone auto-registers.
3. The user or admin dials the IVR application and satisfies the prompts.
4. The IVR application deletes the auto-registered phone and adds it back using templates associated with the user via their User Profile.

There are two requirements related to self-provisioning:

1. Before a phone can be self-provisioned, the user must exist in Cisco Unified Communications Manager along with their primary extension, self service ID, and user profile.
2. After the phone is self-provisioned, in order to do additional subscriber management for the user in VOSS-4-UC, the user, line, and phone must be at the site level in the VOSS-4-UC hierarchy.

20.2. Bottom-Up User Management

A bottom-up approach to user management means users are configured on Cisco Unified Communications Manager (Unified CM) and synced into VOSS-4-UC. Two possible methods for bottom-up user management are:

- Sync LDAP directory into Unified CM. Do not configure the LDAP directory sync in Unified CM to use a line mask or DN pool to create the user's primary extension. Instead, the user's primary extension and self-service ID are generated in VOSS-4-UC, using a line mask, universal line template, and self-provisioning user profile at the site level.

  Note:

  During LDAP sync to Unified CM, the user is assigned a User Profile via the Feature Group Template associated with the LDAP directory. In order for the line mask configured at the site on VOSS-4-UC to get applied, the User Profile assigned previously must be empty or it must be named the 'Standard (Factory Default) User Profile'.
- Use Unified CM Quick User/Phone Add to create a user and the user's primary extension.

20.3. Top-Down User Management

A top-down approach to user management means users and lines are configured on VOSS-4-UC and pushed into Cisco Unified Communications Manager (Unified CM). Users may be added via LDAP sync, the GUI, or bulk loading. When users are pushed to Unified CM the user's primary extension is created, and when a phone is self-provisioned for the user, the phone is automatically moved to the user's Site.

Use either of the following methods to configure the user in VOSS-4-UC:

- Generate the user's primary line and self-service ID using a line mask, universal line template, and a user profile at the site level.
- Set the self-service ID per user using Quick Add Subscriber.

Note: You can associate multiple devices (Jabber, iPhone, iPad, 78xx series IP phones, and 88xx series IP phones) to a single subscriber through VOSS-4-UC (Subscriber Management > Subscribers). This cannot be done through Quick Add Subscriber (QAS) as the default 9971 is added through QAS.

Using a combination of the methods above is possible but is not recommended. For example, you can enable the line mask at the site and use Quick Add Subscriber to set the primary line for some users while not setting it for others. When the line mask is applied, it first checks to see if a primary extension is already assigned to the user (perhaps via Quick Add Subscriber). If a primary extension is already assigned, the line mask is not applied.

20.4. Cisco Unified Communications Manager Configuration for Self-Provisioning

To use self-provisioning, regardless of whether top-down or bottom-up user management is used, you must complete these one-time configuration tasks on Cisco Unified Communications Manager:

- Ensure that the Cisco CallManager, Cisco CTIManager, and Self-Provisioning IVR services are activated
- Configure Auto Registration
- Create one partition and calling search space unique for self-provisioning
- Configure an Application User and credentials so the system can connect to the IVR self-provisioning service
- Configure a CTI Route Point (provides the number that users dial to connect to the IVR)
- Configure Self-Provisioning with the Application User and CTI Route Point

Refer to the Cisco Unified Communications Manager documentation for details.

20.5. Site Configuration for Self-Provisioning

Regardless of whether top-down or bottom-up user management is used, ensure that the following items have been configured in VOSS-4-UC:

- Site Dial Plan: **Dial Plan Management > Site > Dial Plan**

- Site Defaults: **Site Management > Defaults**
- Directory Number Inventory: **Dial Plan Management > Customer Management > Add Directory Number Inventory**

20.6. Generate a User's Primary Line

For top-down management, the system creates the user's primary line, associates the line as the primary extension, sets the self-service ID, and sets the user's profile. These activities occur when users are pushed to Cisco Unified Communications Manager.

For bottom-up management, the user's primary line is created (if necessary) when the user is moved to a site, or updated once at a site.

You create the line when you perform these tasks.

- Apply the line mask to a user attribute (typically the user's phone number).
- Use the Universal Line Template (ULT) to determine the route partition name and other line attributes. The ULT is specified in the Self-Provisioning User Profile, which is specified in the Site's Default User Profile.

For this approach, the administrator configures these items at the site level.

20.6.1. Procedure

1. Configure Universal Device Templates. See *Add a Self-Provisioning Universal Device Template*.
2. Configure Universal Line Templates. See *Add a Self-Provisioning Universal Line Template*.
3. Configure Self-Provisioning User Profiles. See *Add a Self-Provisioning User Profile*.
4. Configure a Site Default User Profile. See *Set a Default User Profile for a Site*.
5. Configure the Line Mask. See *Add Self-Provisioning Line Mask*.

20.7. Specify the Primary Line per Subscriber

In the top-down method that uses Quick Add Subscriber, the primary line pattern is specified by the admin. This creates the user's primary line, associates it as the primary extension, sets the self-service ID, and sets the user profile. The line attributes come from Quick Add Group configuration. Therefore, the Universal Line Template does not need to be configured.

20.7.1. Procedure

1. Configure Universal Device Template(s). See *Add a Self-Provisioning Universal Device Template*.
2. Configure Self-Provisioning User Profile(s). See *Add a Self-Provisioning User Profile*.
3. Configure a Site Default User Profile. See *Set a Default User Profile for a Site*.
4. Configure primary line per user.

For Quick Add Subscriber, add at least one line, and select the Self-Service ID check box.

20.8. Add a Self-Provisioning Universal Device Template

When the administrator or user self-provisions a phone, Cisco Unified Communications Manager deletes the autoregistered phone and adds the phone back into the database. The Universal Device Template (UDT) for the user's profile determines the various phone settings for the user's phone.

20.8.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Choose **User Management > Self-Provisioning > Universal Device Template**.
4. Click **Add**.
5. Enter the following required UDT information.

Field	Description
Name	Enter the name of the UDT.
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC regulates audio quality and video availability by limiting the amount of bandwidth for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.
Common Phone Profile	Choose a common phone profile.
Phone Personalization	Enable this setting to allow the UDT to work with Phone Designer, a Unified Communications widget. The widget lets a user customize the wallpaper and ringtones on a device.
Busy Trigger	This setting, which works with Maximum Number of Calls and Call Forward Busy, determines the maximum number of calls to be presented at the line. If the busy trigger is set to 40, incoming call 41 is rejected with a busy cause (and is forwarded if Call Forward Busy is set). If this line is shared, all the lines must be busy before incoming calls are rejected.
Max Number Of Calls	You can configure up to 200 calls for a line on a device. As you configure the number of calls for one line, the number calls that are available for another line decreases.
Multi-Level Precedence and Preemption	This setting specifies whether a device that can preempt calls in progress uses the capability when it places an MLPP precedence call.
Do Not Disturb Option	When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls.
Blf Presence Group	Enter the presence group applicable for busy lamp field buttons.
Device Mobility Mode	Turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device.

The following fields can be prepopulated, depending on customer, site, and dial plan configuration:

- Name
- Location
- Common Phone Profile
- BLF Presence Group

6. Enter the following optional, but highly recommended information. These fields can be prepopulated, depending on customer, site, and dial plan configuration.

Field	Description
Device Pool	Enter a site-specific device pool.
Owner User ID	The userid of the user associated with the phone. The recommended is Current Device Owner's User ID.

7. Enter other optional settings, if applicable.
8. Click **Save**.

20.9. Add a Self-Provisioning Universal Line Template

The Universal Line Template (ULT) is used before self-provisioning actually takes place. ULTs are used to create directory numbers on Cisco Unified Communications Manager. A directory number is identified by a pattern (the number portion) and a route partition. A directory number also has various settings that can be configured for the line. When a directory number is created using a ULT, the ULT determines the route partition and the line settings.

20.9.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Choose **User Management > Self-Provisioning > Universal Line Template**.
4. Click **Add**.
5. Enter the following required Universal Line Template information.

Field	Description
Name	The name of the universal line template
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC regulates audio quality and video availability by limiting the amount of bandwidth for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.
Partition	Enter the route partition used to create lines at the site.
Blf Presence Group	Enter the presence group applicable for busy lamp field buttons.

6. Enter other optional settings, if applicable.
7. Click **Save**.

20.10. Add a Self-Provisioning User Profile

20.10.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Choose **User Management > Self-Provisioning > User Profile**.
4. Click **Add**.
5. Enter the user profile information.

Field	Description
Name	Enter the name of the user profile. This field is mandatory.
Universal Line Template	Enter a site-specific ULT. This field is highly recommended.

6. Click the **Device Template Desk Phone** tab.
   a. Click '+' to add a new template.
   b. From the **Device Security Profile** drop-down, choose **Model-independent Security Profile** .
   c. From the **Sip Profile** drop-down, choose the required SIP Profile.
   d. Select the **Allow Control of Device From Cti** check box.
   e. From the **Calling Search Space** drop-down, choose the appropriate option, for example Cu2Si4-InternalOnly-CSS.
7. Click the **Line Template** tab.
   a. Click '+' to add a new template.
   b. From the **Partition** drop-down, choose the appropriate partition, for example Cu2-DirNum-PT.
   c. From the **Calling Search Space** drop-down, choose the appropriate calling search space, for example Cu2Si4-InternalOnly-CSS.
   d. From the **Voice Mail Profile** drop-down, choose the appropriate option, for example Default.
8. Click **Save**.
9. Enter other optional settings, if applicable.

20.10.2. What to Do Next

Set a Default User Profile for a Site.

20.11. Set a Default User Profile for a Site

Set a default user profile for a site, to be used when no user profile is specified when adding a subscriber.

20.11.1. Procedure

1. Choose **Site Management > Defaults**.
2. Click the user profile to set as the default.
3. On the **General Defaults** tab, and from the **Default User Profile (for User Self Provisioning)** drop-down, choose the default user profile for the site.
4. Click **Save**.

20.12. Add Self-Provisioning Line Mask

20.12.1. Procedure

1. Log in as provider, reseller, or customer administrator.
2. Set the hierarchy path to the site node where you want to configure self-provisioning.
3. Choose **User Management > Self-Provisioning > Line Mask**.
4. Click **Add**.
5. Provide the following information:

Field	Description
Description	A description of the Line Mask.
User Attribute	Select the user attribute used to generate the user's primary extension. The default is telephoneNumber. This field is mandatory.
Mask	Provide a mask which gets applied to the user attribute. The result is used as the user's primary extension. For example, assume user attribute is telephoneNumber and the mask is 4XXXX. Special characters and blanks are stripped from the user attribute before applying the mask. If the mask is applied to '(919) 867-5309', the user's primary extension would be set to 45309. This field is mandatory.

6. Click **Save**.

21 Administration Tools

21.1. Import

21.1.1. Import: Overview

Model definitions and instances can be imported using JSON files. These can be compressed (`.json.zip`) or be uncompressed files with extension `.json`.

The format of the JSON files should correspond with the JSON schema for the model or instance that is imported. Typically, a model instance is exported as a JSON file in order to obtain such a schema. The export can then for example be edited as required.

For each model instance in a JSON file, if it contains the same values for a business key as an existing model instance, then the import will update the existing instance. Otherwise, the import will add a model instance. The business key of a model is specified on its design form and can be seen in the Add Form schema of the Model API Help Reference.

When exporting items that belong to a package, all hierarchy information will be removed from item meta business keys so that the packages have no hierarchy.

The importing process will still adhere to the hierarchy specified in the meta of each item except for a data/Package instance, which will be imported at the import hierarchy (breadcrumb hierarchy). For items other than Packages, the hierarchy where the items is loaded can be overridden (to the same or lower hierarchy level only) by specifying the hierarchy in the meta of the item.

If no hierarchy is found in the meta of the item, then the hierarchy will be taken from the import hierarchy (breadcrumb hierarchy).

21.1.2. Import a File

1. Choose the hierarchy level for the import (not applicable to packages - see *Import: Overview* for more details).
2. Choose **Administration Tools > Import** to open the Import screen.
3. Click **Browse**, and choose the file (`.json`, `.json.tar.gz`, or `.json.zip`) that you want to import. Wait until the file name is displayed on the form.
4. Click **Import** on the button bar to import the file to the hierarchy.

21.2. Bulk Administration

21.2.1. Bulk Load Overview

The bulk loader tools enable the quick and easy management of system data using pre-populated MS Excel formatted spreadsheets.

A spreadsheet template can be generated by the system for any of the resources in the system - either from the GUI or the API.

The data on the sheet includes column headers to indicate the hierarchy, action, search criteria and attribute names of the model to which the data applies. Rows include the data for model individual instances.

Use a single sheet in the file to manage multiple templates by adding additional header rows and data under them. A file can include multiple sheets with a single or multiple templates on each.

When the file is loaded, it can either be processed immediately or scheduled for a date and time. A scheduled bulk load file is listed on the Schedule list view as a Single Execution schedule type and with resource type of data/BulkLoad. Items on the Schedule list are deleted once the scheduled item has been executed. This means that after a scheduled bulk load has been executed, you will no longer see it in the list of schedules.

A single parent transaction is created for the entire bulk load. Unless a sheet is set to execute rows in parallel, each row in the bulk load sheet results in a separate sub-transaction that is executed sequentially and synchronously. If a single sub-transaction fails, the bulk load transaction continues and does not roll back the preceding sub-transactions. In the case where a bulk load sub-transaction has other sub-transactions - for example a provisioning workflow with multiple steps - failure in any of the steps will cause a roll back of all the steps in the bulk load sub-transaction.

If a sheet is set to process rows in parallel, then by default, 14 rows are processed in parallel. Refer to the topic on the bulk load sheet layout for more details.

If a file is processed and further files are loaded, they are processed in parallel. Thus, bulk load transactions are executed in parallel, as with all transactions. Bulk load transactions are executed immediately.

Transactions, once started, cannot be canceled.

21.2.2. Data Export

Data can be exported in JSON format and as MS Excel spreadsheets.

The system JSON file format is used to Export and Import various operations on model instances. The operations available via JSON files are: Add, Modify, Delete. This Import and Export task is carried out from the GUI or API using the file Export and Import functionality.

The JSON file format for the different operations is available from the **Action** button on the GUI form of the specific model and choosing JSON as Export format from the drop-down list on the Export menu. The API provides a request URL and parameter for this task - refer to the API documentation. The export file format is a compressed JSON file. The import filename and format can be <filename>.JSON, <filename>.JSON.zip or <filename>.JSON.gz.

The Excel file format for data export of selected items can be carried out in the list or instance view of a model.

The commands are available from the **Action** button on the GUI form by choosing either Excel or Excel (formatted) from the drop-down list on the Export menu. The API provides a request URL and parameter for this task - refer to the API documentation. The export file format is a MS Excel XLSX file.

The Field Display Policy that applies to a menu item from which an Excel (formatted) export of data is carried out, is reflected in the Excel (formatted) exported sheet as follows:

- Titles of attributes
- Sequence of the attributes
- Group names
- Hidden fields, with the exception of mandatory fields.

21.2.3. Bulk Export of Model Data

1. Choose the hierarchy to which the model belongs.
2. Choose the items to be exported from the List view and click the **Action > Export**.
3. From the **Export format** drop-down, choose the required export format and click **OK** to export the selected items. The following file formats correspond with the selected drop-down item in the list:
   - JSON - an export containing data in JSON format as in the system database. Item properties such as strings that are empty or Boolean values that are not set, are not included. The filename format is:

     `export_YYYY-MM-dd_HH_MM_SS.nnnnn.json.zip`
   - Excel - an export containing data and Excel columns for all fields as shown in the JSON export format. The filename format is:

     `<type>_<name>_exportedsheet_CCYY-MM-DD_HH-MM-SS.xlsx`.

     An example would be:

     `data_User_exportedsheet_2015_01_01_12-25-22.xlsx`.
   - Excel(formatted) - an export containing data and Excel columns as arranged by any Field Display Policies that apply. The columns correspond with those of a Bulk Load Template export sheet. This sheet can therefore be used to modify and update data if required. The filename format is:

     `<type>_<name>_exportedsheet_formatted_CCYY-MM-DD_HH-MM-SS.xlsx`.

     An example would be:

     `data_User_exportedsheet_formatted_2015_01_01_12-25-22.xlsx`.
4. If required, the export JSON file can be decompressed, and the JSON file (.json) can be opened in a text editor. The XLSX file can be opened in MS Excel.

Note: The bulk export of Device Model data will export locally *cached* data, not data on the device itself.

21.2.4. Bulk Load Template Export

You can use the MS Excel format spreadsheet bulk load template of a model to easily create a template of a sheet from the user interface. See *Bulk Load Template Sheet Layout*.

The VOSS-4-UC multi-domain core supports the ability to generate a MS Excel format spreadsheet bulk load template for any of the resources in the system directly from the user interface.

You can populate the template sheet with data and then load it using the Bulk Load administration tool.

Excel Bulk Load operations using spreadsheets support multiple (tabbed) worksheets that are loaded in tab sequence. Defined Configuration Templates on the system can be referenced in the sheets and applied during the Bulk Load operation.

The field specific help of the product can be used to assist the user with populating the bulk loaders with the correct data. See *Bulk Load Template Sheet Layout*.

21.2.5. Carry out a Bulk Load Template Export

The button to export a Bulk Load Template of a model is available on any of the following forms: Model design form, Model instance, Model list view.

1. Choose the Hierarchy where the model is available.
2. Choose the required form and click **Action > Export Bulk Load Template** on the button bar to export the bulk load template.

A MS Excel sheet is created that contains the bulk load template for the selected model. The sheet is available in the download directory of the browser application.

Use the bulk load template sheet to enter data.

Use the Bulk Load administration tool to upload the bulk load template sheet.

21.2.6. Bulk Load Sheets

An exported bulk load template is a workbook containing a single sheet and serves as the basis for bulk loading. A workbook can also be created that contains more than one sheet as a tabbed workbook.

For tabbed workbooks, bulk load transactions are carried out from the leftmost sheet or tab to the rightmost. For example, if a site is to be added under a customer, the customer sheet tab should be to the left of the associated site.

The spreadsheet workbook is in Microsoft Excel .xlsx format. Any name can be provided for the workbook and the same filename can be loaded multiple times, although the best practice is to use different names.

To bulk load data, preliminary steps need to be carried out. Verify existing information on the sheet and determine required information in order to complete the required data and prepare the spreadsheet.

21.2.7. Bulk Load Limitations

The VOSS-4-UC automation templates include a rich set of features that incorporate the use of Configuration Templates, customizable Field Display Policies and GUI rules that are used to enhance the user experience of the user interface.

Generated bulk load templates for certain resources that make use of such advanced features are limited in their ability to produce the same provisioning results that can be obtained when using the user interface and as such require additional consideration.

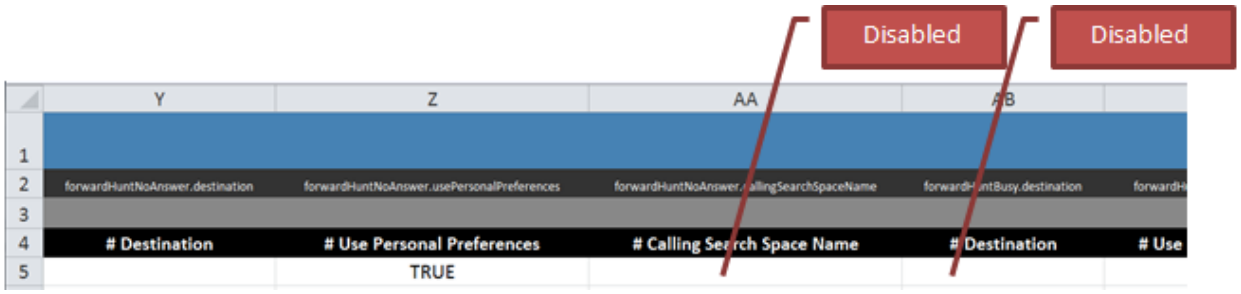
An overview of these limitations is provided below, whilst the implications of these limitations, how they may apply to specific resources in the system as well as how best to use the generated loaders, are documented in the Bulkload Reference Guides under resource specific sheet notes.

- Certain fields are used to link together different resources (for example, the name of the Cisco Unified CM remote destination is linked to the user ID of the user name).

  These fields may not be exposed in the user interface or may, for some resources, be exposed as read-only in the user interface. Such fields are currently exposed as mandatory fields in the generated bulk load templates. The fields and the specific conventions that are used in the template to link the fields together are highlighted in notes specific to the resource. For example, the value for remote destination name should be specified as `RDP-<username>`.

- Certain fields are derived from other data in the system. The notes specific to the resource highlights where to get the possible values for such fields. Examples of this are key-value type fields of a phone's vendor configuration settings.
- GUI Rules defined in the user interface that are not replicated in the backend workflow need to be considered in the loader to get the same provisioning results as the GUI. For example, the GUI rules may:
  - Set a default value for a visible field (fixed value or derived from other data in the system). This column and corresponding value will have to be included in the loader for this to be provisioned.
  - Set a value for a hidden field - This column and corresponding value will have to be included in the loader for this to be provisioned. Note that this means that fields may be included in the loader that would not be visible in the user interface.
  - Make a field visible depending on some condition such as the value of another field (for example, a check box being selected). The column(s) need to be included in the loader and populated under the appropriate conditions.

A GUI Rule may for example disable input fields based on the state of a check box. On the sheet, the ticked check box is represented as TRUE in the column. The columns associated with the disabled fields should not be filled.



To overcome the complexities introduced by the above limitations, a set of sample bulk load sheets have been generated that enable users to get started quickly and to leverage the best practices developed by VOSS.

21.2.8. Sample Bulk Loaders

Sample loaders enable a quick start by providing working examples of the most frequently used loaders. These can be be customized according to user requirements and data.

Furthermore, sample bulk load sheets incorporate best practices for using bulk loaders; ensuring rapid customer and subscriber on-boarding.

Note that the sample loaders are built according to the default Field Display Policies and Configuration Templates that are shipped with the product. Since these are configurable, the use of non-default Field Display Policies or Configuration Templates may result in a change of the sample loaders. For example, if an additional field is exposed by the Field Display Policy, it needs to be added if it is to be managed in the loader.

The latest sample bulk loaders can be obtained from your account team.

21.2.9. Bulk Load Template Sheet Layout

This topic describes a typical generated sheet when using the Export Bulk Load Template menu option.

Colors and styles are applied to the exported sheet:

- dark colors style for header rows
- yellow text for base group titles
- mandatory fields have red title text headers
- optional fields text headers are in white

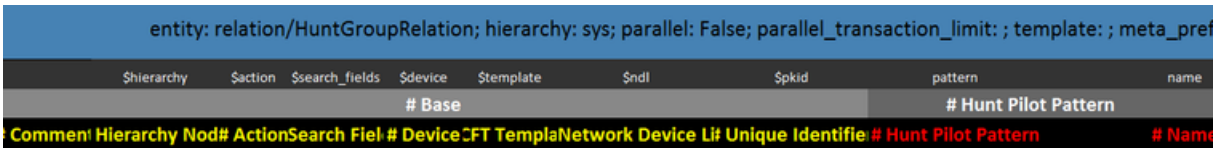
Although an attribute that has nested attributes may be optional, if this attribute has mandatory nested attributes, then the containing attribute becomes mandatory. If a field is mandatory, it is shown on the sheet regardless of any Field Display Policy instruction to hide it.

The Field Display Policy that applies to a menu item from which a Bulk Load Template Export is carried out, is applied to the exported sheet as follows:

- Titles of attributes
- Sequence of the attributes
- Group names
- Hidden fields, with the exception of mandatory fields.

Note:

- Macros can be included in the loader to either be loaded as text or evaluated as part of the load. See documentation in this guide around *evaluate_macros* header for more details on macro behavior in the loaders.
- A single sheet of a file can be used to manage multiple templates by adding additional header rows and data under them. A workbook file can include multiple sheets with single or multiple templates on each.



Refer to the example sheet snippet. A bulk load sheet contains the following information:

Sheet name (tab on spreadsheet workbook)

Any name can be provided on the tab or sheet If the name is prefixed with a # on the tab, the sheet is ignored during loading.

Row 1 - Resource and instructions

The exported bulk loader template will have the resource as target entity (model) as well as the hierarchy shown on the top row of the sheet. Verify the entity in the first row of an exported sheet. The reference data in the first row is of the format shown below, with variable values indicated in {}:

```
entity: {entity name}; \
hierarchy: {hierarchy}; \
parallel: {True | False}; \
parallel_transaction_limit: {n}; \
template: {config_template}; \
meta_prefix: {c}; \
evaluate_macros: {True | False}
```

- *entity*: *{entity name}*: the name of the model, in the format *{modeltype}/{model name}*, for example `data/User`
- *{hierarchy}*: the hierarchy, in the format *{level1}.{level2}.{level3}*, where *{level1}* is the first system level. Verify the hierarchy at which the bulk load should take place.
- *parallel*: True or False. By default, the value is False and rows are processed sequentially. If multiple templates are entered on a single sheet, they should all *only have a single value*: True or False.

  Sheet rows can be processed in parallel. The sheet should then not contain multiple, sequence dependent models. If there are a large number of rows for complex models on the sheet, the duration of a bulk load transaction is significantly reduced by parallel processing.

  By default, 14 rows are processed in parallel, since bulk loads are low priority transactions that are limited to 50% of the maximum allowed parent transactions, which is by default set to be 30 per unified node. The default value supposes that one slot is used by the parent bulk load transaction itself.

  The maximum allowed parent transaction limit can be modified from the Command Line Interface (CLI) using the command: **voss workers <number>**.
- *parallel_transaction_limit*: the maximum number of rows that can be processed in parallel by the bulk load at any given time. The minimum value that can be set is 1 and the maximum is 100.
- *template*: The Configuration Template *{config_template}* that is associated with the user's menu item for the *{entity_name}* from which the export was carried out. The exported sheet will show a row of values from the Configuration Template.

  When a sheet is created to bulk load, the Configuration Template should be available on the target system and it will only apply to rows on the sheet that has **add** specified in the `# Action` column.

  Note: this header item is not used when Configuration Templates are loaded.
- *meta_prefix*: By default, the value is $. The # character cannot be used, as it is used for comments. The character is prefixed to the `# Base` group of columns in Row 2.

  The purpose of the prefix is to distinguish a special set of base columns from the entity attributes on bulk load sheets.

  Note that the bulk load sheets will fail to load if the # character is is used as prefix. An error message will be shown in the transaction log.
- *evaluate_macros*: By default, the value is `False`. When set to `True`, named macros can be added as values to be evaluated before the sheet is loaded. Otherwise, the value is a string.

  The format of the macro is *{{ fn.bulkload_evaluate macro.NamedMacro }}*, where *NamedMacro* is the name of an existing `data/Macro` instance. The function prefix `fn.bulkload_evaluate` is required in the value for the macro to be evaluated.

  - For examples, see *Bulk Load Sheet Macro Evaluation*.

Note: `fn.bulkload_evaluate` is not available via the Macro Evaluator. For testing purpose using the Macro Evaluator, please use the `fn.evaluate` function prefix.

Base columns (grouped by `# Base` in Row 3)

The list below describes the column values with the default value of `meta_prefix`, in other words, column names by default prefixed by `$`.

The purpose of the columns is to provide more detailed instructions or overriding data for a row.

- Comments: Any row that contains a # character in column A is considered a comment row and will be ignored. Empty rows are also ignored. Column A - the first column - is also a `# Comment` column, so that any value entered in it is considered a comment. If all rows on a tab are commented, but the tab name itself is not commented, the tab sheet load will fail.
- `$hierarchy`: A hierarchy column with the name `# Hierarchy Node` is also available so that individual rows of a sheet can be loaded to a specified hierarchy. If a hierarchy is specified in this column for the row, it takes precedence over the hierarchy in the first row. The format for the hierarchy in the row is the same as for the first row: the full hierarchy, with levels separated by dots.
- `$action`: Any row that contains an action in the `# Action` column : **add**, **delete**, **modify**, **execute** or a custom action name, will have the action carried out. The action values in the column are case insensitive.

  If no action is entered, the **add** action is carried out. The list below shows the functionality for the values entered in the row. Also refer to the Search Fields entry below.

  - **add** or empty - the data in the attribute columns is added. Any values in the `# Search Fields` column are ignored.
  - **delete** - the row matching the unique criteria in the `# Search Fields` column is deleted.
  - **modify** - the row matching the unique criteria in the `# Search Fields` column is updated with values in the attribute columns. Refer to the Search Fields entry below.
  - **execute** - if the action is available for the model, the row matching the unique criteria in the `# Search Fields` column is executed, using any values entered in attribute columns.
  - custom action name - if the custom action is defined for the model, it is carried out for the row matching the unique criteria in the `# Search Fields` column.
- `$search_fields`: The column applies to rows where the action is not **add** and consists of a colon-separated list of attribute names and values, for example, `fullname:'John Smith', username:jsmith`.

  Note however that the `pkid` field takes precedence over search fields criteria.

  - **delete** - the search fields and corresponding attribute values uniquely identify the model instance to delete.
  - **modify** - the search fields and corresponding attribute values uniquely identify the model instance to modify, with the values to modify in the attribute columns.
  - **execute** - the search fields and corresponding attribute values uniquely identify the model instance to execute.

  Where the sheet is for a Relation model, only the left model attributes in the Relation can be in the Search Fields column. This is the standard search behavior for Relations.

- `$device`: The column is used when a sheet includes attribute columns that belong to a device model. This column then contains the comma-separated list of business keys of the device model, as well as its hierarchy. These values narrow the search for the device to which the data in the sheet applies. Examples of such sheets would contain device models or relations that have device model attributes in the left hand association of the relation.

  The format of the values in this column is:

  `<business_key1>,<business_key2>,...,<business_keyn>,<device_hierarchy>.`

  For example, if a Unified CM instance in a model `data/CallManager` has `host` and `port` as business keys, the value would for example be: `10.120.2.175,8443,sys.Varidion.InGen.Tokyo`.

- `$template` (Configuration Template): If a row that contains a Configuration Template name that applies to the model, this template is applied to the row when it is loaded. Upon bulk loading, values in this column will override any value for `template` in the sheet header.
- `$ndl` (Network Device List): The column is used when a sheet includes attribute columns that belong to a device model. This column then contains the name of the Network Device List that includes the required device in the list of devices. If the Device column is also filled in, then the value in the Network Device List column overrides it.
- `$pkid` (Unique Identifier): On modify, delete, execute, and custom action operations, this `pkid` is used to identify the resource represented in the row data. The `pkid` field takes precedence over the search fields criteria when locating a resource. The pkid is unique to the resource on the particular database and cannot be relied upon when attempting to manipulate an identical resource on a different database.

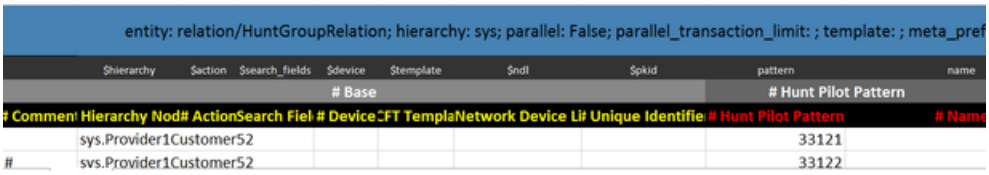
Row 2 - Column names

- base column names (prefixed by the `meta_prefix` character and listed above)
- attribute names. Entity attribute names show as column header data in the spreadsheet.

Columns can be in any order in a row. Nested object attribute names follow a dot notation.

Array objects will be sorted, so that attributes with names such as `filter_fields.<number>.xx` will be in sequence: `filter_fields.0.xx`, `filter_fields.2.xx`, and so on - before further ordering (represented by `.xx` here) is applied.

- If a column header starts with a #, the column will not be loaded.
- If a column header is blank, this indicates the end of the sheet header. Subsequent columns will not be loaded.



Row 3 - Group or description

The row provides a description of a column or columns (as for example `# Base` for the sheet base columns), or else the group name of attributes that are grouped on the GUI as tabs on the detail or input GUI form.

A group is specified in the row by merging the group name across all the columns of the group. For attributes that are required and are not grouped in the GUI (or may be hidden in the GUI), the group name: Not Grouped Fields is given on the sheet.

"Default" values of attributes in this group need to be removed from an exported sheet before the sheet is used to bulk load rows.

Row 4 - Title

Title of:

- the reference for base column names (hierarchy, action and so on)
- the column attribute as on the GUI. This title may be modified by a Field Display Policy.

Data rows

The exported template contains no data.

Important: As a part of bulk loader sheet design, attention should be paid to the API payload posted to the system. The data entered in the loader sheet columns should correspond with the API payload.

GUI drop down lists may contain user-friendly titles, while the actual value sent to the API may differ.

21.2.10. Export Data Sheet Layout

This topic describes an exported sheet, either formatted or not formatted.

For both exported sheet formats, the header and column layout shows correspondences with the Bulk Load Template sheet.

The following items apply to sheets containing data exports:

- The `# Comment` column shows the text "Exported data" in green for each row of data.
- The `# Hierarchy Node` column shows the source hierarchy of the exported row. The `hierarchy:` value in the sheet header shows the hierarchy from which the data export was run.
- If device instances were exported, the `# Device` columns shows the business key of the device (for example, comma-separated: host, port, hierarchy).
- If a Configuration Template was applied during the export - for example if it applied to the GUI form - `# CFT Template` column will show this name for each row, as well as the `template` value in the sheet header. If a sheet is used for loading, the row value overrides the sheet header value.
- The `# Unique Identifier` contains the `pkid` that is used to identify the exported resource represented in the row data. On modify, delete, execute, and custom action operations, this `pkid` is used to identify the resource instance on the database represented in the row data.

  The `pkid` field:

  - takes precedence over the search fields criteria when locating a resource
  - is unique to the resource on the particular database and cannot be relied upon when attempting to manipulate an identical resource on a different database
- For a formatted Excel export, the columns in the sheet correspond with an exported Bulk Load Template sheet.

- For a non-formatted Excel exported sheet, the columns correspond with the properties of an exported JSON file. For example, only properties where strings are not empty and boolean values are set, are exported.
- A formatted, exported sheet of data can be used just as a Bulk Load Template sheet to bulk load data. For other Actions, the `# Search Fields` column needs to be completed. Refer to *Bulk Load Template Sheet Layout*.
- "Default" values of attributes in any Not Grouped Fields group need to be removed from a sheet before it is used to bulk load rows.
- The rows and data in the columns of an exported sheet are bound by the limitations of the MS Excel format. For example, model data with property values longer than 32,767 characters (maximum length of MS Excel cell contents) will be truncated in the exported sheet.

21.2.11. Bulk Loading a File

Completed Bulk Load XLS sheets can be loaded immediately. Verify the following:

- Ensure that:
  - The file has a valid file extension `.xlsx`. An error message will display on the user interface to indicate that the file does not have a valid file extension.
  - Any Configuration Templates that are referenced, are available.
  - Any comments that your spreadsheet application allows you to add (for example showing as a marker in the cell with a pop-up) have been removed. Otherwise, an error message is shown: "An error occurred while opening the workbook. For possible resolution, please remove all comments from the worksheets and try again. If the problem persists, contact your administrator for support."
- To send empty values for a files, type a space in the cell of the value column on the sheet.
- Spreadsheet formulas (such as `'=7+2'`) in data will not be evaluated.

1. Browse to the hierarchy level at which you want to perform the bulk load.
2. Choose **Administration Tools > Bulk Load**. The **Bulk Load**** form is displayed.
3. Click **Browse** to open the file upload dialog.
4. Click **Bulk Load File** on the button bar to carry out the bulk load.
5. Choose **Administration Tools > Transaction** to inspect the bulk load in the transaction log if necessary. The **Execute Bulk Load** sub-transaction list shows the transaction for each row of the sheet.
6. Alternatively, to schedule the bulk load, clear the **Execute Immediately** check box and add scheduled date and time values in the mandatory **Execution Date**, **Execution Time** and **Execution Timezone** fields. A scheduled bulk load is shown on the list view of the Schedule and has the name and upload load date of the sheet.

21.2.12. Bulk Load Sheet Macro Evaluation

Bulk load sheets can be configured to allow for macro evaluation.

The first row of a bulk load sheet has a variable to enable or disable macro evaluation (see *Bulk Load Template Sheet Layout*):

```
evaluate_macros: {True | False}
```

- If the variable is set to `True`, macros in a sheet will be evaluated upon loading. In this case, it is important that:
  1. The macro be prefixed with `fn.bulkload_evaluate`.
  2. A named macro must be used, in other words, a `data/Macros` instance.

For example:

1. If the sheet is used to update a site at its hierarchy, and the `evaluate_macros:` value is set to `True` in the first row, then:
   - The macro `{{ fn.bulkload_evaluate macro.SITENAME }}` will be evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - The macro `{{ fn.evaluate macro.SITENAME }}` will be *not* evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - The macro `{{ macro.SITENAME }}` will be *not* evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - The macro `{{ input.sitename }}` will be *not* evaluated to the site name when the sheet is loaded, but inserted as plain text.
   - Rows containing entries with a *combination* of the type `{{fn.bulkload_evaluate <named macro> }}` and other types macros will *only evaluate* the former type and load others as plain text.
2. If the sheet is used to update a site at its hierarchy, and the `evaluate_macros:` value is set to `False` in the first row, then *all* macros entered will be inserted as plain text.

Note: If the named macro needs to be tested with the macro evaluator, the format is {{ fn.evaluate macro.SITENAME }}.

- See the topic *Macros in VOSS-4-UC* in the Core Guide for more named macro examples.
- For further details, also refer to the Advanced Configuration Guide and Named Macro Reference.

21.2.13. Bulk Load Transactions

The transaction log is available on the user interface after a bulk load transaction has been run. Refer to the topics on transactions and viewing transactions in the Core Feature Guide.

Choose **Administration Tools > Transaction**. Bulk load transactions show in the log:

- In the list view, the bulk load is shown in the Action column of the log. If the bulk load was scheduled, this is shown as a schedule with the detail column indicating it to be a bulk load. The Action column will show “Execute Bulk Load” or “Execute Schedule” respectively.
- The submitted, start and stop time for the entire bulk load transaction is also shown.
- The Detail section will hold the name of the file that is bulk loaded as well as the workbook sheet number and the number of successful rows out of the total, for example:

```
[ 8/9 ] succeeded from [ 1 ] sheet in data_Users_bulkloadsheet.xlsx.
```

Checks are made to validate the user's access profile, the provided hierarchy information and data constraints for the bulk load transaction when updating the target models. The parent bulk load transaction will show the error message if this validation fails and no rows will be loaded.

Where rows are loaded, each row in the bulk load sheet appears as a sub-transaction within the bulk load transaction. The Message box shows the number of successful and failed rows loaded.

For each loaded sheet, bulk load transactions are run in series for each row. Multiple bulk load sheets can be loaded and these transactions will load in parallel.

Sheet rows can be processed in parallel. The sheet should then not contain multiple, sequence dependent models. Refer to *Bulk Load Template Sheet Layout*.

For each row of the bulk load sheet carrying out the default add action, a Create action is shown on the list of transactions. Sheet rows that led to a successful Create action have a Success status, while rows that failed show a Fail status. If a row fails, the load process continues. For failed actions, the transaction can be selected to show the error message.

If one or more rows of the sheet failed to load, the Bulk Load Sub Transaction shows a Success status, while the Log list will show "error" for failed rows.

On the list of sub transactions, choose the transaction **Link** hyper-link to inspect the details of each sub transaction. For example, the submitted, start, and stop time for the bulk load sub transaction corresponding with a row on the bulk load sheet is shown. In the case of a failed sub transaction, further information about the failure - such as the error message and row data - is shown in the sub transaction Link.

A canceled bulk load transaction means the Processing worksheet sub transaction, as well as all sub transactions within the worksheet transaction in a Processing or Queued state, will fail.

For parallel transactions, multiple resource transactions may be in a Queued or Processing state. By default, 14 rows are processed in parallel. Refer to *Bulk Load Template Sheet Layout* for more details. If a worksheet transaction fails as a result of bulk load transaction cancellation, subsequent worksheet tabs in the bulk load workbook will not be processed by the bulk loader.

21.3. Alerts

21.3.1. Alerts

An Alert list can be exposed on the GUI by adding the `data/Alert` model to the administrator menu. This will enable an administrator to inspect the list of alert messages.

The Alert list is summarized by:

- ID: A reference to the source of the alert. Alerts with the same ID and code will update the count of this alert as well as the last time that the alert occurred. This means that a single alert is shown on the list for each alert with the same ID and code.
- alert code: an error or warning code associated with the alert
- alert category: A specific category to which the alert belongs, for example: "Device Change Notification Collector".

Administrators can also filter alerts by any of these fields.

When features are enabled to send alert messages, these are recorded in the list. Each alert also has such properties as a severity (Error, Warning or Info), the number of times that the same alert has been raised and the time stamp of the last alert instance. See: Field Reference for `data/Alert`.

When an alert is raised, the Notifications indicator on the main user interface will show this. Clicking the **Notifications** button will show a message in red that alerts have been raised: “There are one or more alerts. Click here to view them.” When clicking on this message, the user is directed to the list of alert messages.

Alert messages can be inspected and then acted upon by the administrator. If an issue that raised the alert has been resolved, the administrator can delete the alert from the list. If no alerts are present in the list, no notification is shown.

21.3.2. Field Reference for data/Alert

- The field Title is indicated in bold. An asterisk * indicates the field is mandatory.
- If the field Type is an array, its the Field Name has a .[n] suffix, where n is the array index placeholder.
- Object and array names are listed to provide the context of fields.
- If a field belongs to an object or an array, the full name is in dot separated notation.
- Where cardinality is shown, the range is [MinItems..MaxItems].
- If a field has a Default value, the value is shown.
- If a field has a Pattern, the regular expression pattern is shown.

ID *	
Field Name	alert_id
Description	The unique ID of the alert
Type	String
Code *	
Field Name	alert_code
Description	The code of the alert
Type	String
Category *	
Field Name	alert_category
Description	The category of the alert
Type	String
Severity	
Field Name	alert_severity
Description	The severity of the alert
Type	String
Choices	[“Error”, “Warning”, “Info”]
Message	
Field Name	alert_message
Description	The message describing the alert
Type	String
Count	
Field Name	alert_count
Description	The number of times this alert has occurred
Type	Integer
Latest Alert	
Field Name	alert_timestamp
Description	The last time this alert occurred
Type	String
Format	date-time

21.3.3. Database Maintenance Alerts

If database maintenance schedules have not been set up from the Command Line Interface (CLI), alerts are shown *at the provider level hierarchy* for each required schedule.

The schedules are required to periodically:

- Archive or delete database transaction logs (CLI: **voss transaction archive** or **voss transaction delete**)

Refer to the Platform Guide topic “Enable Database Scheduling ” for details.

The format of the alert is:

- ID: A generated identifier:
  - `TRANSACTION_DATABASE-<hostname>`

Note: The `<hostname>` will be a primary unified node. These are where alerts are generated.

- Code: An error or warning code associated with the alert. (`-1`)
- Alert category: `Database Maintenance`
- Severity: `Warning`
- Message:
  - `TRANSACTION DATABASE MAINTENANCE NOT SCHEDULED`
- Count: Displays the number of times the alert has occurred.
- Latest Alert: Displays the last time this alert occurred.

21.4. Transactions

21.4.1. Transaction Logging and Audit

Activity on the VOSS-4-UC system results in transactions that are recorded. The Transaction menu provides auditing information for each transaction.

The recorded information includes:

- Transaction ID - identifier of the transaction.
- Detail - A brief description of the processed transaction.
- Username - Of the user who initiated the transaction.
- Action - The type of action recorded in the transaction, for instance Execute, Create, Modify, Data Import and so on.
- Status - for running transactions, this is In Progress; for completed transactions it is Fail or Success.
- Submitter Host Name - The host name of the application node that scheduled the transaction. On a clustered system, this can differ from the Processor Host Name.
- Processor Host Name - The host name of the application node that processed the transaction (this value will only be set once the transaction is processed). On a clustered system, this can differ from the Submitter Host Name.
- Rolled Back - Indicates whether the transaction was rolled back or not.
- Priority - The priority of the transaction, for example Normal.
- Submitted Time, Started Time and Completed Time - The date and time of the progress of the transaction.
- Duration - The duration of the selected transaction. If there are sub-transactions, this parent transaction duration is the total duration of the transaction. This includes the total duration of import transactions that carry out provisioning workflows asynchronously.

On the GUI, details of a specific transaction are displayed when the transaction is selected from the list view. Refer to *Bulk Load Transactions*.

When a transaction is selected, the **Base** tab shows details of the columns of the transaction list view. The button bar on the detail list view shows **Help** and **Refresh** buttons if the transaction is still running. If the transaction is running, click the **Refresh** button to update the Progress field.

Lists of transactions can also be filtered. Refer to *Filtering Lists* for details.

If you want to cancel a transaction while it is still running, click the **Cancel** button. If a transaction, with sub-transactions, is canceled, the sub-transaction currently in progress will complete. This sub-transaction as well as all preceding sub-transactions will then roll back to their previous states. Note that bulk load transactions do not follow this behavior. Each bulk load sub-transaction is seen as a main transaction, and only the 'in progress' sub-transaction will roll back to its previous state.

A **Replay** button is available if the transaction is complete. A transaction can be replayed if required, for example if a transaction failed because a target system service was not running. The replay of the transaction can then be used instead of re-entering data on a GUI form.

An **Edit and Replay** button is also available for completed transactions. This is similar to the **Replay** button, but allows you to first make changes to the previously submitted form before the transaction is resubmitted.

The button is available for transactions that did not originate from bulk loads, wizards or pop-up forms.

Replay and Edit and Replay functionality are not supported by the bulk loader, because the bulk load files are not stored by default. The bulk loader extracts data from the spreadsheets and then performs the necessary action(s). The only time a bulk load file is stored in the database is when the bulk load is scheduled. In this case, the bulk loader keeps the file until it is triggered by the scheduler to execute the actions in the file. When the data is extracted from the file, it is deleted.

When using Edit and Replay for a failed Quick Add Subscriber transaction, the user information fields will not automatically update when changing the Username field:

- Entitlement Profile
- Firstname
- LastName
- Email
- Jabber Device

These need to be edited manually.

Selecting the button opens the original input form that resulted in the transaction. The form also contains the original data that was posted. This data can be edited and the form can be submitted to replay the transaction. This functionality can therefore be used to for example edit a failed transaction or to modify data of a successful transaction.

Since GUI Rules apply to a form from a specific hierarchy, the Edit and Replay functionality should only be used from the same hierarchy as the original transaction was executed.

If a transaction has sub-transactions, a sub-transaction list is available on the form, with links to their details. The sub-transaction form displays a link to a parent transaction. On the transaction list view, sub-transactions are identified by a ≡ preceding the Id number.

Failed transactions show a Message of the error. However, a sub-transaction with a Create action that has a "fail on error" workflow condition for *duplicates*, may show its Status as Fail when not creating a duplicate, while the parent transaction then shows its Status as Success.

For asynchronous transactions and sub-transactions, refer to Parent and Sub-transactions for Asynchronous Transactions.

The Log section on the Transaction base tab displays Message and Severity details of transactions performed by VOSS-4-UC. For example, if the Severity has the status of error, the Message section can be expanded to inspect the error, and optionally copy it send it to Support. If a workflow is inspected, a separate log entry provides details of each step with a log message as *Step n*, starting with Step 0. For more details, refer to *Transaction Log Example*.

The **Resource** tab, which has content for transaction types where a resource changed, displays the additional information, depending on the transaction type:

- Hierarchy - The point in the hierarchy at which the transaction occurred.
- Model Type - For example data/User.
- Current State - if available, click the Entity link to inspect the instance on the GUI form.

The **Back** button on the button bar can be used to navigate to the previous screen, for example from the parent transaction screen to the list view of all transactions.

21.4.2. Parent and Sub-transactions for Asynchronous Transactions

Parent and sub-transactions for asynchronous transactions are shown in the transaction logs as follows:

- Parent transactions are in a “Processing” state until the last asynchronous child transaction completes (with either “Success”, “Success With Async Failures”, or “Fail”). These include:
  - Asynchronous workflows triggered by Device Import
  - Asynchronous operations triggered by Bulk Load (with parallel = true)
  - Asynchronous workflow steps
- Asynchronous transactions for non-bulk operations are not grouped under the parent transactions. These include:
  - Asynchronous device import triggered by DataSync execute
  - Asynchronous event execute triggered by another operation
- The status of top level transactions with failed asynchronous at any level of sub-transactions is “Success With Async Failures”. The detail view of the top-level transaction also shows the list of failed async transactions below the list of sub-transactions. This list allows for easy access to all failed async transactions. The Detail column of the sub-transactions also show the number of failed async transactions.
- The details of parent transactions with the status “Success” also show the number of failed sub-transactions for the following:
  - Device Import
  - Workflows

21.4.3. View a Transaction

You can only view transactions that are relevant to your specific hierarchy level. For instance, if you are logged into the system as a Customer Administrator you will be able to view all transactions that were performed at the customer for which you are the administrator. This includes transactions that were performed at any of the sites that belong to the customer. If you are logged in as a Site Administrator you will be able to view only the transactions that were performed at your specific site. Refer to the topic on Data Partitioning in the

Core Feature Guide and to the API Guide to view transactions by means of the API. The steps below can be followed on the GUI.

1. Choose **Administration Tools > Transaction**.

   By default, the **Transaction** list view shows all parent transactions in progress or executed. This is indicated in the **Status** column of the list. Parent transactions are identified by a − preceding the Id number.

   If you also want to see the child transactions (sub-transactions) in the list view, click the **Filter** button, select the **Include Sub-transactions** check box and click **Search**. The list view refreshes and shows both parent and sub-transactions.

   Sub-transactions are identified by a ≡ preceding the Id number.

   For completed transactions, the **Status** column displays either **Success**, **Success With Async Failures**, or **Fail**. Failed transactions are highlighted in red by default, but this can be overridden in the Theme if required. An exclamation icon is also displayed next to the word **Fail**.

   The **Detail** column provides additional details on the transaction if available. See “Transaction Details” for more information.

2. Click an individual transaction or sub-transaction (if required) to show a detailed view. If the **Include Sub-transactions** check box is not selected, you can view details of the sub-transaction by clicking on the relevant parent transaction, and then clicking the required Link in the **Sub Transactions** area of the detailed **Transaction** view.

   If the top-level transaction has the status **Success With Async Failures**, the list of failed async transactions show below the list of sub-transactions. The failed async transactions can be at any level below the top-level transaction. Click on the Link in the **Transaction** column to see the details of the failed async transaction. The **Detail** column of the sub-transactions also show the number of failed async transactions.

21.4.4. Transaction Details

This Detail column of the list of transactions in the transaction log user interface shows information according to the type of entity and the operation carried out by the transaction.

The rules listed below should be considered when creating a transaction filter and specifying the value of the filter text.

The following conditions apply to content in the Detail column:

Action	Entity	Comment
Create, Update, Clone and Delete	all models	Detail will only contain the name on the model
Execute	DataSync, Workflow, Event, Scheduler	Detail will contain the instance name
Bulk operations on Modify, Delete, Move	all models	• The parent transaction detail contains: "[no. of succeeded / no. of total] were [updated / deleted / moved to destination_hierarchy] successfully." • Bulk move from different hierarchies to one hierarchy show the destination hierarchy name in the parent transaction detail. • Each child transaction detail will contain the name of instance that is deleted.
Data Import	all models	Detail shows only the imported file name.
Device Import	all devices	Detail shows host name or device address
All operations	all models	The following attribute values are considered first for inclusion in the Detail column: `country_name`, `DialPlanName`, `name`, `ip`, `host`, `address`, `description`, `username`, `type`, `entity_id`, `userid`, `pattern`, `RoleCurrent`. Otherwise, the Detail column will be empty.

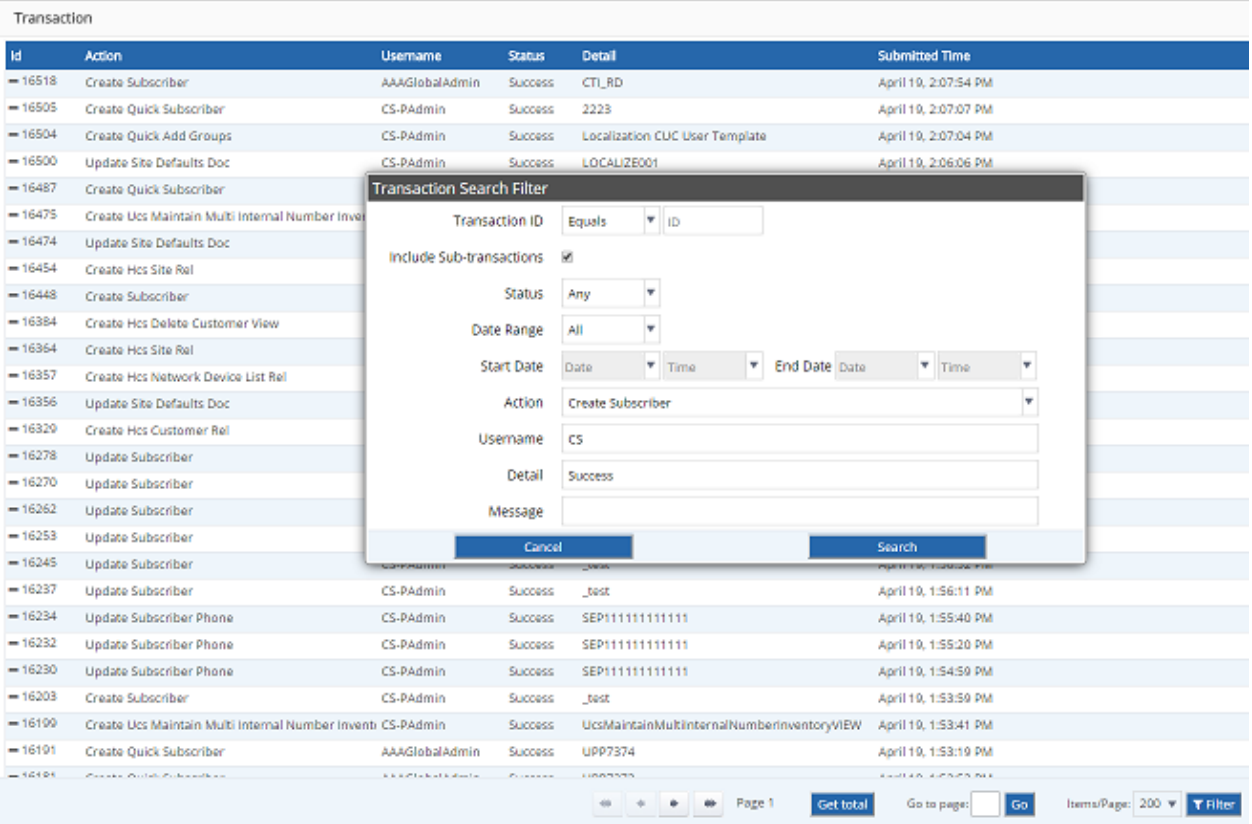
Note that the contents of the Detail column of transaction lists are not localized.

21.4.5. Filtering Transactions

Choose **Administration Menu > Transaction** to open the list of parent (−) transactions. When a parent transaction is selected and opened from the list view, its details and sub-transactions are shown.

To open the **Transaction Search Filter** pop-up, use either:

1. the **Filter** button at the bottom of the list
2. one of the filter icons in a column header of the list



A transaction filter is a logical AND operation over a number of active search criteria related to column values that are entered in the **Transaction Search Filter** pop-up form:

- **Transaction ID**:
  - Equal: Default setting. The search only matches on the entered transaction or sub-transaction ID value.
  - If a value is entered, all other criteria are disabled.
  - If no value is entered, any transaction ID is matched according the other criteria.
  - Range: Start and End ID input boxes are available to specify the search ID range.
- **Include Sub-transactions**:
  - Criteria in the search filter also apply to sub-transactions. Only one level of sub-transactions are filtered, in other words, if sub-sub-transactions are for example present, these are not included.
  - The search result list view shows both parent (−) and sub-transactions (☰).
  - By default, sub-transactions of a parent are listed *above* the parent in the search result list view, latest date at the top.
- **Status**:
  - A drop-down is available to select the transaction status
- **Date Range**: a drop-down is available so that the last day, week or month can be selected quickly.

  Note that if a date range: Last Day, Last Week or Last Month is selected, the subsequent re-opening of this filter will show it as a *Custom* date range, since the range is then less than the selected interval.

  All and Custom date options will enable **Start Date** and **End Date** controls.

- **Start Date** and **End Date** and **Time**: specify a transaction date and time range in the format of the system locale. For example, for language code `en-us`, the typed format is `mm/dd/yyyy`. The number format “9” instead of “09” is also valid.

  Date picker widgets and time drop-downs can be used to specify the range, but values can also be typed in. While time drop-down values only show 15 minute intervals, any valid minute value can be typed in. The widget values also follow the system locale format.

  - If a Username, Detail or Message filter is added, a warning about possible slow filtering will show if the transaction date range is more than 7 days.
  - By default, all transaction dates are searched, but if used, *both* Start Date and End Date values are required.
- **Action**: a drop-down to select a value from the **Action** column.
  - The drop-down options are filtered while text is entered.
  - If text is entered that does not match any action exactly, all actions containing the text (case-insensitive), will be listed.
  - If the transaction date range is more than 7 days, a warning about possible slow filtering will show.
- **Username**: filter on the **Username** column text.
  - The column should contain the entered text, case-insensitive.
  - If the transaction date range is more than 7 days, a warning about possible slow filtering will show.
- **Detail**: filter on the **Detail** column text.
  - The column should contain the entered text, case-insensitive.
  - If the transaction date range is more than 7 days, a warning about possible slow filtering will show.
- **Message**: filter on the transaction message
  - The message contains the entered text, case-insensitive
  - If the transaction date range is more than 7 days, a warning about possible slow filtering will show.
  - For *failed transactions*, hover over the **Status** column to see the message or inspect it in the detail view.
  - Some *successful transactions* also show messages when viewing its details, for example data import and bulk load.

Since transaction filters can take a long time, a filter timeout is added to limit the filter duration to 2 minutes.

Active transaction, sub-transaction and transaction log filters are displayed:

- at the bottom of the list view, as an **X** button next to the active Filter funnel icon. Select this **X** button to cancel a running filter. If the filter is a modification of a previous successful filter, the running filter will be reverted to the successful filter.
- in the columns headers that have been filtered, as highlighted funnel icons on the right hand side of the column header.

21.4.6. Filtering Sub-Transactions and Logs

Some transactions have sub-transactions as well as a log list on the transaction detail view. The filtering of sub-transactions and logs works like the list view filter, in other words, a range of matching operators are available.

If a sub-transaction has further sub-transactions, click the Link in its Transaction column to carry out any filtering on nested sub-transactions. To navigate up the sub-transaction hierarchy, click the parent Link.

The sub-transactions and log columns to filter by, are:

- Sub-Transactions:
  - Action
  - Status
  - Detail
- Logs:
  - Severity
  - Message
  - Duration (some logs - only equals and not equals)

For details on matching operators when filtering sub-transactions and logs, refer to Filtering Lists.

21.4.7. Transaction Behavior

The VOSS-4-UC transaction engine ensures that configuration changes are made efficiently and reliably.

In the event of a transaction failure or error, VOSS-4-UC allows for transactions to be rolled back to a state preceding the failed transaction.

For example, where a workflow step fails, all successful steps prior to a failed step are rolled back.

Transactions are hierarchical and have parent-child relationships with other transactions. Sub-transactions are always executed sequentially and synchronously, in other words the child transactions of a workflow parent transaction are executed one after another.

Transaction behavior is different for the following actions in the system:

- API

  The API supports executing transactions in both synchronous and asynchronous modes. When executed in synchronous mode the API responds only once the transaction has completed. When executed asynchronously, the API responds immediately with a transaction ID so that the progress and status of the transaction can be polled.

- Bulk Loaders

  With bulk loading, the load of each row on a sheet is a separate transaction. These transactions are run in series. There is no rollback of rows that have loaded successfully prior to, or subsequent to, a failed transaction (a failed row on a sheet). Multiple bulk load sheets can be loaded in parallel.

- Data Import

  A single transaction is created for each record in the import file. If a single transaction fails, the import continues and does not roll back the preceding successful transactions.

- Data Sync

  A single parent transaction is created for a data sync action. The subsequent device API requests are not handled as sub transactions but are executed in-line.

- Events

Events can be triggered as part of data sync operations or as triggers on operations performed on certain model types. The provisioning workflow executed when the event triggers is executed as a new parent transaction. Transaction failures with the workflow executed after an event do not affect the original transaction that triggered the event.

All transactions are placed on a queue before they are actioned. Parent transactions can run concurrently, but their subtransactions run serially. There is priority in parent transactions so that user input such as adding on a GUI form will be prioritized over a running import or bulk load process.

21.4.8. Transaction Priority

Transactions can currently have two levels of priority: normal and low.

Normal priority transactions will be processed ahead of any low priority task in the queue.

Low priority transactions have a time limit associated with them. This means that if a low priority transaction is in the queue for more than a day, it will be processed as a normal priority transaction.

The following transactions have a low priority:

- Data sync
- Bulk load
- Data import (JSON import)

Any sub-transaction of these transactions also have a low priority.

21.4.9. Transaction Log Example

This section aims to examine the transactions, sub-transactions and logs that are displayed when an example wizard is executed.

The aim of the wizard is to to provide the user with a series of steps to allow input and choices. When the wizard is executed, a Workflow is run and this is displayed as an Action on the Transaction list.

The workflow executes tasks to:

- Add a hierarchy.
- Add devices at the created hierarchy if selected.
- Add a user to the system and if selected, add a user to devices and also LDAP and SSO users if selected.

After the wizard is run, the sub-transactions show the actions of the workflow. In the example, only the Unified CM is selected. The first action in the wizard is to execute a workflow, that results in three sub-transactions. The first sub-transaction is itself a workflow that carries out three actions:

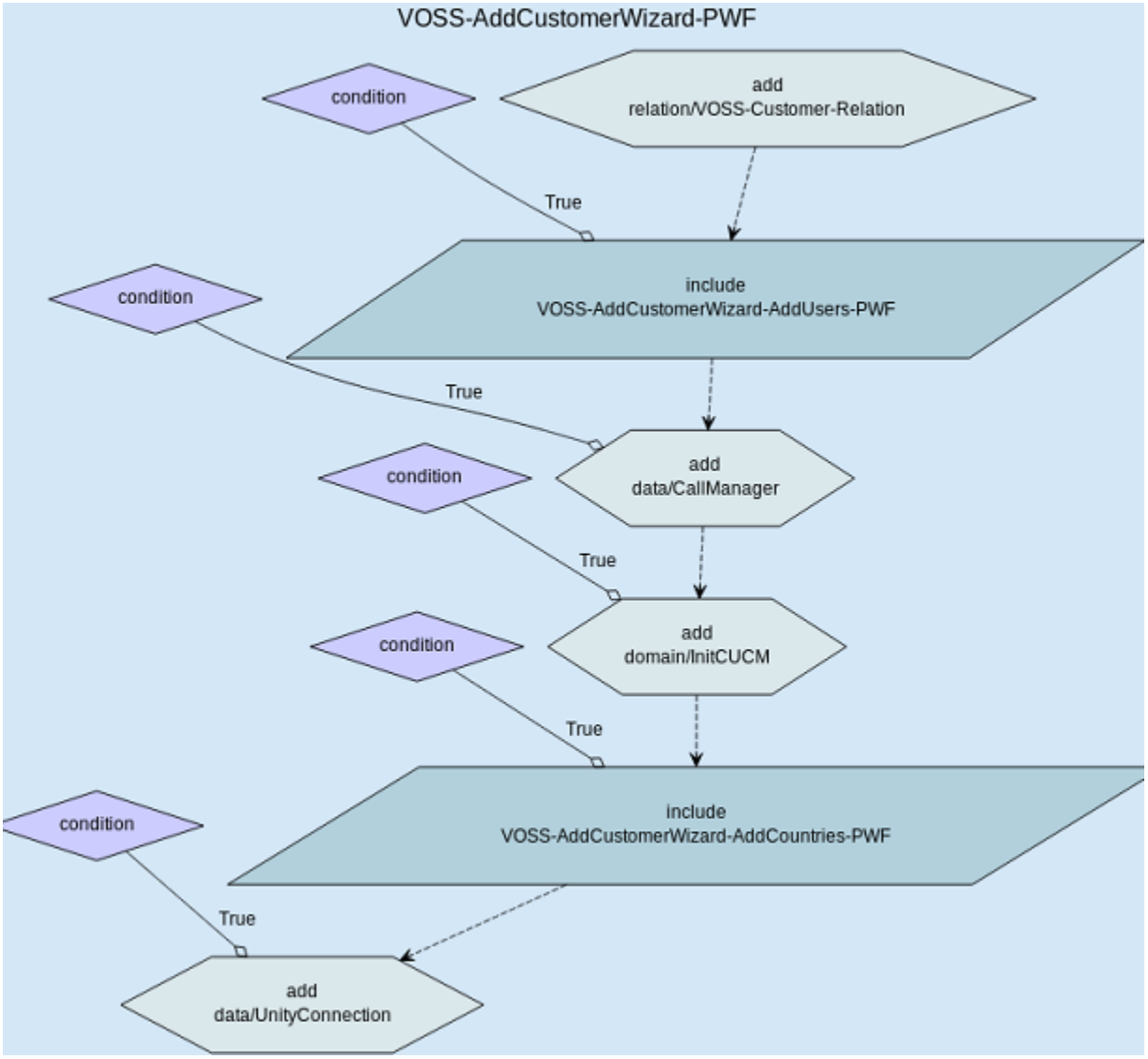
Execute : VOSS-AddCustomerWizard-PWF

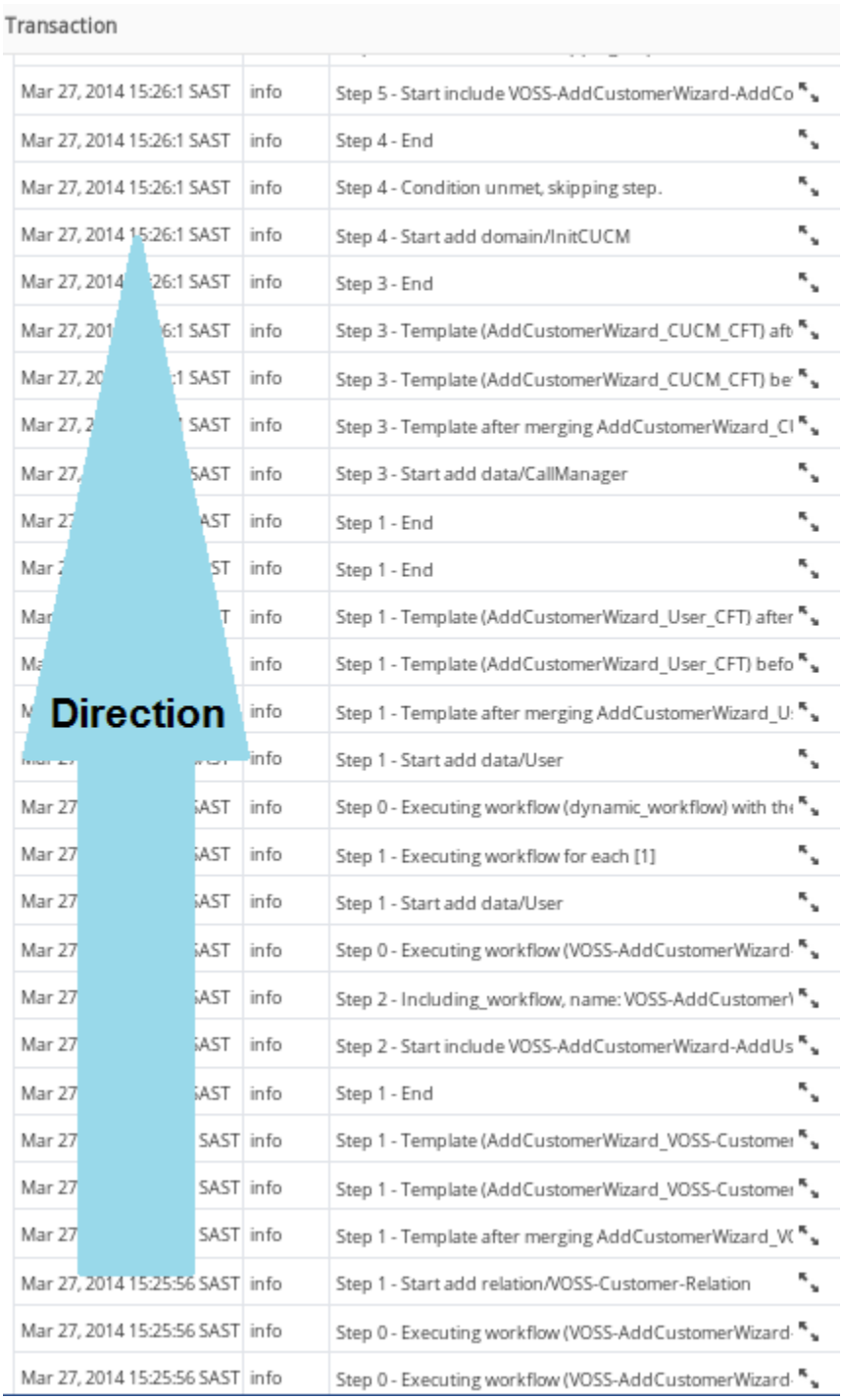
1. Create Voss-Customer-Relation Execute : VOSS-Relation-Add-Customer-PWF
    a. Create Hierarchy Node
    b. Create Base Customer Dom
    c. Create Voss Cust Dp
2. Create User

3. Create Call Manager

The transaction log shows all the steps of all the workflows that are executed. The first log entry of the wizard is at the bottom of the log list. The first step of each workflow is marked as `Step 0`.

The figures below show the example wizard flow and the corresponding logs.





21.4.10. Device Data Sync Errors in Transactions

The DataSync from a device has two steps:

1. A list request for all the resources of a specific type is made, for example for a User or Phone.
2. Requests for detailed information of each resource of the specific type.

The tables below show errors raised by devices and how these are handled or written to the transaction log by VOSS-4-UC. In the case of failed transactions, the tables point to possible causes of some errors.

Note:

- A number of CUCM device model errors are non-critical and will not fail data sync transactions.

- CUCM AXL handled by VOSS-4-UC (DataSync transaction final status is not failed)

Model	Operation	Device Error Message Match	VOSS-4-UC DataSync Action and/or error log
LocalRouteGroup	GET	No Search Criteria Defined	Ignored known error
LdapDirectory	GET	Item not valid: The specified LdapDirectory was not found	Ignored known error
UniversalDeviceTemplate	GET	Item not valid: The specified UniversalDeviceTemplate was not found	Ignored known error
LicensedUser	GET	Item not valid: The specified LicensedUser was not found','The endpoint reference (EPR) for the Operation not found is No License found for the specified user: Could not open database table	Ignored known error
LdapSyncCustomField	GET	Invalid ldapConfigurationName	Ignored known error
EndpointReleaseKey	GET	Column (name) not found in any table in the query (or SLV is undefined)','The endpoint reference (EPR) for the Operation not found is	Ignored known error
DirNumberAliasLookupandSync	GET	Item not valid: The specified DirNumberAliasLookupandSync was not found	Ignored known error
DeviceSerialNumber	GET	endpoint reference (EPR) for the Operation not found is	Ignored known error
LicenseCapabilities	GET	The endpoint reference (EPR) for the Operation not found is	Ignored known error
PhoneTypeDisplayInstance	GET	Wrong value for Protocol. Please enter a valid value.	Not all Phone Types have Vendor Config Rules. Ignored.

- CUCM Device errors not handled by VOSS-4-UC (DataSync transaction final status is failed)

Model	Operation	Model Error	Possible Cause
(All model types)	GET	Resource not found	A workflow in VOSS-4-UC deleted an item between the DataSync LIST operation and the GET operation
(All model types)	GET	AXL Error [-1]	This is a non-specific error raised by CUCM. Follow up with the CUCM team.

- CUC Device errors not handled by VOSS-4-UC (DataSync transaction final status is failed)

Model	Operation	Model Error	Possible Cause
(All model types)	GET	Resource not found	A workflow in VOSS-4-UC deleted an item between the DataSync LIST operation and the GET operation
ImportUser	GET	Resource not found	1. A sync between CUC and LDAP is running at the same time as the VOSS-4-UC sync to CUC. If the User is disabled or deleted on LDAP, then the User would removed as an Import User on CUC. 2. A workflow on VOSS-4-UC promoted a user from Import User to User by creating a Voicemail Box for that User, which also causes the user to be removed as Import User and created as a full User.

21.4.11. Export a Transaction

From the Transaction detail view, administrators can export upper level parent transactions. This will include their child sub-transactions as well as the associated transaction log entries in JSON format.

The exported files may also be requested by VOSS support operators for troubleshooting purposes.

1. As an administrator, choose **Administration Tools > Transaction** and select a parent transaction from the list.
2. From the transaction details view, choose **Action > Export Transaction**. A `.zip` archive file is downloaded by the browser.

Transaction Export Files and Format

The `.zip` archive filename format:

export-tx-<Transaction ID>_<YYYY>-<MM>-<DD>T<HH_MM_SS>.json.zip

Example: `export-tx-20705_2019-01-22T06_18_15.json.zip` for parent transaction ID 20705.

The `.zip` archive contains two files in JSON format:

- The Transaction Detail file - containing transaction (parent and sub-transaction) details as on the GUI - upper level and **Sub Transactions** table entries in JSON format:

  export-tx-<Transaction ID>_<YYYY>-<MM>-<DD>T<HH>:<MM>:<SS>.json

- The Transaction Log file - containing entries as on the table of **Log** entries of a transaction on the GUI (up to 1000 entries) in JSON format:

  export-tx-logs-<Transaction ID>_<YYYY>-<MM>-<DD>T<HH>:<MM>:<SS>.json

Transaction Detail File Format

The example snippet below shows transaction details data of the the upper level parent.

- Upper level parent entries are identified by the same `pkid` and `top_level` values, with `"parent_pkid": null`.
- Child and descendant entries show different `pkid` and `parent_pkid` values. The tree of parent and child entries can be determined by inspecting these values.


```
"processor_host_name": "VOSS-voss-queue",
"pkid": "c0a03e99-0c93-4d85-8736-f05b54f8fe55",
"hierarchy": "5c46a8efce894e001453b2a8",
"submitted_time": "2019-01-22T06:18:15.804000Z",
"started_time": "2019-01-22T06:18:15.839000Z",
"detail": "[ 9\\/9 ] succeeded from [ 1 ] sheet in H2-5-VOSS4...
"top_level": "c0a03e99-0c93-4d85-8736-f05b54f8fe55",
"priority": "Normal",
"duration": 3.187191,
"submitter_host_name": "VOSS",
"txn_seq_id": "20705",
"parent_pkid": null,
"action": "Execute Bulk Load",
"message": null,
"completed_time": "2019-01-22T06:18:19.026000Z",
"operation": "execute"
```


Transaction Log File Format

The snippet below has been formatted for readability. The `transaction_id` in the two entries shown will correspond with `pkid` entries in the Transaction Detail file, so that the Log entries can be associated with the transactions and sub-transactions.


```
{
   "severity": "info",
   "format": "text",
   "log_id": "5c46b5a7ce894e0014569a0b",
   "time": "2019-01-22T06:18:15.871000",
   "message": "H2-5-VOSS4UC-HCS-Customer_Data_ClassOfService...
   "transaction_id": "c0a03e99-0c93-4d85-8736-f05b54f8fe55"
},
{
   "severity": "info",
   "format": "text",
   "log_id": "5c46b5abce894e0014569ab3",
   "time": "2019-01-22T06:18:19.012000",
   "message": "Summary for sheet: Sheet1, No errors",
   "transaction_id": "d7aa7333-f692-40b4-a637-80cf456c1f70"
},
```

22 Advanced Tools for System Administrators

22.1. Custom variables

22.1.1. Add Custom Variables

System administrators can create custom macros for use in for example custom Configuration Templates.

Note:

- The macro needs to be evaluated at the hierarchy that it is created.
- The same macro variable can be defined to have different values at different hierarchies.

---

1. Choose **Advanced Tools > Custom Variables** and click **Add**.
2. Enter the macro name, optional description and value. The name must be prefixed with `CV_`. For details on macro syntax, refer to the “Advanced Configuration Guide”.
3. Click **Save**.

To test the macro, enter it in the macro evaluator at **Administration Tools > Macro Evaluator**.

Example

Create:

```
CV_current_time

Current time is: {{ fn.now }}
```

Invoke:

```
{{ macro.CV_current_time }}
```

Output example:

```
Current time is: 2017-03-31 13:20:18.509871
```

22.2. Model Report

22.2.1. Create Model Report

System and advanced administrators can create and display reports on the data under a selected site hierarchy. The purpose of such a report is to show the model types: device and data models at a site as well as the number of instances of each model type.

Reports for a hierarchy can be created, listed, viewed and deleted. Note that the relation data type is not shown, but component data models are reported on.

1. Log in as system administrator.
2. Navigate to the hierarchy for which the report is to be created.
3. Choose **Advanced Tools > Model Report > Create Model Report**
4. Verify that the Hierarchy level value is the required hierarchy.
5. Choose the model types to be reported on:
    - DATA Models
    - CUCM Models
    - CUC Models
    - LDAP Models
    - HCM-F Models (only if HCM-F is installed)
6. Click **Save** to create the report.

The time stamp of the report at the hierarchy is recorded. To see the progress of the report creation, choose **Advanced Tools > Model Report > Model Reports** and from the list of reports, either inspect the value in the **Status** column or choose the report to see the status. The report is available when the status is **Done**.

22.2.2. Manage Model Reports

Reports can be viewed and deleted.

1. Log in as system administrator.
2. Choose **Advanced Tools > Model Report > Model Reports**
3. To view a report, click the report to view. Details for each model type are displayed on a tab.
4. The **Detail** tab shows:
    - the type of report
    - date of creation
    - hierarchy of the report

    The model tabs show Count value for each model type, if these were selected. If a model type has no instances, in other words a zero count, this is not shown.
5. To delete a report, choose the report and click **Delete**.

23 UC Prep Management

23.1. Introduction

The UCPrep Profile tool further streamlines the preparation process of deployment of Cisco applications with VOSS-4-UC Provider and Enterprise so that administrators will not have to repeat the same configuration tasks over and over every time they stage or build a UC Application.

The tool provides an easy, flexible and repeatable way to define, store and load static configurations and other infrastructure setup needed in the UC applications. One or multiple sets of static configuration data can be set up and stored. The UCPREP Profile tool use can vary from provider to provider and even by customer within a provider.

The created static configuration can then be pushed to UC Apps as a “one-off”, and does not always have to be tied into a overall workflow.

23.1.1. UCPrep Feature Scope

The UCPrep tool covers the following areas of the Cisco Application Deployment:

- CUCM Date Time Groups
- CUCM Groups
- CUCM Host Adjustment
- CUCM SIP Trunk Security Profiles
- CUCM SIP Profiles
- CUCM Audio Codec Preferences
- CUCM Application Users
- CUCM Feature Control Policies
- CUCM Route Filters
- CUC Authentication Policies
- CUC User Templates

It is not necessary to adjust all of these UC Application elements within a given UCPrep Profile. For example, if a Unity server is not part of a deployment, the CUC elements may remain un-configured. Similarly, if there is no need to adjust the hostname of a CUCM node, then the input form tab for that configuration can remain empty.

23.2. Caveats

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

23.3. Menu Descriptions

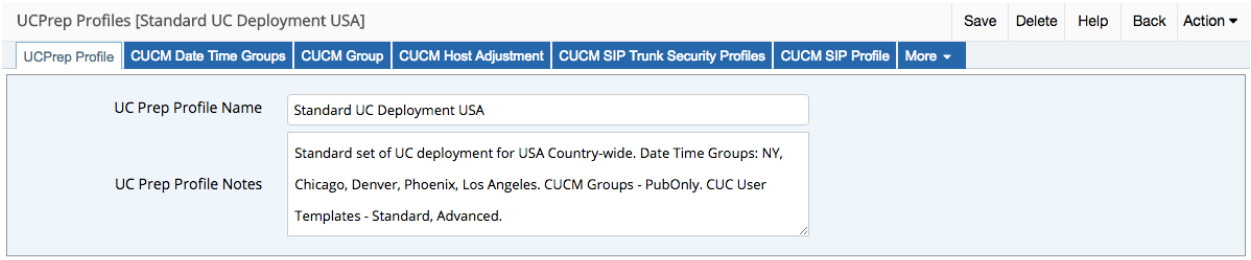
When the feature is exposed on an administrator menu, a list of menus items are available to carry out the UCPrep tasks.

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

- Initial Timezones can be selected before the UCPrep Profile configuration in order to simplify the management of the drop-down list of timezones in the tool.
- The UCPrep Application User List can also be set up where these are repeatedly used and pushed to UC Applications.
- The related Configuration Templates that drive the workflows of the configuration of the elements are grouped together for detailed customization and management.

Menu Name	Description and Notes
UCPrep Profile Push	This is the menu element used to push profile data into the target Cisco UC Applications.
UCPrep Profiles	The VOSS data structure that contains the configurations that can be repeatedly applied to UC Applications.
UCPrep Friendly Time-zones	List of time zones that is a mirror of the Call Manager available time zone database. This table is used to populate the Date/Time Group portion of the UCPrep Profile.
UCPrep Applica-tion User List	Administrator configurable list of Application Users that may be pushed into a Cisco Call Manager.
UCPrep Config-uration Templates	The collection of configuration templates that are utilized to provision the individual UC Application elements. Note that the menu item filters the configuration templates based on the prefix “ucprep”. Should any configuration template be cloned for customization please use the prefix.

23.4. UCPrep Profiles



From the **UCPrep Profiles** menu, the list view shows all created profiles at the administrator's hierarchy and below.

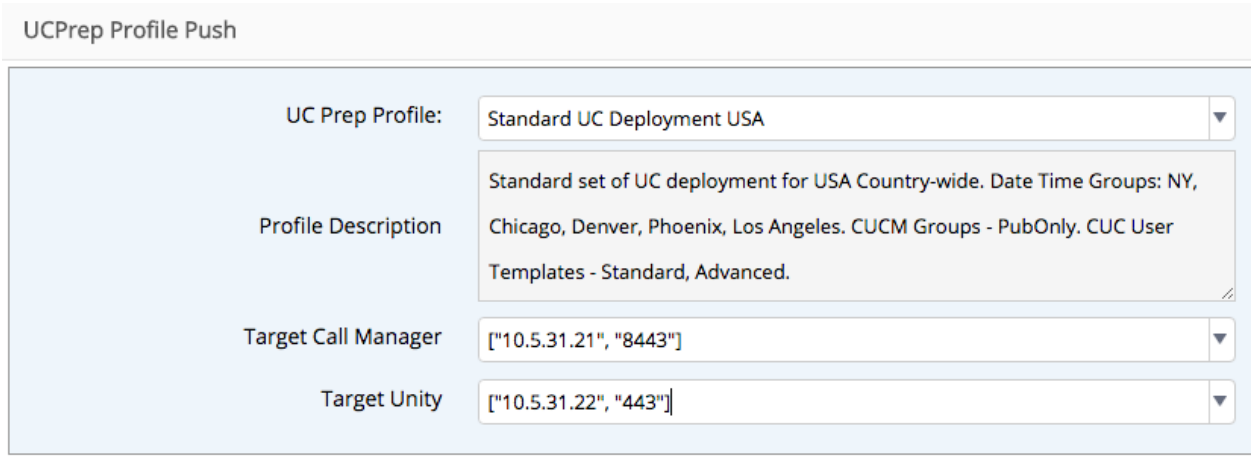
UCPrep Profiles are intended to be templates at a higher level in the hierarchy and are then cloned to a lower level for specific settings to a cluster. When cloning a UCPrep Profile the UC Prep Profile Name must be unique. The **UCPrep Profile Notes** should also be descriptive so that this information is available when the UCPrep Profile Push tool is used.

For example, a provider level profile may contain global element configuration that are not site or cluster specific. At a customer or site level, this profile can then be cloned and updated with configuration elements that apply to the customer or site.

23.4.1. UCPrep Profiles Reference

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

23.5. UCPrep Profile Push

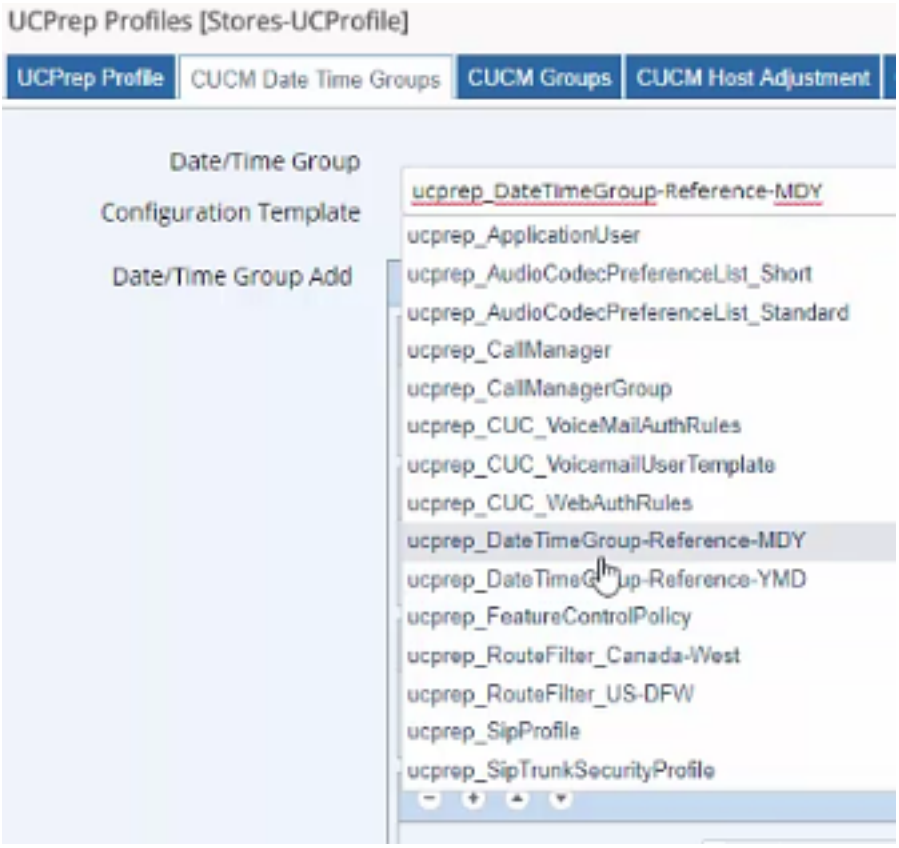


23.5.1. UCPrep Profile Push Reference

Name	Field Description
UCPrep Profile	Drop-down providing the available UCPrep Profiles configured on the system.
Profile Description	Description populated automatically when a UCPrep Profile is chosen from the UC Prep Profile drop-down.
Target Call Manager	Cisco Call Manager to which the UCPrep Profile Data will be pushed.
Target Unity	Cisco Unity server to which the UCPrep Profile Data will be pushed.

23.6. Date Time Groups

- Configuration Templates can be customized and added so that these become available in the **Date/Time Group Configuration Template** drop down list, for example to templates to customize the date format and listed in the **UCPrep Configuration Templates** menu.
- The **UCPrep Friendly Timezones** menu can be used to manage the list available in the **timezones** drop-downs, for example to shorten the list to only include the timezones that are used in the Data/Time groups.



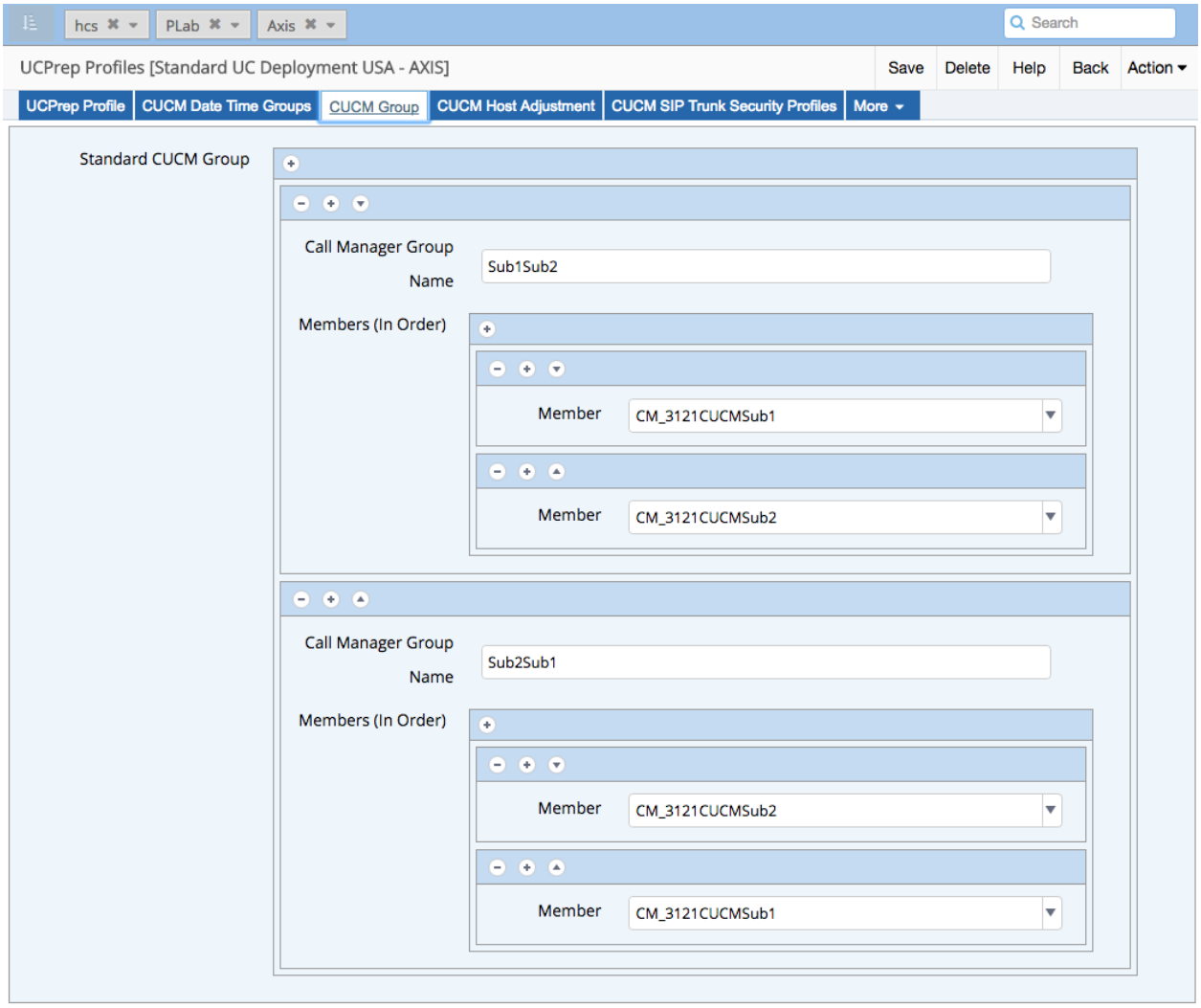
23.6.1. Date Time Groups Reference

Field	Field Description
Date/Time Group Configuration Template	Configuration template used to configure the specific settings to a Data-Time Group in Call Manager. Options available in the Configuration template are date format, separator, Time format, and so on. Note: the name of the date time group is automatically configured based on the chosen timezone entry. A timezone drop-down entry of `America/New_York` will create a date time group named `America-New_York`.
Date/Time Group Add	Timezones are chosen and added via drop-down. Any number of timezones may be chosen.

23.7. Call Manager Groups

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

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



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

23.7.1. Call Manager Groups Reference

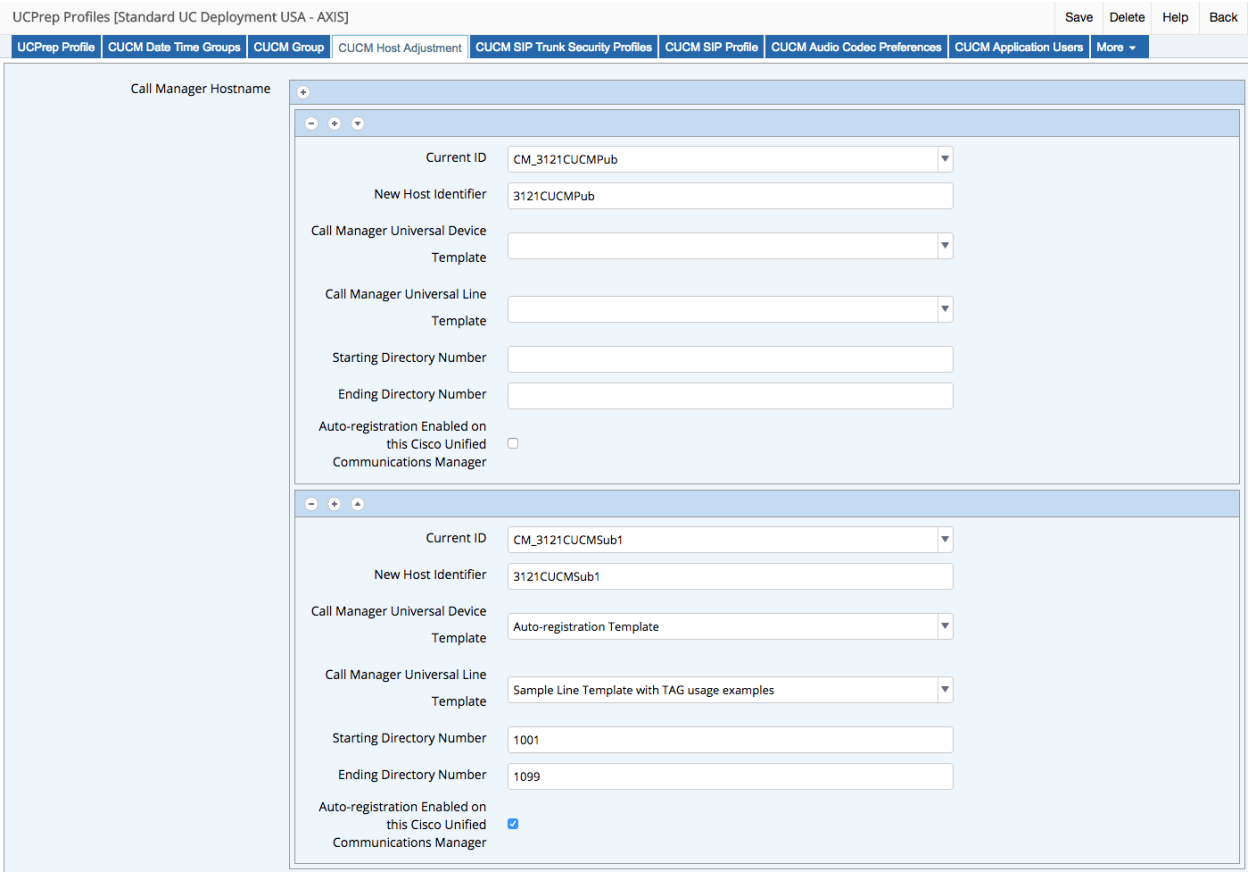
Name	Description
Standard CUCM Group	Entry mechanism to allow for configuration of an unlimited number of Call Manager Groups.
Call Manager Group Name	Free text entry box for Call Manager Group Name.
Members (In Order)	Add Call Manager nodes via drop-down by adding member entry boxes. The Call Manager nodes are added to the Call Manager Groups in the order presented in the input box.

23.8. Call Manager Host Adjustment

Multiple nodes of the cluster at the hierarchy can be modified.

Considerations for Host Adjustment are:

- Since the CUCM Host Adjustment modifies existing data in Call Manager, the data must be re-set or removed if a UCPrep Profile must be applied more than once.
- The CUCM Host adjustment occurs after the Call Manager Group configuration because the Call Manager will internally adjust the node names within a Call Manager Group when the node is renamed.
- If a node name is adjusted and a UCPrep profile is run a second or more times, the data on the **CUCM Groups** tab must be updated from the drop-downs to be the current CUCM node name.

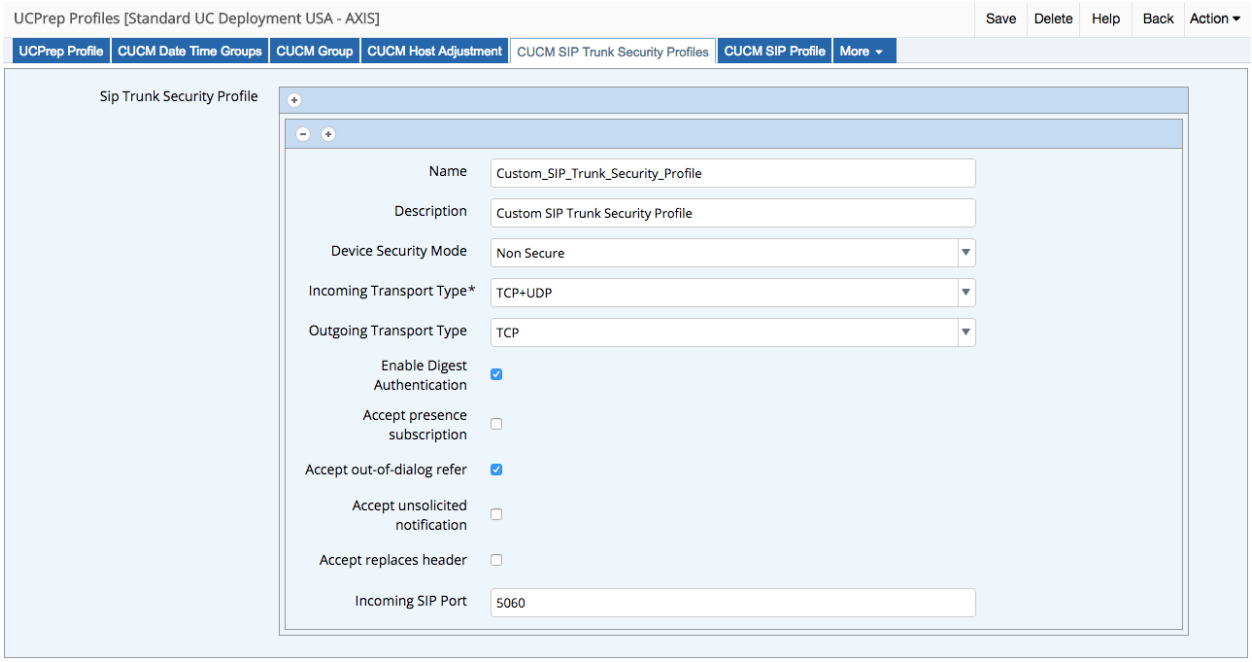


23.8.1. Call Manager Host Adjustment Reference

Name	Description
Call Manager Hostname	Entry area for multiple Call Manager Hostname adjustments.
Current ID	Drop-down providing the current Call Manager node names in the cluster.
New Host Identifier	Free text area to enter the new name as per business standards.
Call Manager Universal Device Template	Drop-down providing the CUCM configured Universal Device Templates. These templates are only required when configuring auto-registration on the Call Manager Node.
Call Manager Universal Line Template	Drop-down providing the CUCM configured Universal Line Templates. These templates are only required when configuring auto-registration on the Call Manager Node.
Starting Directory Number	Free text field for entry of starting directory number for auto-registration.
Ending Directory Number	Free text field for entry of ending directory number for auto-registration.
Auto-registration Enabled on this Cisco Unified Communications Manager	Check box to enable auto-registration on the Call Manager node.

23.9. Call Manager SIP Trunk Security Profiles

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

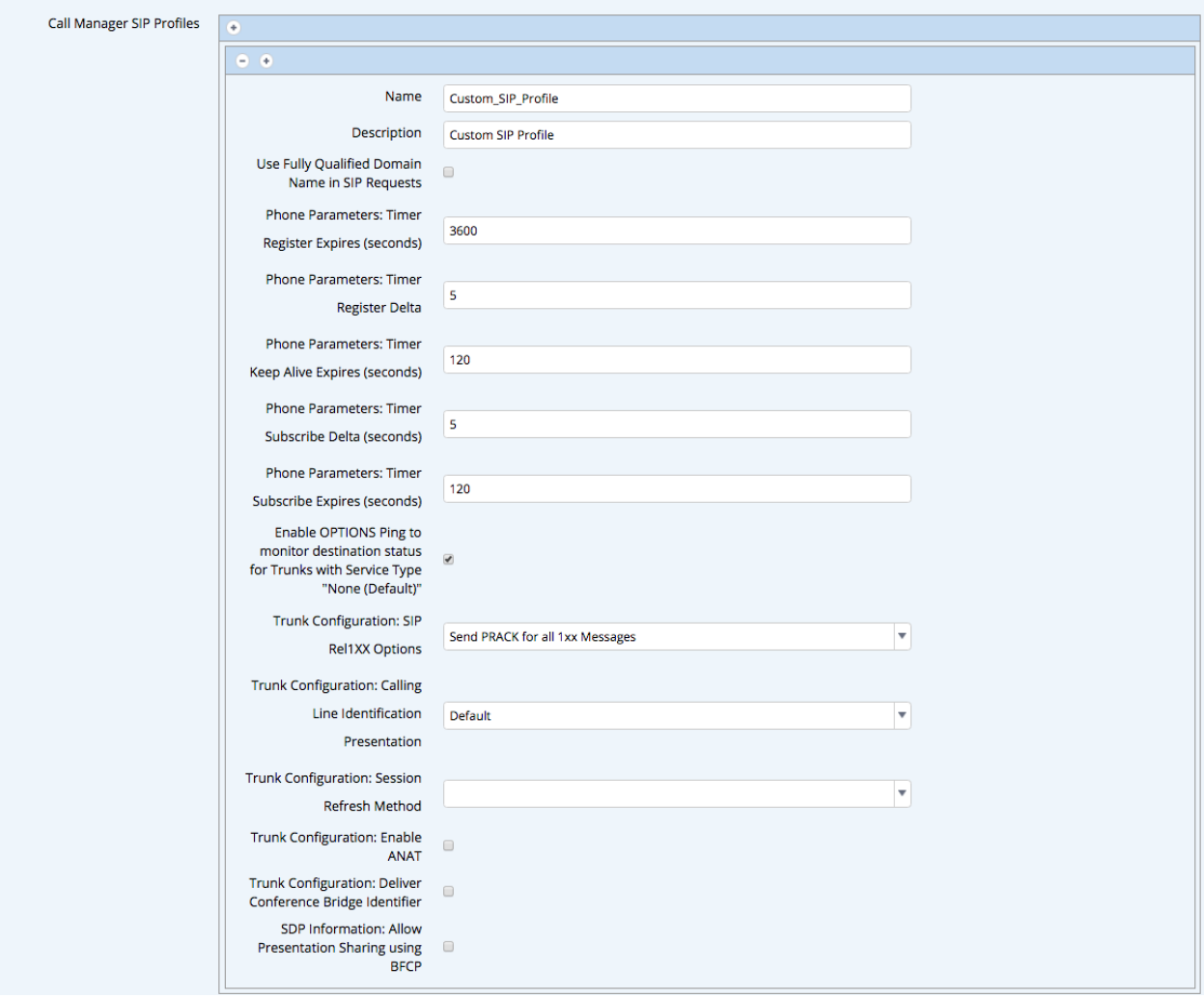


23.9.1. Call Manager SIP Trunk Security Profiles Reference

Name	Description
Name	Free text field to enter Sip Trunk Security Profile name.
Description	Free text field to enter Sip Trunk Security Profile description.
Device Security Mode	Drop-down providing options: • Non Secure • Authenticated • Encrypted
Incoming Transport Type	Drop-down providing options: • TLS • TCP and UDP
Outgoing Transport Type	Drop-down providing options: • TCP • UDP • TLS
Enable Digest Authentication	Check box to enable Digest Authentication.
Accept presence subscription	Check box to enable Accept of presence subscription.
Accept out-of-dialog refer	Check box to enable Accept out-of-dialog refer.
Accept unsolicited notification	Check box to enable Accept unsolicited notification.
Accept replaces header	Check box to enable Accept replaces header.
Incoming SIP Port	Free text box to set Incoming SIP Port.

23.10. Call Manager SIP Profiles

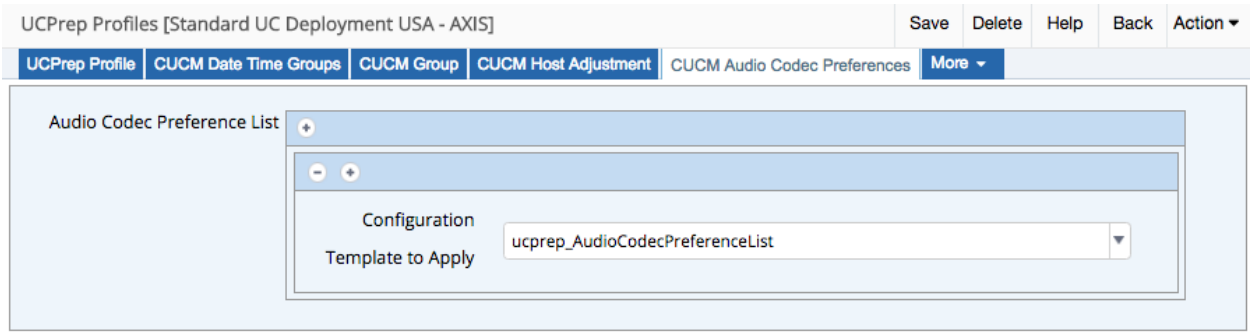
- Where values or time settings are shown in the fields of the form when adding a profile, these are the static values corresponding with the Call Manager defaults.



23.10.1. Call Manager SIP Profiles Reference

Field Name	Description
Call Manager SIP Profiles	Entry box to add any number of SIP Profile definitions.
Name	Free text field to enter name of SIP Profile.
Description	Free text field to enter description of SIP Profile.
Use Fully Qualified Domain Name in SIP Requests	Check box to enable Use Fully Qualified Domain Name in SIP Requests.
Phone Parameters: Timer Register Expires (seconds)	Free text box to adjust the Timer Register Expired timeout. Default 3600
Phone Parameters: Timer Register Delta	Free text box to adjust the Timer Register Delta. Default 5
Phone Parameters: Timer Keep Alive Expires (seconds)	Free text box to adjust the Timer Keep Alive Expires. Default 120
Phone Parameters: Timer Subscribe Delta (seconds)	Free text box to adjust the Timer Subscribe Delta. Default 120
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type “None (Default)”	Check box to Enable OPTIONS Ping.
Trunk Configuration: SIP Rel1XX Options	Drop-down providing options • Disabled • Send PRACK if 1xx Contains SDP • Send PRACK for all 1xx Messages
Trunk Configuration: Calling Line Identification Presentation	Drop-down providing options • Default • Strict From URI presentation Only • Strict Identity Headers presentation Only
Trunk Configuration: Session Refresh Method	Drop-down providing options • Invite • Update
Trunk Configuration: Enable ANAT	Check box to enable ANAT
Trunk Configuration: Deliver Conference Bridge Identifier	Check box to enable Deliver Conference Bridge Identifier.
SDP Information: Allow Presentation Sharing using BFCP	Check box to enable Allow Presentation Sharing using BFCP

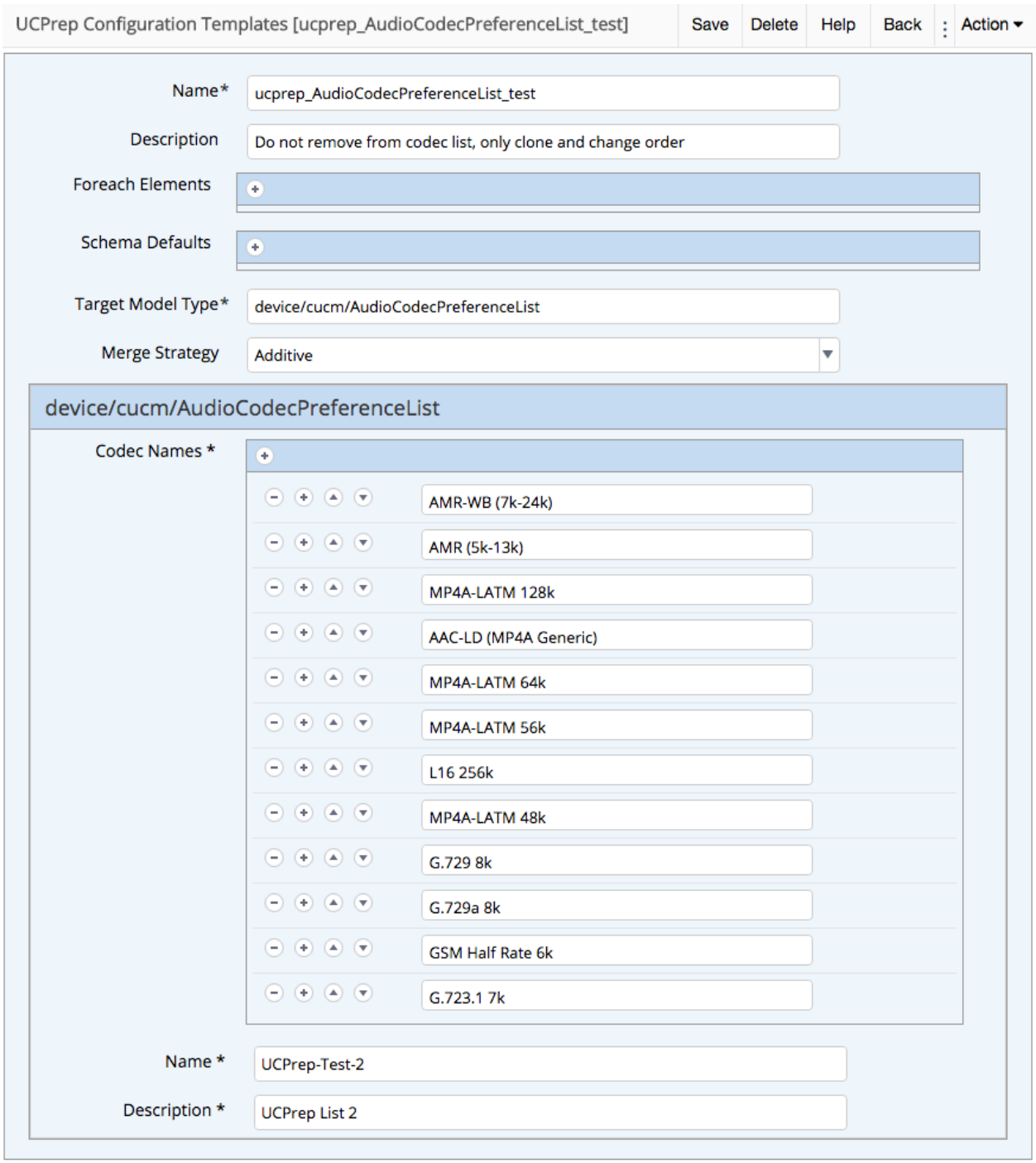
23.11. Call Manager Audio Codec Preferences



The Audio Codec Preferences List lends itself to be driven by a configuration template rather than a GUI input of a list of codecs.

The lists are written to Call Manager by selecting any number of configuration templates that have been set up to list out groups of codecs. Typically, a configuration template from the menu **UCPrep Configuration Templates** list view is cloned and modified to show the required codecs and settings.

Audio Codec Preference List Configuration Template Example:

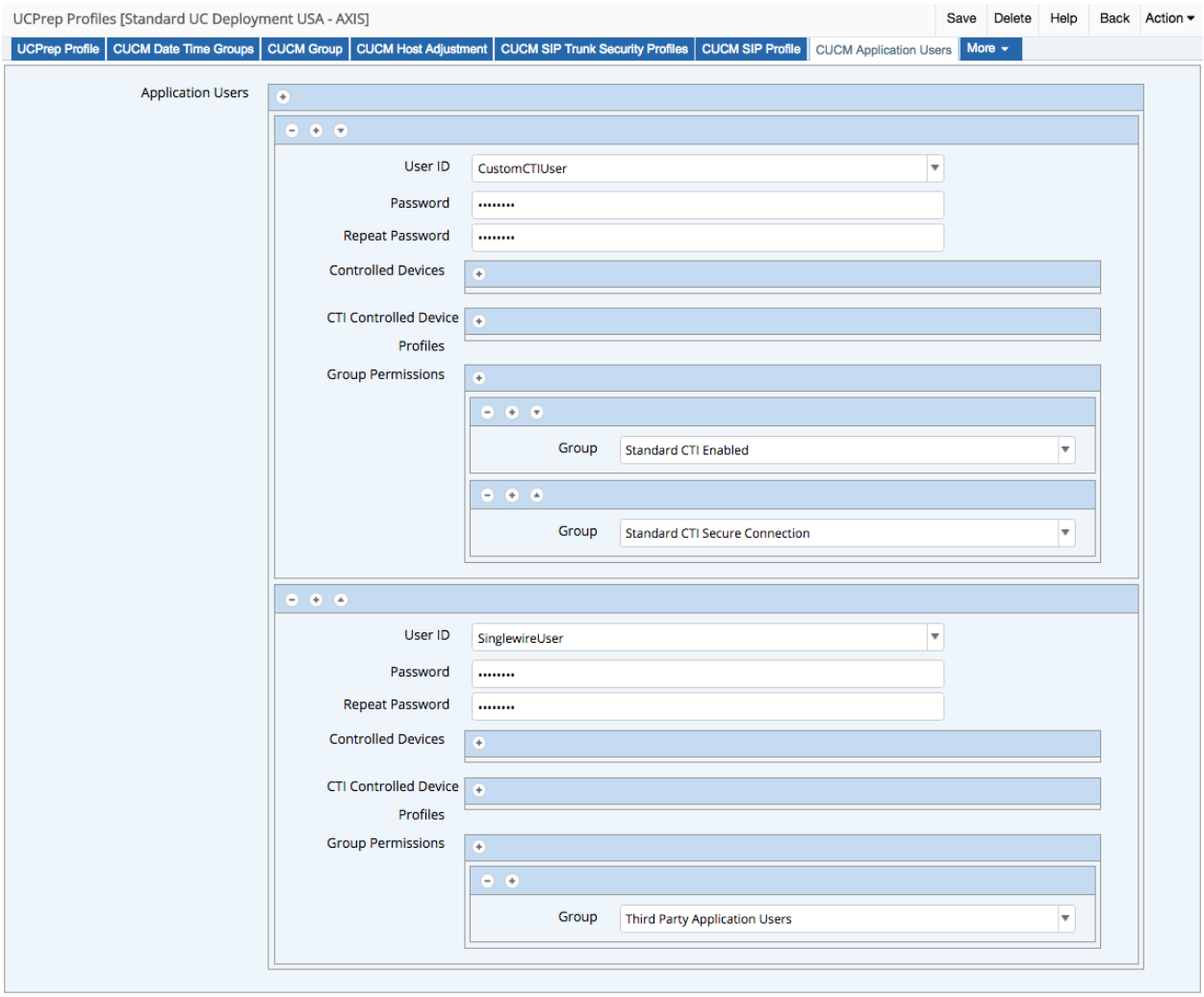


23.11.1. Call Manager Audio Codec Preferences Reference

Name	Description
Audio Codec Preference List	Entry mechanism for any number of Codec lists.
Configuration Template to Apply	Drop-down providing a list of available configuration templates.

23.12. Call Manager Application Users

- Application Users can initially be set up from the **UCPrep Application User** menu, to be available from the **Application Users** drop-down on the input form of this tab.
- New Application Users can also be added on the form by entering the user name directly into the **Application Users** input.
- Application User roles are automatically added from the selected **Group Permissions**.

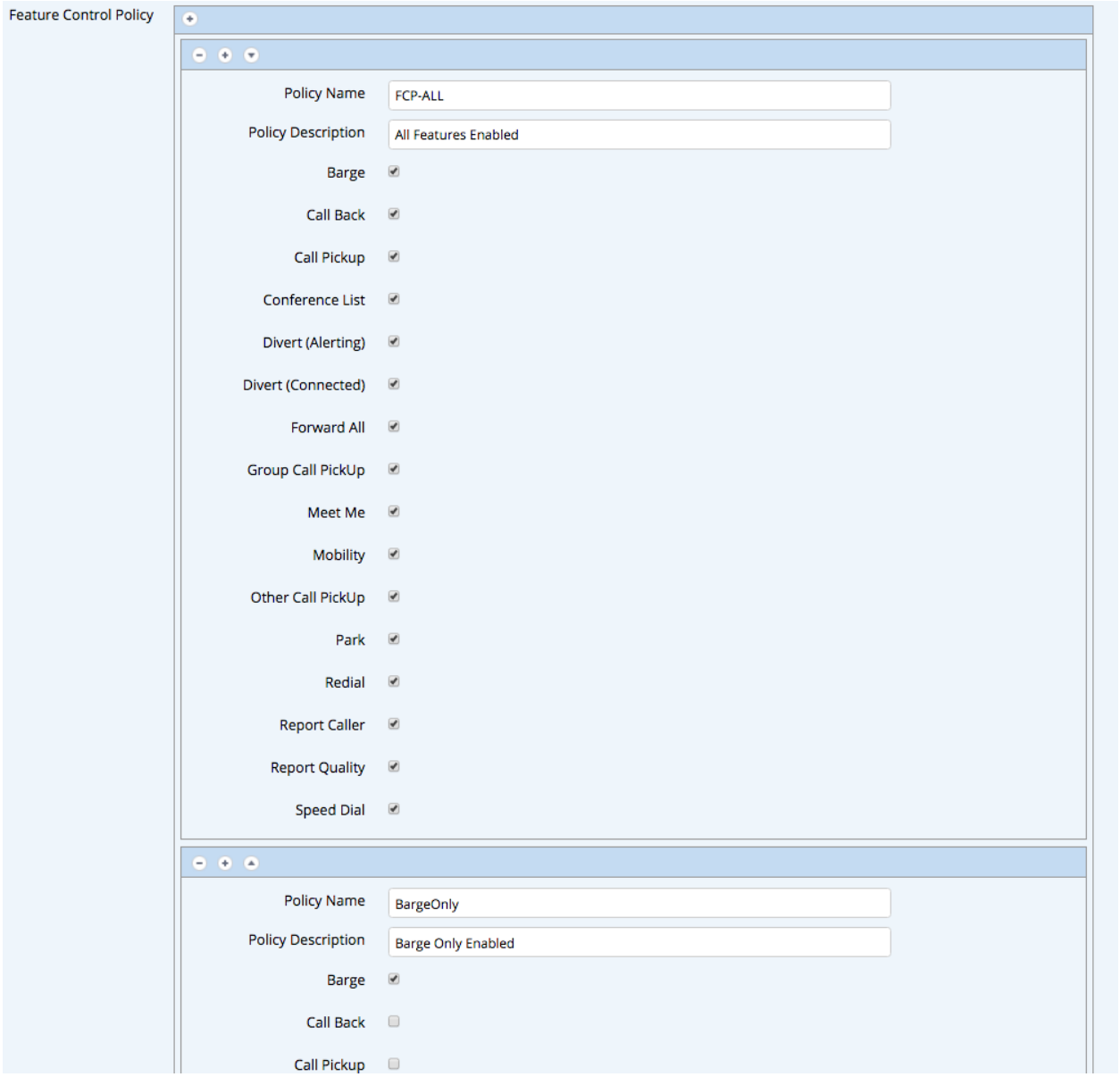


23.12.1. Call Manager Application Users Reference

Field Name	Description
Application Users	Mechanism for adding an unlimited number if application users to a Call Manager.
User ID	The Application User ID. This drop-down is driven from the UCPrep Application User List in the menu. The idea behind this is to cut down on AppUser misspelling.
Password	Password for the application user
Repeat Password	Confirmation of entered password.
Controlled Devices	Drop-down that provides a list of configured devices on Call Manager should an association be necessary.
CTI Controlled Device Profiles	Drop-down that provides a list of configured device profiles on Call Manager should an association be necessary.
Group Permissions	Drop-down that provides the ability to build group permissions for the application user. The drop-downs will provide all configured groups from the Call Manager.

23.13. Call Manager Feature Control Policies

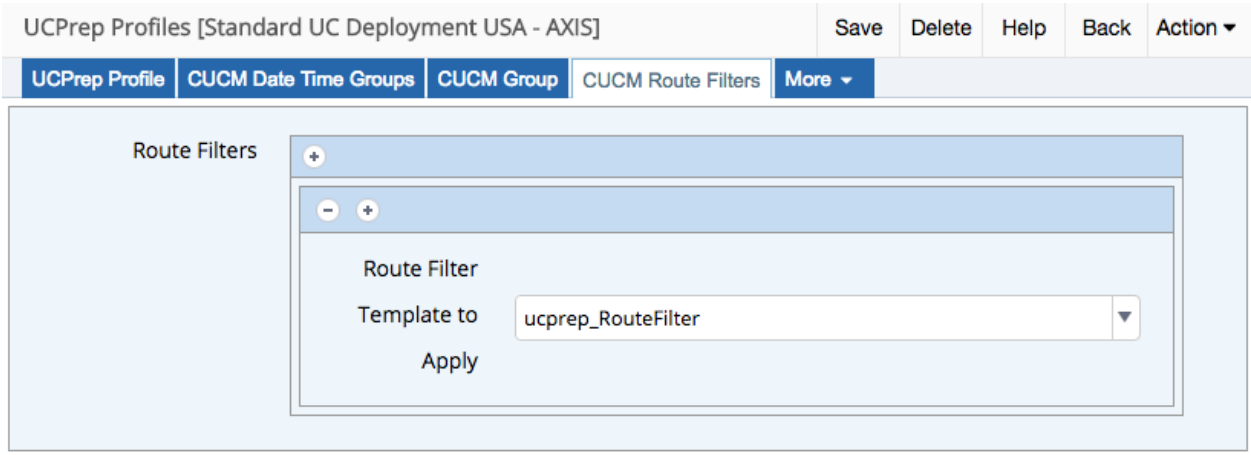
Feature Control Policies are defined by entering policy names and selecting features from the list of check boxes.



23.13.1. Call Manager Feature Control Policies Reference

Field Name	Description
Feature Control Policy	Mechanism to enter an unlimited number of Feature Control Policies
Policy Name	Free text field for entry of Feature Control Policy Name.
Policy Description	Free text field for entry of Feature Control Policy Description.
Check boxes to add the individual services into the Feature Control Policy	• Barge • Call Back • Call Pickup • Conference List • Divert (Alerting) • Divert (Connected) • Forward All • Group Call PickUp • Meet Me • Mobility • Other Call PickUp • Park • Redial • Report Caller • Report Quality • Speed Dial

23.14. Call Manager Route Filters

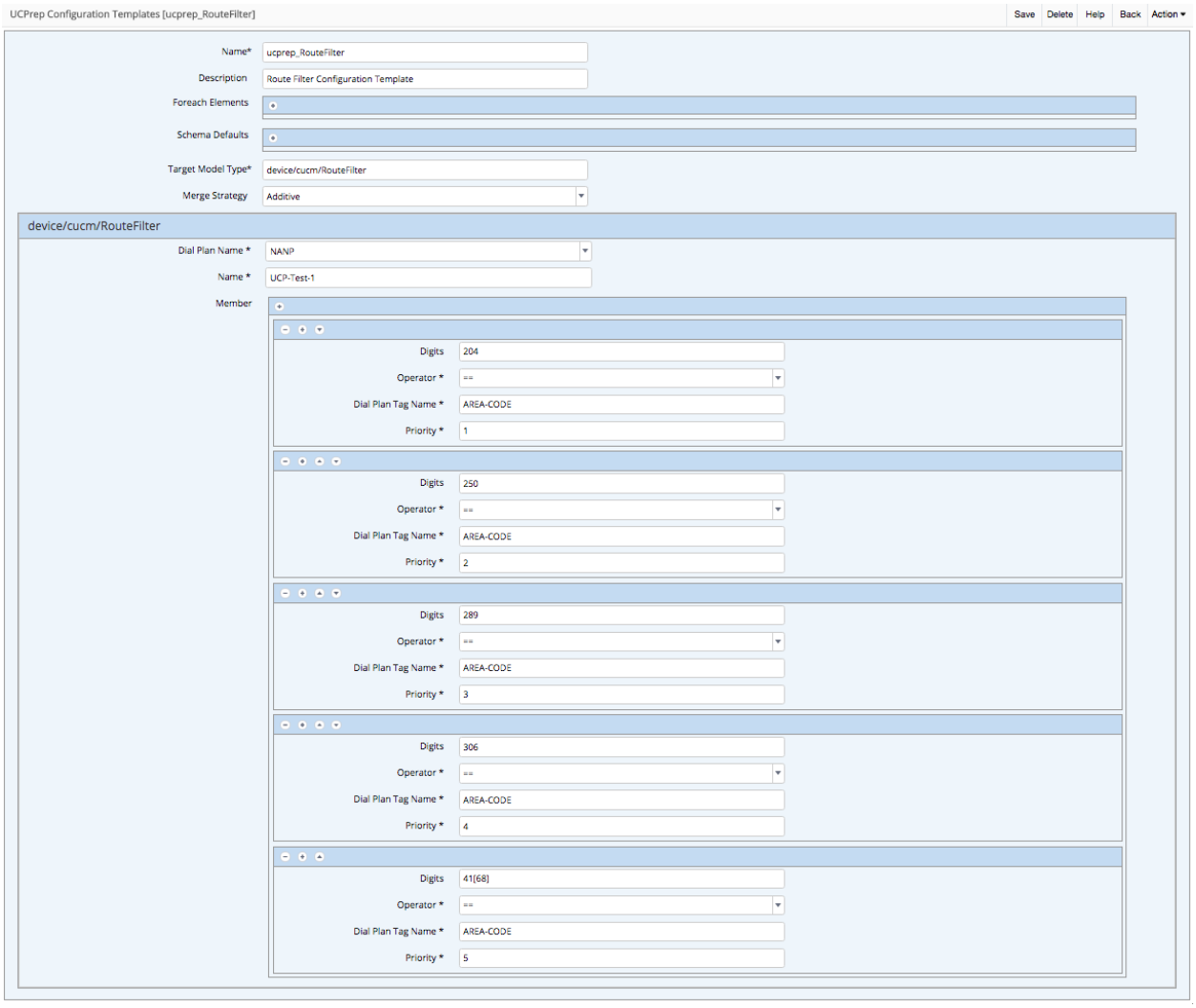


The Route Filter lends itself to be driven by a configuration template rather than a GUI input of clauses.

The filters are written to Call Manager by selecting any number of configuration templates from the **Route Filter Template to Apply** drop-down on the input form.

Typically, a configuration template from the menu **UCPrep Configuration Templates** list view is cloned and modified to show the required Route Filter settings.

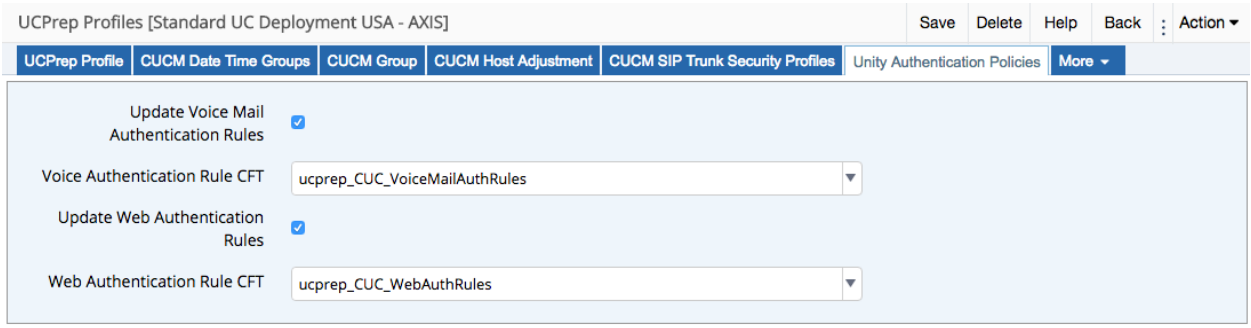
Example of Route Filter Configuration Template:



23.14.1. Call Manager Route Filters Reference

Name	Description
Route Filters Route Filter Template to Apply	Mechanism to add an unlimited number of route filters via configuration template. Drop-down to provide a list of available configuration templates.

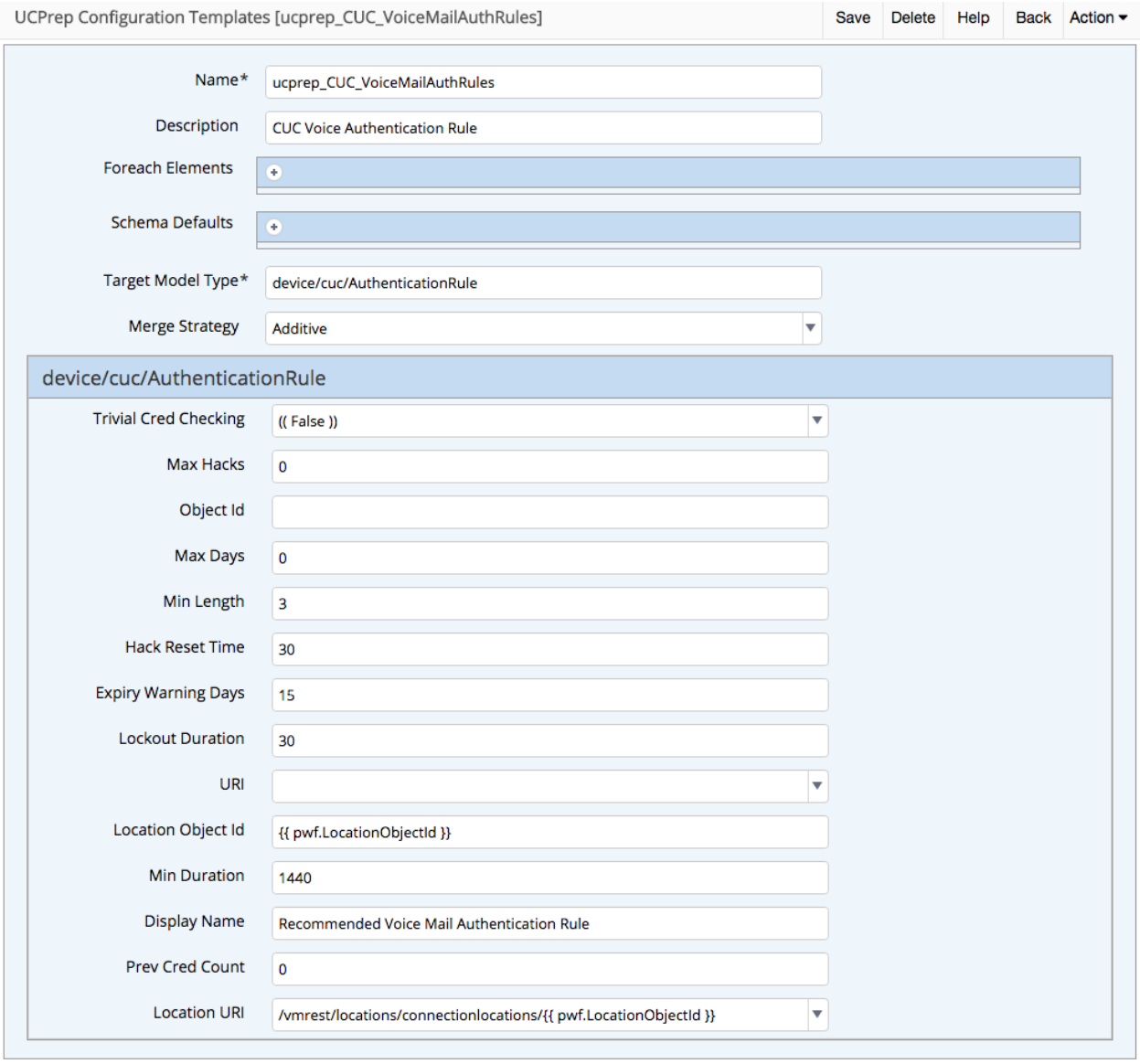
23.15. Unity Authentication Policies



The Unity authentication rule lends itself to be driven by a configuration template rather than a GUI input, since settings commonly do not change and the same group of settings are repeated.

Typically, configuration templates from the menu **UCPrep Configuration Templates** list view are cloned and modified to show the required Voice and Web Authentication Rules.

Example of Authentication Rule Configuration Template:



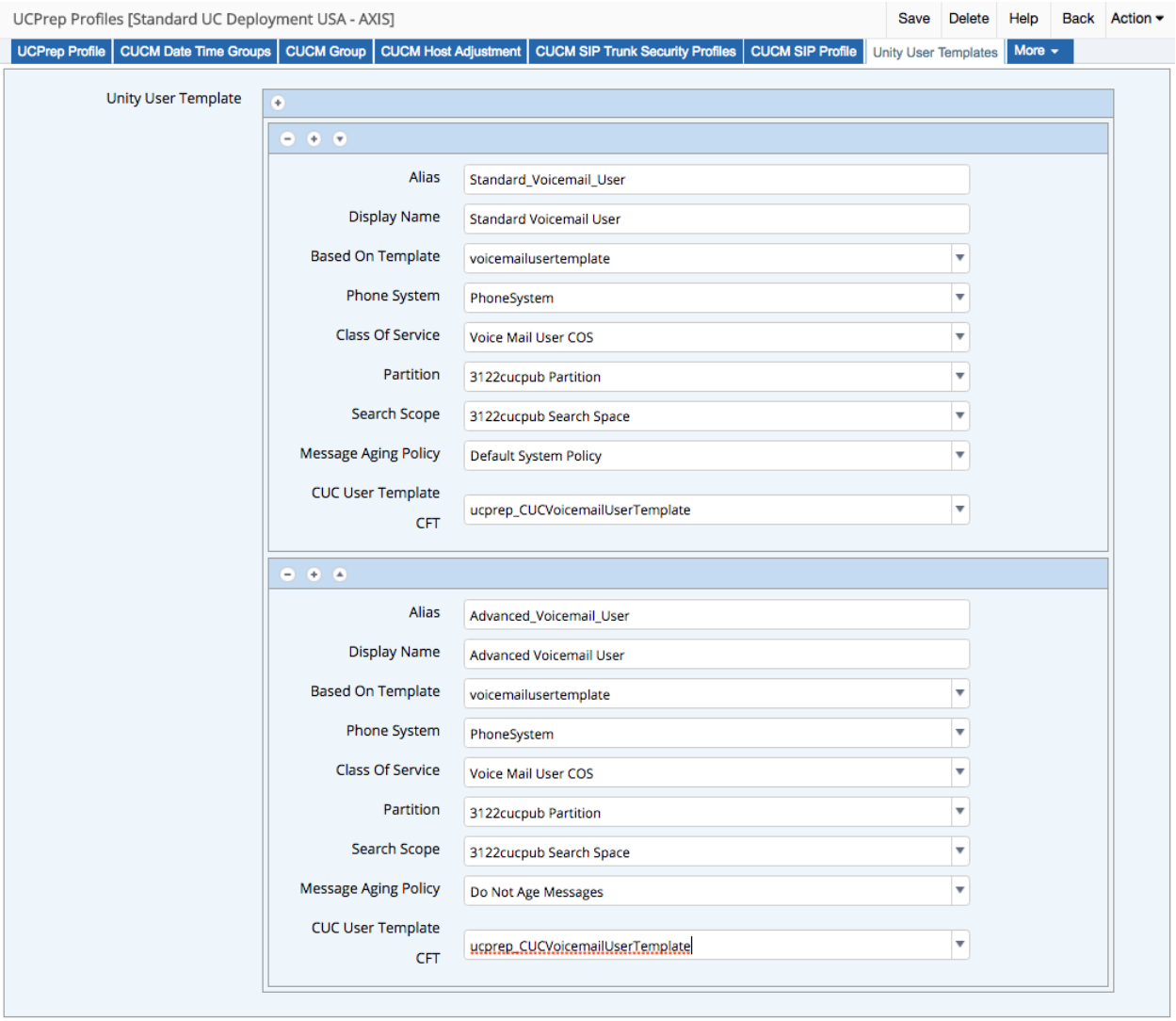
23.15.1. Unity Authentication Policies Reference

Field Name	Description
Update Voice Mail Authentication Rules	Check box to enable the update of the Voice Mail Authentication Rule from the UCPrep Profile.
Voice Authentication Rule CFT	Drop-down providing a list of available configuration templates.
Update Web Authentication Rules	Check box to enable the update of the Web Authentication Rule from the UCPrep Profile.
Web Authentication Rule CFT	Drop-down providing a list of available configuration templates.

23.16. Unity User Templates

The list of user templates shown on the input form are those that are most often changed. Own templates can be added as new entries and options selected from the available drop-downs.

Additional required fields can be added by selecting a created Configuration Template containing these from the **CUC User Template CFT** drop-down.



Field Name	Description
Unity User Template	Mechanism to enter an unlimited number of user templates.
Alias	Free text field to enter the User Template Alias.
Display Name	Free text field to enter the User Template Display Name.
Based On Template	Drop-down providing a list of Unity configured templates to use as the required reference.
Phone System	Drop-down providing the Unity configured phone system.
Class Of Service	Drop-down providing the Unity configured and available Class of Service.
Partition	Drop-down providing the Unity configured and available Partitions.
Search Scope	Drop-down providing the Unity configured and available Calling Search Spaces.
Message Aging Policy	Drop-down providing the Unity configured and available Message Aging Policies.
CUC User Template CFT	The VOSS configuration template, which will be used to populate the unexposed fields of a User Template.

24 Appendix: Microsoft Configuration

24.1. VOSS-4-UC PowerShell Proxy Configuration

VOSS-4-UC utilizes the Web Services-Management protocol (WSMan) to create the PowerShell sessions used to manage Microsoft UC applications. On Windows computers, WSMan is implemented by the Windows Remote Management (WinRM) service.

This section defines how to configure WinRM on a PS Proxy.

24.1.1. Domain Membership

All PS Proxy computers must be joined to the Active Directory domain under VOSS-4-UC management.

24.1.2. Enable PowerShell Remoting

PowerShell Remoting must be enabled on any computer with the PS Proxy role.

Starting with Windows Server 2012, all server versions of Windows have PowerShell remoting enabled by default.

On older versions of Windows Server, and on Windows client machines, you must enable PowerShell remoting manually. To do this, issue the following command from an elevated PowerShell prompt:

Enable-PsRemoting

24.1.3. Remote Management Service Account

Clients, including VOSS-4-UC, that connect to the WinRM service must provide credentials for an account with the characteristics listed below.

Remote Management Service Account

Account Type	Local Computer Account (Note: Not a domain account)
Local Group membership	Administrators Remote Management Users

24.1.4. WinRM Configuration

Configure WinRM with the appropriate settings for VOSS-4-UC by issuing the following commands from an elevated PowerShell session:

Enable-WSManCredSSP -Role Server -Force

Enable-WSManCredSSP -Role Client -DelegateComputer * -Force

Set-Item WSMan:\localhost\Service\AllowUnencrypted $true

Set-Item WSMan:\localhostServiceAuth\Basic $true

Set-Item WSMan:\localhost\Client\AllowUnencrypted $true

Set-Item WSMan:\localhost\Client\Auth\Basic $true

Set-Item WSMan:\localhost\Client\TrustedHosts "localhost" -force

24.1.5. Firewall Settings

Any firewalls between VOSS-4-UC and the computer hosting the WinRM service, including Windows Firewall on that computer, must permit the connections listed in the table below.

Note: These firewall exceptions are automatically created by the **Enable-PSRemoting** cmdlet.

WinRM Firewall Settings

Service	Protocol	Port
WinRM 2.0 (HTTP)	TCP	5985
WinRM 2.0 (HTTPS)	TCP	5986

24.1.6. Software Prerequisites

To manage a UC application such as Skype for Business Server, the management software specific to that application must be installed on the PowerShell Proxy. For example, to manage Skype for Business Server, the Skype for Business Server Administrative Tools must be installed on the PS Proxy.

Refer to *Required Management Software and Prerequisites* for details.

24.2. Domain Service Accounts

A domain account with the appropriate privileges is required for each of the applications managed by VOSS-4-UC: Active Directory, Skype for Business Server, Exchange Server, Skype for Business Online / Teams, and Exchange Online. You may use the same domain account for all of these applications, or you may create a separate account for each. The choice will depend on your organization's security requirements.

The minimum privileges required to manage each application are listed in the table below.

Important: In addition, any domain service account used by VOSS-4-UC to manage a UC application must be a member of the local Remote Management Users security group on the PowerShell Proxy.

Minimum Privileges by UC Application

UC Application	Service Account Minimum Required Privileges
Active Directory	AD (general[1]): Read AD (managed OU[2]): Read + Write
Skype for Business Server	Security group membership: • RTCUniversalServerAdmins
Exchange Server	Security group membership: • Recipient Management • UM Management
Microsoft Online / Skype for Business Online	Office 365 admin role: • Skype for Business administrator
Exchange Online	Create a custom role group with the following assigned roles: • Address Lists • Mail Recipient Creation • Mail Recipients • Mailbox Import Export • Migration • Move Mailboxes • Reset Password • SendMailApplication • UM Mailboxes

24.3. Required Management Software and Prerequisites

Download links and installation directions are listed below. *Management Software Requirements by UC Application* summarizes the required software and prerequisites.

Be sure to install all available critical and security Microsoft Windows updates before attempting to install the management software or prerequisites.

24.3.1. Active Directory

Management of Active Directory requires that the ActiveDirectory Powershell module be installed on any PS Proxy used for this purpose. If the PS Proxy is running a server version of Windows you can install this module by running the following cmdlet from an elevated PowerShell session:

[1] As an Authenticated User, the service account should already have read access to Active Directory.
[2] Read and write permissions are required for the parent OU containing the user and contact objects managed by VOSS-4-UC. Be sure to apply those permissions to the parent OU and all descendant objects.

Add-WindowsFeature RSAT-ADDS

If the PS Proxy is running on a client version of Windows (Windows 7 Professional through Windows 10 Professional), download and install the appropriate version of Remote Server Administration Tools. Select the applicable version from the links on this page:

https://support.microsoft.com/en-us/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems

24.3.2. Skype for Business Server

Skype for Business Server is managed with the Skype for Business Administrative Tools. Install those tools on the PS Proxy from the Skype for Business Server installation media.

24.3.3. Exchange Server

There are no specific software requirements for managing Exchange Server.

24.3.4. Office 365

Management of Office 365 requires the following software, which you should install in the order listed:

- Online Services Sign-in Assistant

  Download and install the `.msi` from this link:

  https://download.microsoft.com/download/5/0/1/5017D39B-8E29-48C8-91A8-8D0E4968E6D4/en/msoidcli_64.msi

- Windows Management Framework 5.1

  If your PS Proxy is running Windows Server 2016 or later, or Windows 10 Professional or later, then you already have WMF 5.1 and can skip this step.

  For older Windows versions download the appropriate version of WMF 5.1 from the link below, then install it:

  https://docs.microsoft.com/en-us/powershell/wmf/5.1/install-configure

- Azure Active Directory Module for Windows PowerShell

  Once WMF 5.1 has been installed, you can download and install this module directly from an elevated PowerShell session:

  Install-Module AzureAD

24.3.5. Skype for Business Online

The Skype for Business Online, Windows PowerShell Module is used for managing Skype for Business Online. This module has several prerequisites, which must be installed in the order listed below:

- Office 365 Management

  The Skype for Business Online, Windows PowerShell Module requires the Office 365 tools listed above, under *Office 365*, to be installed on the same PS Proxy. Install the Online Services Sign-in Assistant, WMF 5.1, and Azure Active Directory Module for Windows PowerShell before proceeding.

- KB2919442

  Download and run the installer, which can be found here:

  https://www.microsoft.com/en-us/download/details.aspx?id=42153

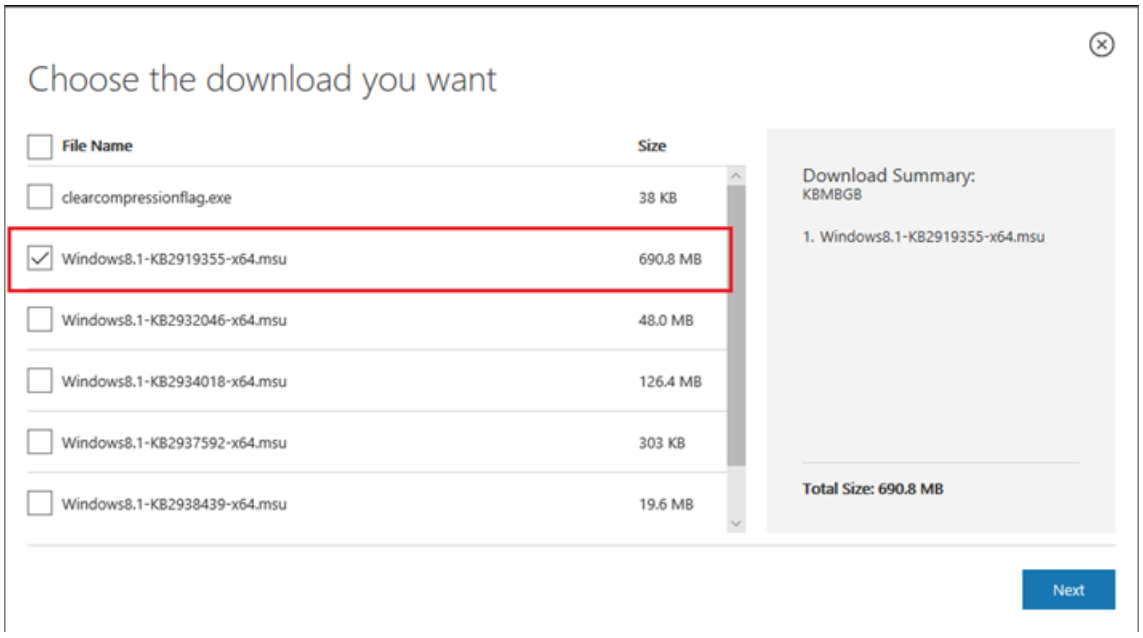
- KB2919355

  Download the package found at this link:

  https://www.microsoft.com/en-us/download/details.aspx?id=42335

  This package contains multiple updates. Of those, the only update required for the Skype for Business Online PowerShell module is KB2919355 itself.

  Restart the computer after installing KB2919355 and before proceeding with the next prerequisite.



- .NET Framework 4.7

  Download and install the package:

  https://www.microsoft.com/en-us/download/details.aspx?id=55170

Once the prerequisites are installed you can install the Skype for Business Online, PowerShell Module. You can find the installer at the link below:

https://www.microsoft.com/en-us/download/details.aspx?id=39366

24.3.6. Exchange Online

There is no specific management software required to manage Exchange Online.

The table below identifies the management software that must be installed on the PowerShell Proxy to support management of each of the UC Applications.

Management Software Requirements by UC Application

UC Application	Management Software Required
Active Directory	ActiveDirectory PowerShell module
Skype for Business Server	Skype for Business Administrative Tools
Exchange Server	No Exchange Server-specific management software required
Office 365	• Online Services Sign-in Assistant • Windows Management Framework 5.1 • Azure Active Directory Module for Windows PowerShell
Skype for Business Online	• KB2919442 • KB2919355 • .NET Framework 4.7 • Skype for Business Online, Windows PowerShell Module
Exchange Online	No Exchange Online-specific management software required

24.4. Step-by-Step Walk-Through

24.4.1. Walk-Through Overview

In this section we will walk through setting up a Microsoft domain for management by VOSS-4-UC, using a lab environment for demonstration purposes. As this is a lab setup, we will be taking a couple of shortcuts that are not recommended for a production environment. Those shortcuts will be highlighted where appropriate, and best practices will be noted.

Once the domain setup is complete we will configure VOSS-4-UC to communicate with the domain.

24.4.2. Lab Topology

The lab used in this example is a hybrid environment: it includes both an on-premises deployment and an Office 365 tenant. The on-premises domain is the fictitious `flexcorp.com`, and in addition to Active Directory this deployment includes Skype for Business Server and Exchange Server.

When selecting a vanity domain name for our Office 365 tenant we had to use a domain that we actually owned. Thus, our end users' email addresses and SIP addresses use the domain `vosslab.net`.

It is not necessary to reveal the underlying topology - Exchange Server addresses, Skype for Business front end pools, and so on. As you will see, all that VOSS-4-UC requires is the addresses of the PowerShell proxies that it will use to communicate with the UC applications.

24.4.3. PowerShell Proxies

For this example we will configure two PowerShell proxies. One of these will be used to for the connections on the on-premises components - Active Directory, Skype for Business Server, and Exchange Server. We

will use the other proxy to connect with the applications hosted in Office 365: Skype for Business Online and Exchange Online.

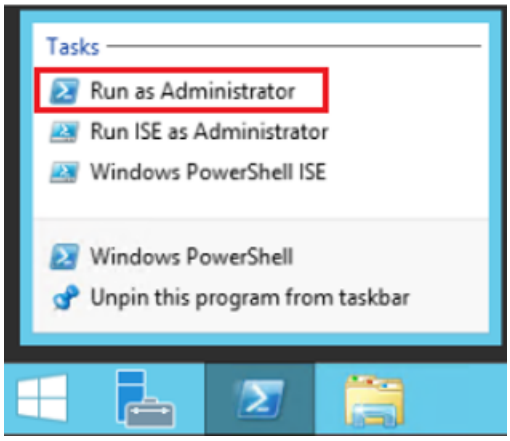
The decision to use two proxies rather than one - or five, or some other number in between - was somewhat arbitrary in this case; we chose two proxies mainly to demonstrate both how to divide the proxy duties between hosts, and how to combine multiple applications into a single proxy. We will install two new servers for this purpose, and we'll call them `psproxy01` and `psproxy02`, with the respective IP addresses of `10.5.25.240` and `10.5.25.241`. After installing Windows Server 2012 R2 on both machines, we join them to the `flexcorp.com` domain. We can now start configuring them.

24.4.4. PowerShell Proxy for On-Premises Applications

Enable PS Remoting

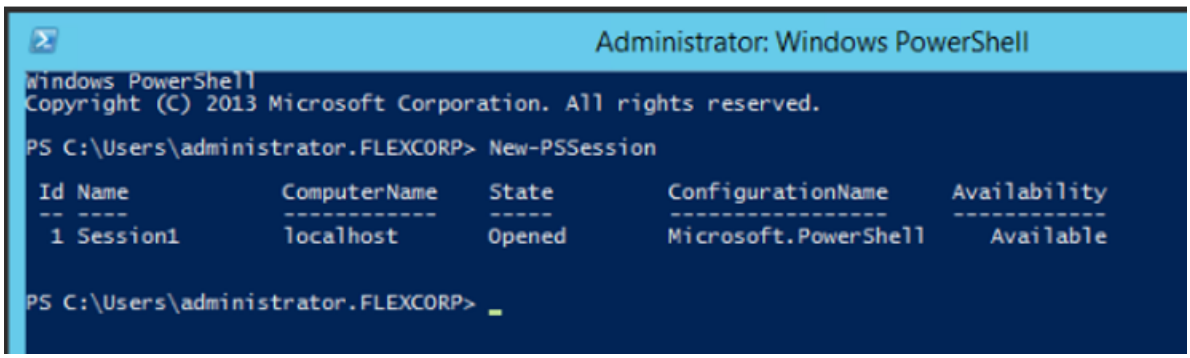
We'll start with the PS Proxy for the on-premises components, `pxproxy01`. The first task is to enable PowerShell Remoting. Since this is a Windows Server installation, PowerShell Remoting should already be enabled. Let's confirm that:

1. Open an elevated PowerShell session by right-clicking on the PowerShell icon in the task bar and choosing **Run as Administrator**.



2. Run the cmdlet **New-PSSession** with no arguments. If PowerShell Remoting is enabled the cmdlet should return information about the new session. (If we were running a client version of Windows, such as Windows 10 Professional Edition, PowerShell Remoting would not be enabled by default. We would have to manually enable it with the **Enable-PsRemoting** cmdlet.)

   Do not close the PowerShell window - we will use it again in a later step.

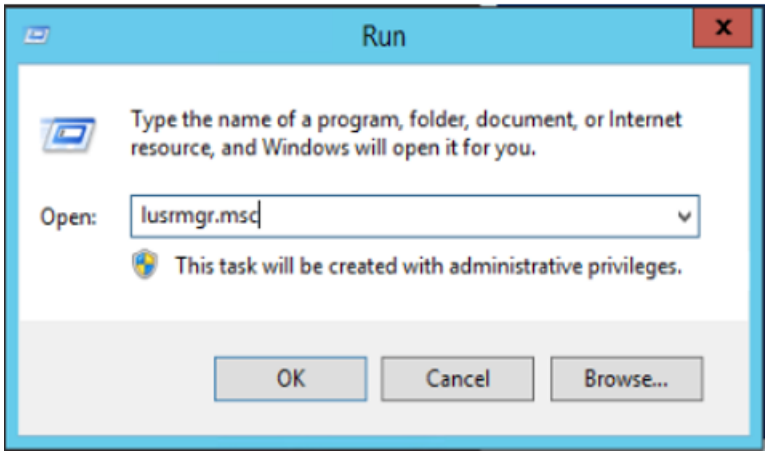


Create Remote Management Service Account

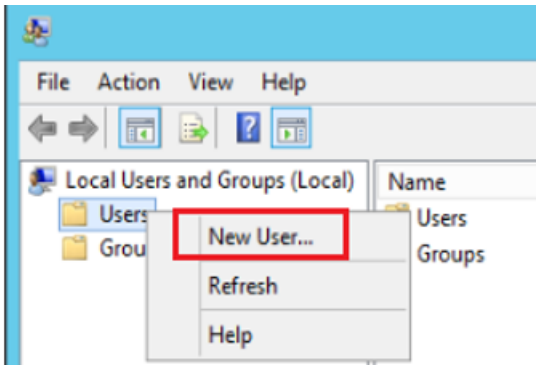
Next, we'll create the Remote Management Service Account and assign it to the correct security groups.

This is a local account on `psproxy01`, and we'll call it `WSMan-svc`.

1. Launch the **Local Users and Groups** console.
2. Right-click on the **Start** icon and choose **Run** to open the **Run** dialog.
3. Type `lusrmgr.msc` in the **Open** field and click **OK**.



4. Right-click **Users** under **Local Users and Groups (Local)** and choose **New User...** to open the **New User** dialog.

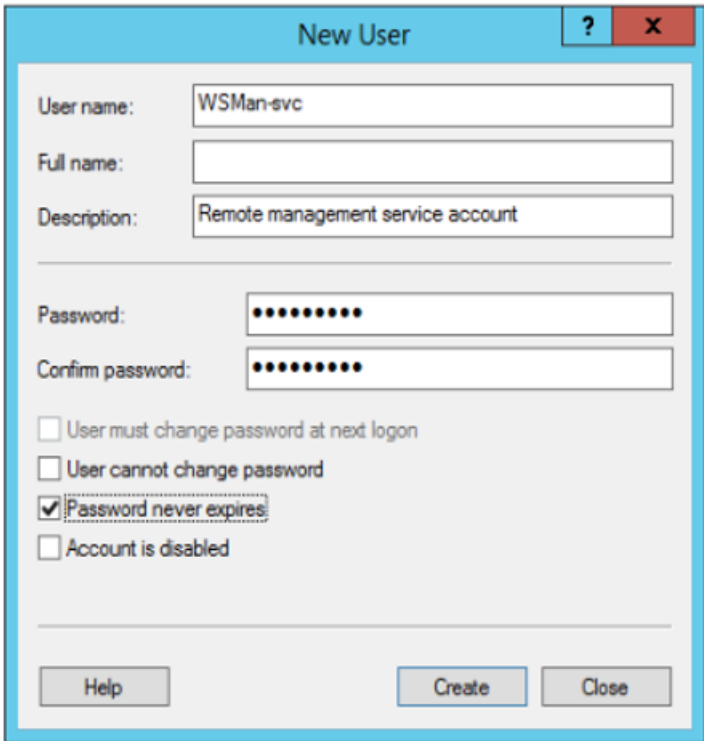


5. On the **New User** dialog:
   a. Enter the **User name** and **Password**.
   b. Clear the **User must change password at next logon** check box.
   c. Leave the **Account is disabled** check box cleared.
   d. Select or clear the **User cannot change password** and **Password never expires** check boxes according to your organization's security policies.

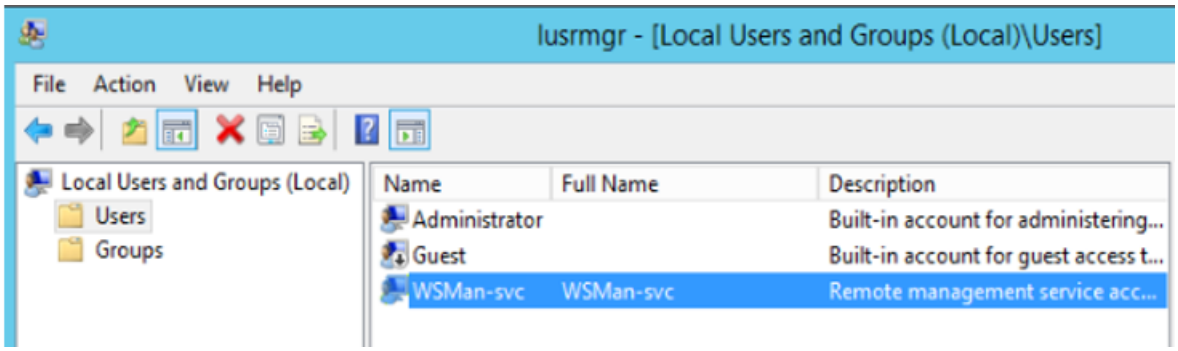
      Note: If you have to change the password, then you will also have to update VOSS-4-UC with the new password at the same time.

   e. Optionally enter a **Full name** and **Description**.

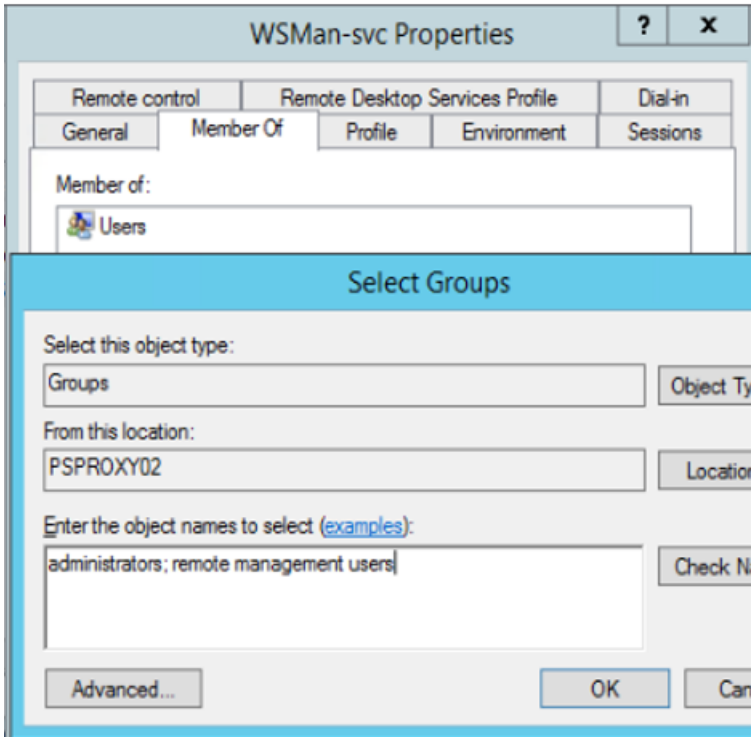
f. Click **Create** and then **Close** to open the **Local Users and Groups (Local)** window.



6. Choose **Users** from the navigation pane, then double-click the user you just created to open the **Properties** dialog for that user.



7. Choose the **Member Of** tab and click **Add...** to open the **Select Groups** dialog.
8. Type `administrators;remote management users` in the **Enter the object names to select** text box.
9. Click **OK** twice.



Configure WinRM Service

Now we'll configure the WinRM service. We will use the elevated PowerShell session we used earlier. (If you have closed it, just open another one by right-clicking the **PowerShell** task bar icon and choosing **Run as Administrator**.) In this PowerShell session run the following cmdlets exactly as shown under *WinRM Configuration*.

```
PS C:\Users\administrator.FLEXCORP> Enable-WSManCredSSP -Role Server -Force


cfg              : http://schemas.microsoft.com/wbem/wsman/1/config/service/auth
lang             : en-US
Basic            : false
Kerberos         : true
Negotiate        : true
Certificate      : false
CredSSP          : true
CbtHardeningLevel : Relaxed


PS C:\Users\administrator.FLEXCORP> Enable-WSManCredSSP -Role Client -DelegateComputer * -Force


cfg         : http://schemas.microsoft.com/wbem/wsman/1/config/client/auth
lang        : en-US
Basic       : true
Digest      : true
Kerberos    : true
Negotiate   : true
Certificate : true
CredSSP     : true


PS C:\Users\administrator.FLEXCORP> Set-Item WSMan:\localhost\Service\AllowUnencrypted $true
PS C:\Users\administrator.FLEXCORP> Set-Item WSMan:\localhost\Service\Auth\Basic $true
PS C:\Users\administrator.FLEXCORP> Set-Item WSMan:\localhost\Client\AllowUnencrypted $true
PS C:\Users\administrator.FLEXCORP> Set-Item WSMan:\localhost\Client\Auth\Basic $true
PS C:\Users\administrator.FLEXCORP> Set-Item WSMan:\localhost\Client\TrustedHosts "localhost" -force
PS C:\Users\administrator.FLEXCORP> _
```

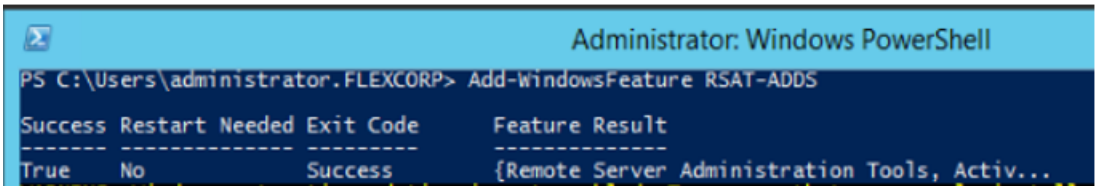
As noted above, we do not need to do anything to configure firewall exceptions as those are configured automatically by the **Enable-PsRemoting** cmdlet. So the next step is to install the software prerequisites.

Install Remote Server Administration Tools

We are configuring this machine to proxy PowerShell sessions to the on-premises environment - specifically Active Directory, Skype for Business Server, and Exchange Server. Of those three, there are specific software requirements for the first two.

For Active Directory we need the Remote Server Administration Tools. This feature is already installed on Windows Server editions, and simply needs to be enabled. Do this by running the cmdlet **Add-WindowsFeature RSAT-ADDS**. Note that if this were a client version of Windows we would have had to download and install Remote Server Administration Tools.

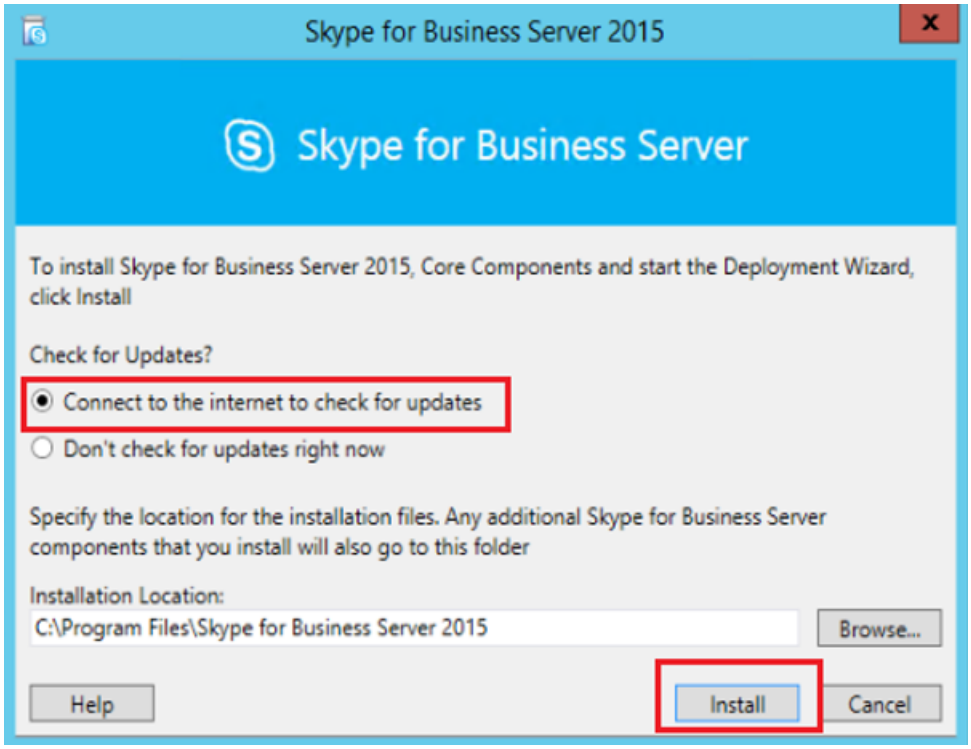
See *Software Prerequisites* for details on where to find the download.



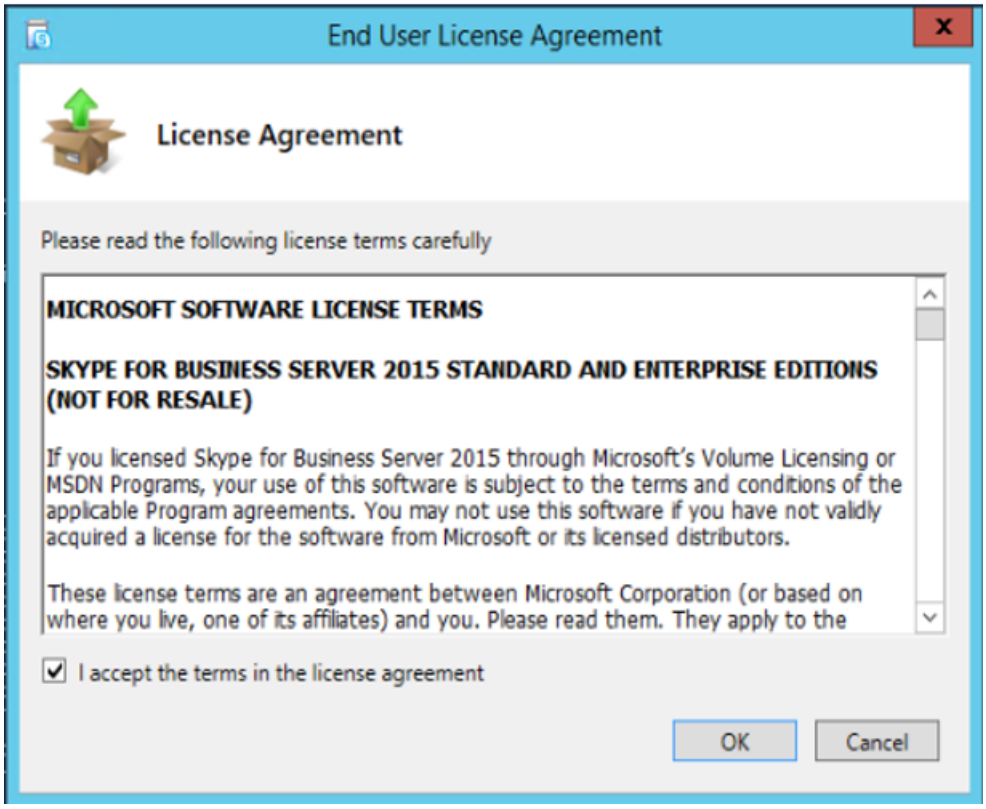
Install Skype for Business Administrative Tools

Next, we need the Skype for Business Administrative Tools. For that we will need the Skype for Business Server installation media corresponding to your Skype for Business Server deployment. In this sample lab we have this mounted on drive `D:`.

1. From Windows Explorer navigate to **This PC** and double-click the icon for your DVD drive (or navigate to the folder containing the Skype for Business Server ISO image and double-click that icon). If the Skype for Business Server installer does not start automatically, navigate to the `Setup\amd64` directory and double-click `Setup.exe`. The installer launches.
2. Choose **Connect to the internet to check for updates** radio button and click **Install**.

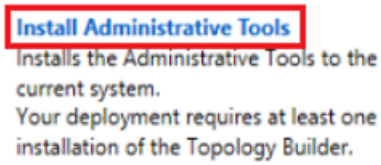


3. Accept the license agreement and click **OK**.

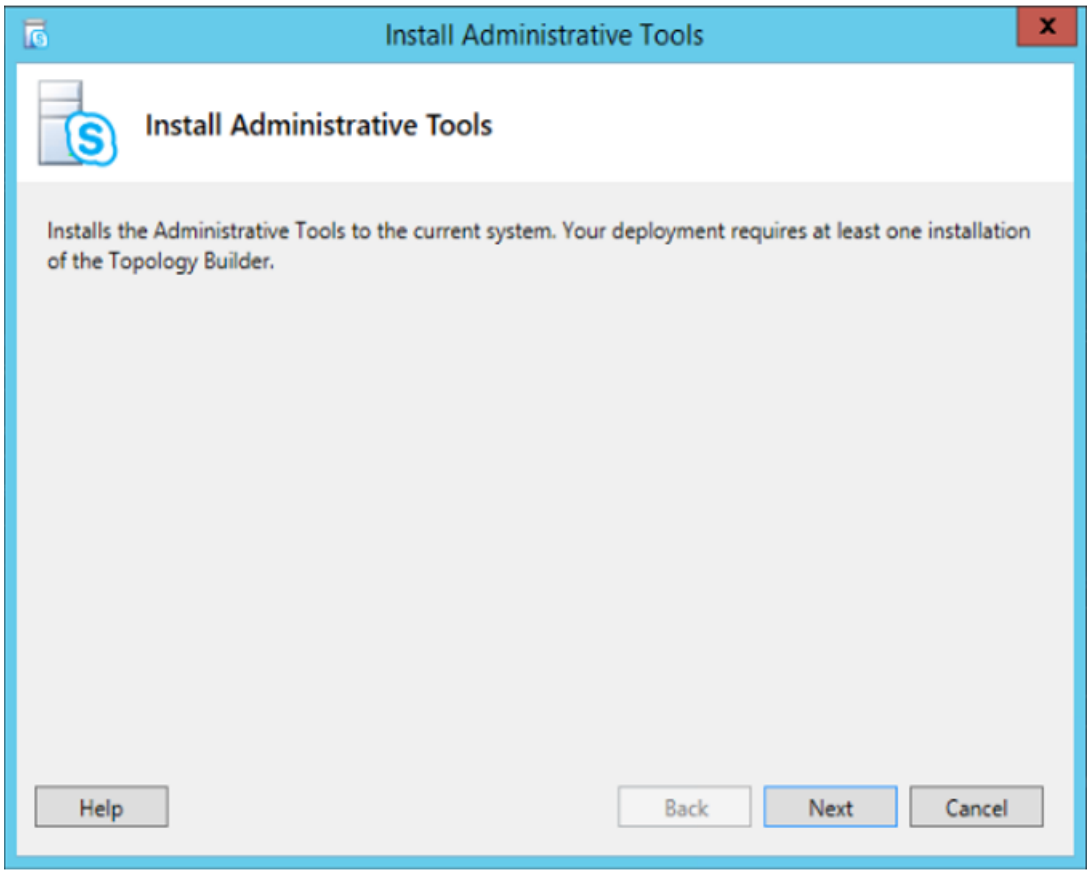


4. After updates have been downloaded and extracted, click **Next**.

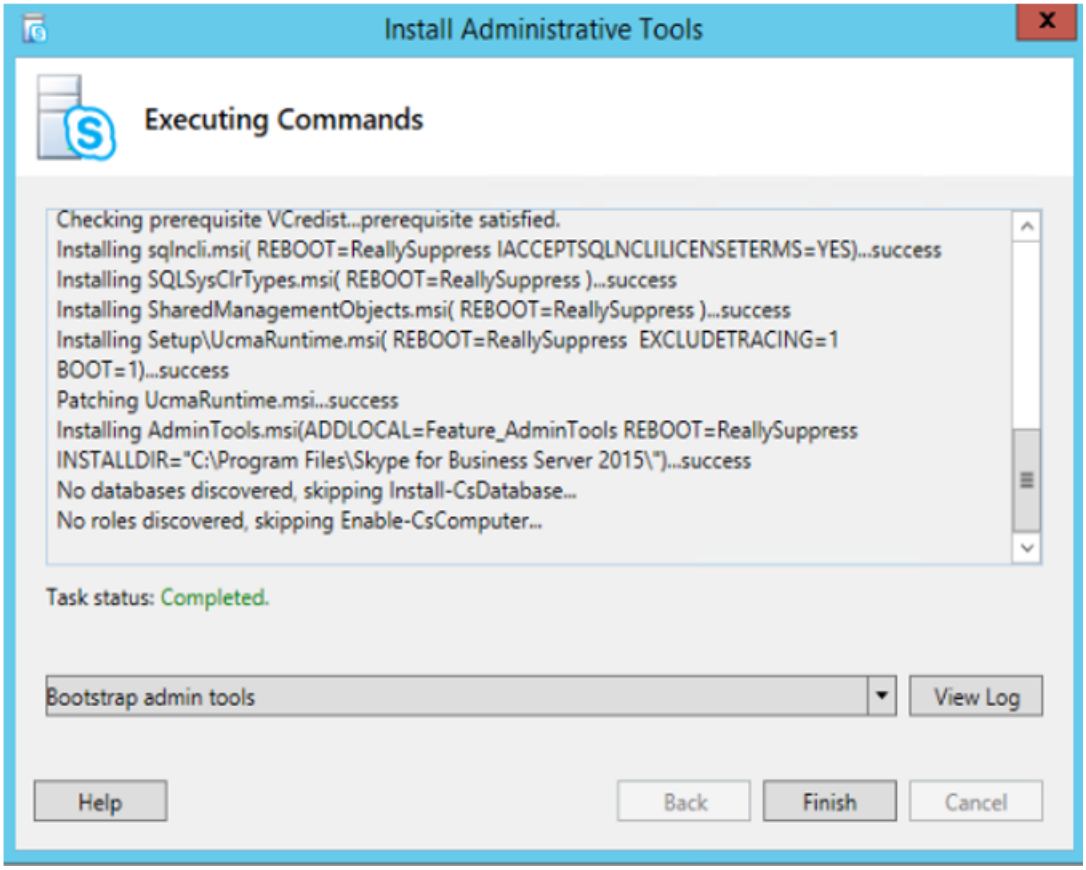
5. After the core components are installed, the Skype for Business Server 2015 Deployment Wizard launches. On the **Welcome to Skype for Business Server 2015** Deployment screen choose **Install Administrative Tools**.



6. Click **Next** on the **Install Administrative Tools** dialog.



7. Click **Finish**, and then click **Exit**. The administrative tools are now installed.



24.4.5. PowerShell Proxy for Online Applications

PowerShell Proxy for Online Applications

We have finished with `psproxy01`. The steps for `psproxy02` are the same until we come to the software prerequisites: we will do the following exactly as we did for `psproxy01`. Repeat on `psproxy02` the first four sections under “PowerShell Proxy for On-Premises Applications”, above.

- Join `psproxy02` to the `flexcorp.com` domain.
- Verify the PowerShell Remoting is enabled.
- Create the Remote Management Service Account. For consistency we will give this account the same name as on `psproxy01`.
- Make the Remote Management Service Account a member of the two local security groups Administrators and Remote Management Users.
- Configure the WinRM service.

Install Online Services Sign-in Assistant

We are now ready to install the software prerequisites.

Since this PS Proxy is going to be used to manage the cloud components we are going to need the Online Services Sign-in Assistant, Azure Active Directory Module for Windows PowerShell, and Skype for Business

Online, Windows PowerShell Module, and any prerequisites required by these modules.

1. Download the Online Services Sign-in Assistant (`msoidclil_64.msi`) and the Skype for Business Online, Windows PowerShell Module (`SkypeOnlinePowershell.exe`) from the links in *Required Management Software and Prerequisites* and copy it to the PS Proxy.
2. On the PS Proxy navigate to the folder where you copied the installer. Double-click `msoidcli_64.msi` to launch it, then follow the on-screen instructions.

Install Windows Management Framework 5.1

Our PS Proxy is running Windows Server 2012 R2, which means that it does not come with WMF 5.1. We'll go to the link documented in *Required Management Software and Prerequisites* and download the installer `Win8.1AndW2K12R2-KB3191564-x64.msu`.

Double-click the installer to get started. The process is straightforward; finish by restarting the computer.

Note: If the PS Proxy had been running Windows Server 2016 or later, or Windows 10 Professional or later, then WMF 5.1 is already part of the operating system and we would not have needed to install it manually.

Install Azure Active Directory Module for Windows PowerShell

Open an elevated PowerShell session, if you don't already have one open.

In that session enter the following command:

Install-Module AzureAD

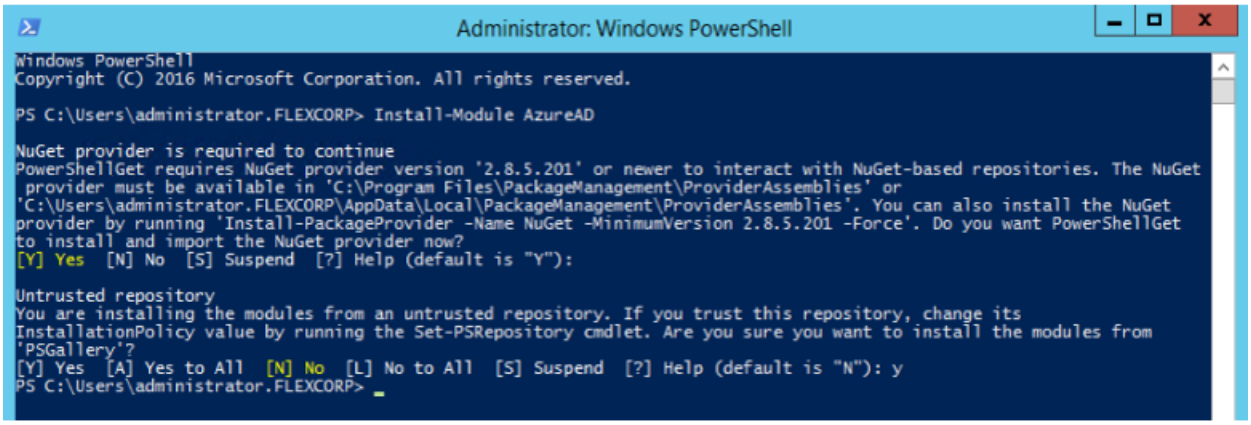
If you are prompted to install the NuGet provider, answer **Yes**.

If you receive a warning about "PSGallery" being an untrusted repository, answer **Yes** to the "Are you sure. . ." prompt.

Note: You can avoid this warning in the future by executing this cmdlet:

Set-PSRepository -Name PSGallery -InstallationPolicy Trusted

Installing Azure Active Directory Module for Windows PowerShell



Install Skype for Business Online, Windows PowerShell Module

1. Download the installers for:
   - KB2919442 (`Windows8.1-KB2919442-x64.msu`)
   - KB2919355 (`Windows8.1-KB2919355-x64.msu`)
   - .NET Framework 4.7 (`NDP47-KB3186500-Web.exe`)
   - Skype for Business Online, Windows PowerShell Module (`SkypeOnlinePowershell.exe`)

   from the links provided in *Required Management Software and Prerequisites* and copy them to the PS Proxy.
2. Install KB2919442 by double-clicking the installer `Windows8.1-KB2919442-x64.msu` and following the on-screen instructions.
3. Install KB2919355 by double-clicking the installer `Windows8.1-KB2919355-x64.msu` and following the on-screen instructions. Restart the computer when the installation is complete.
4. Install .NET Framework 4.7 by double-clicking the installer `NDP47-KB3186500-Web.exe` and following the on-screen instructions.
5. Install Skype for Business Online, PowerShell Module by double-clicking the installer `SkypeOnlinePowershell.exe` and following the on-screen instructions.

24.4.6. Domain Service Account

Domain Service Account Overview

We have the option of designating a separate service account for each application. We could also have designated one account for on-premises applications (Skype for Business Server and Exchange Server) and a different one for online services (Office 365, Skype for Business Online, and Exchange Online).

You can mix and match service accounts in any way that makes sense for your organization.

For this example, we will use a single domain service account for managing all of the on-premises and online applications.

Create the Domain Service Account

There are various ways of creating a domain account in Active Directory.

For the purposes of this example we will use the **Active Directory Users and Computers Management** console. You may have a specific Organizational Unit (OU) for service accounts. For this installation we will simply put the service account in the built-in **Users OU**.

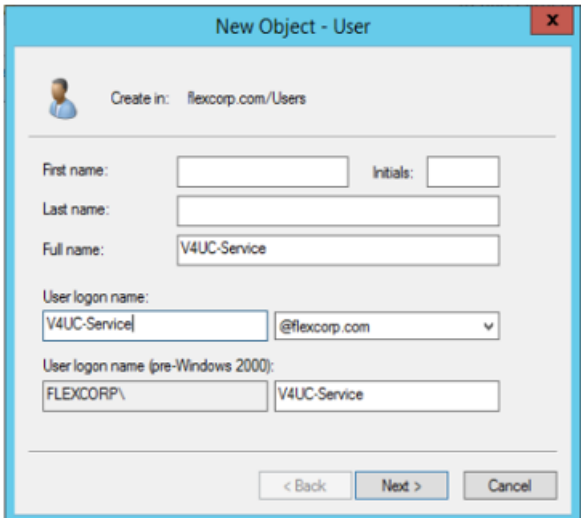
Note: To execute this procedure you must be a domain administrator.

---

1. Choose **Users** OU in the navigation pane of the **Active Directory Users and Computers Management** window.
2. Right-click **Users** and choose **New User** to open the **New Object - User** dialog.
3. Type “V4UC-Service” in the **Full name** and **User logon name** text boxes.

4. Choose the required domain from the drop-down, and click **Next**.

   Create New Service Account



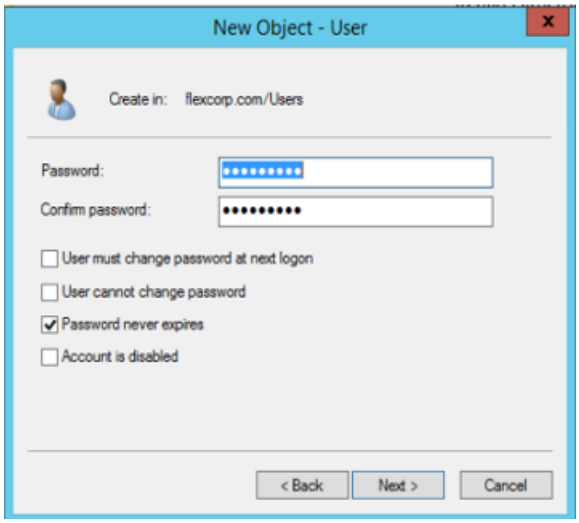
5. Enter and confirm your password, making sure that the password complies with your Provider's password standards for the Windows domain.
6. Clear the **User must change password at next logon** check box.
7. Select the **Password never expires** check box.

Note: Your organization's policy may require periodically changing service account passwords. If that is the case, be sure and change the password in VOSS-4-UC at the same time. See the "Provision VOSS-4-UC" section.

---

8. Click **Next**, and then click **Finish**.

Service Account Security Settings



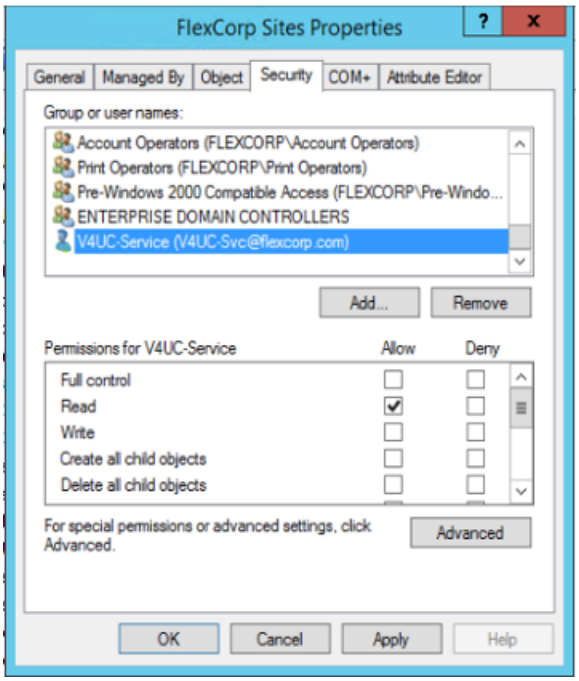
Add Service Account to On-Premises Security Groups

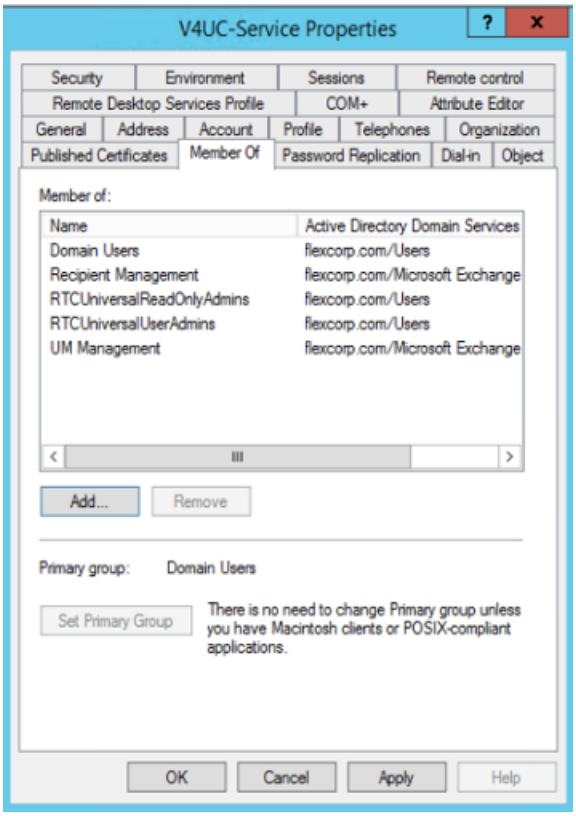
We need to give this account permission to manage Skype for Business Server users and Exchange mailboxes. To do this we will add it to the specific security groups that enable this access.

1. Right-click the service account in the details pane of the **Active Directory Users and Computers Management** console and choose **Properties** from the context menu.
2. Click the **Member Of** tab.
3. Click **Add** and enter the following group names separated by semicolons:

   `RTCUniversalServerAdmins`, `Recipient Management`, and `UM Management`.
4. Click **OK** twice.

Domain Service Account Security Group Membership





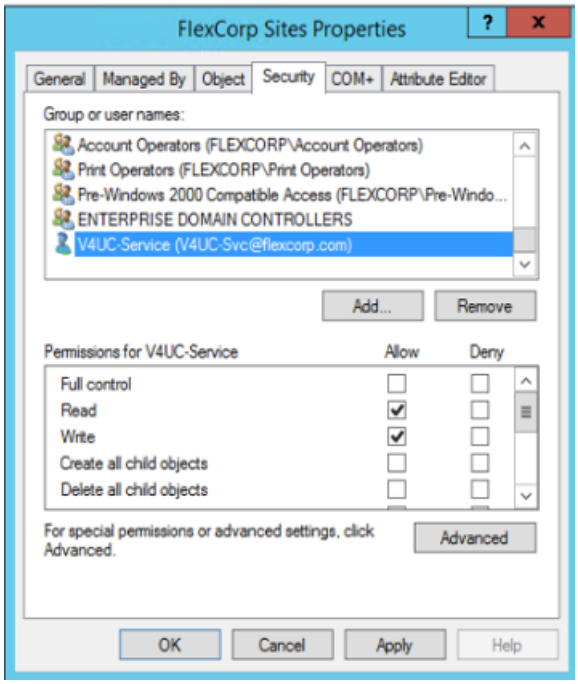
Grant Access to the Users' OU

By default all domain users have read access to user information in Active Directory. We need to give this service account the additional permission to update AD user and contact objects. This is accomplished by modifying specific ACLs in Active Directory.

In our example, all our users are in the Organization Unit called `FlexCorp Sites`. This OU contains multiple sub-units, each of which can contain user and contact objects. We will use the **Active Directory Users and Computers Management** console to modify the ACL of the FlexCorp Sites Organizational Unit.

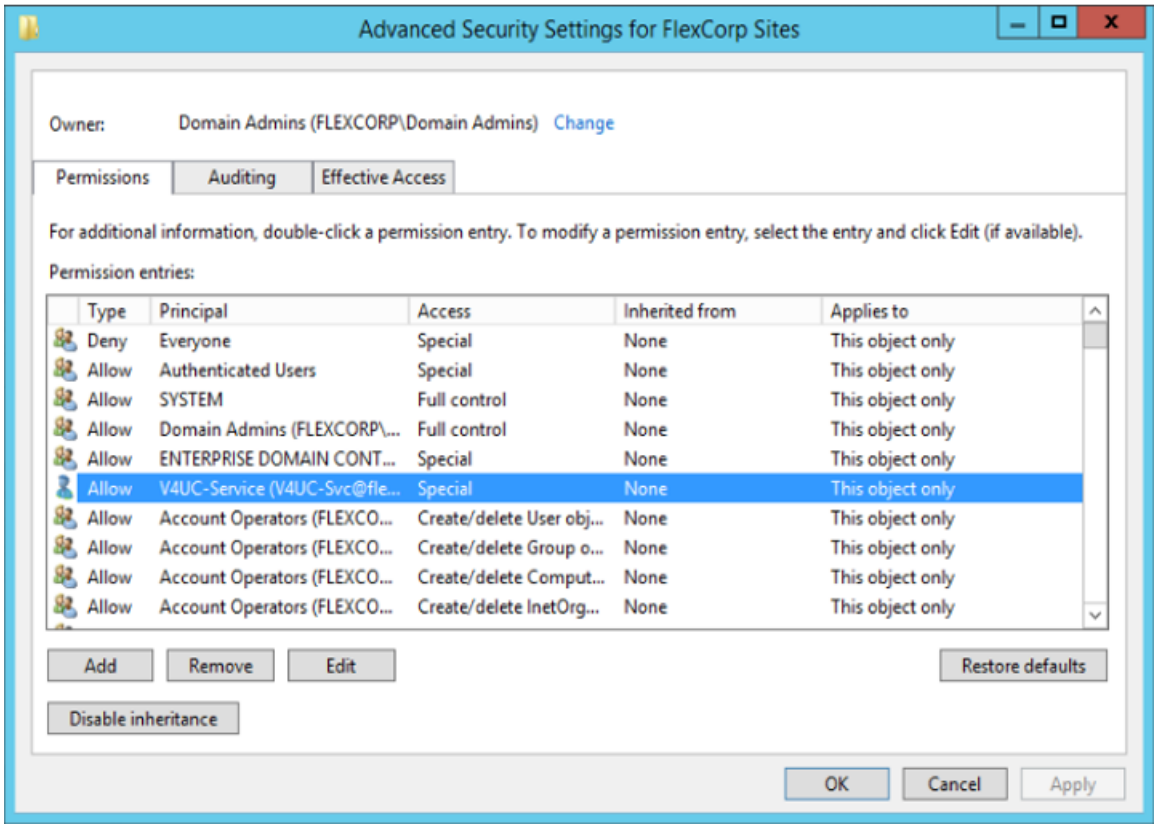
1. Navigate to the FlexCorp Sites in the navigation pane.
2. Right-click **FlexCorp Sites** and choose **Properties** from the context menu.
3. Click the **Security** tab and click **Add...**.
4. Enter the name of your service account in the **Enter the object names to select** text box and click **OK**.
5. Select the **Write** check box and confirm that the **Read** check box is already selected In the **Allow** column .

   Organizational Unit Security Tab



6. Click **Advanced** to open the **Advanced Security Settings for FlexCorp Sites** dialog.
7. Click the **Permissions** tab, then choose the **V4UC-Service** account and click **Edit**.

   Service Account Advanced Security Settings

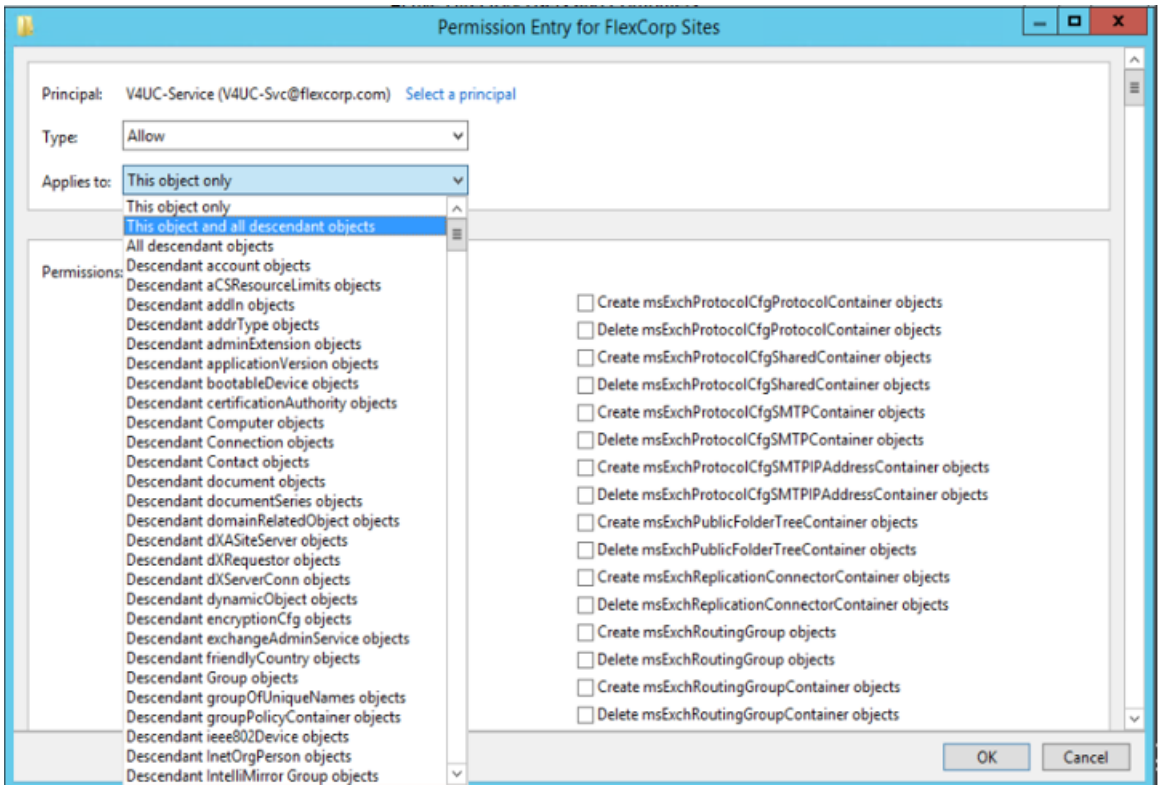


8. Choose the **This object and all descendant objects** option from the drop-down list in the **Applies to**

column.

9. Click **OK** three times.

   Service Account Permission Entry

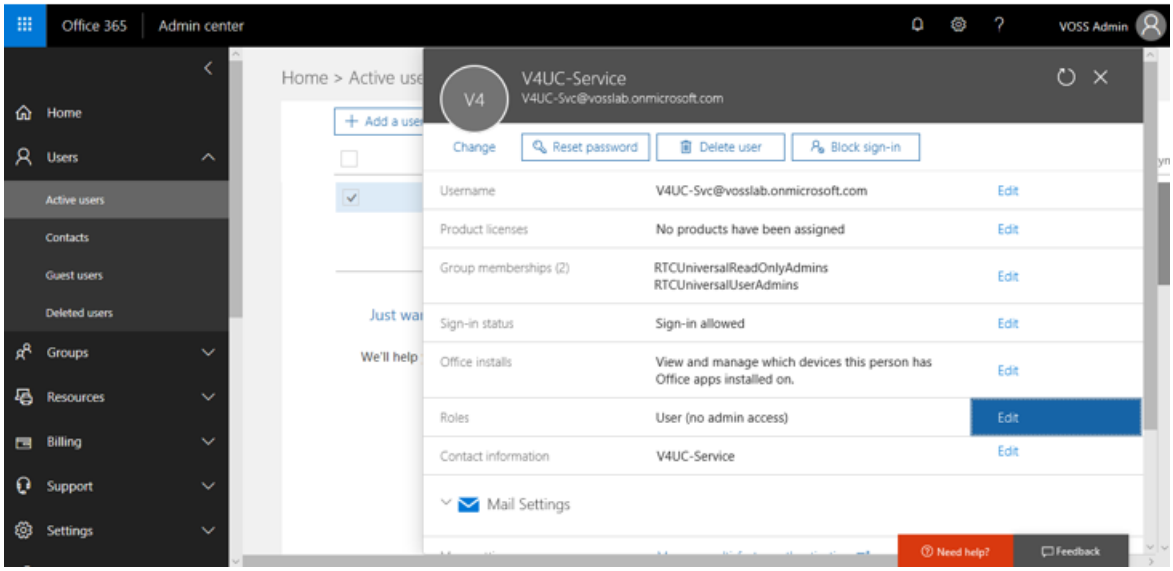


Enable Skype for Business Online Administration

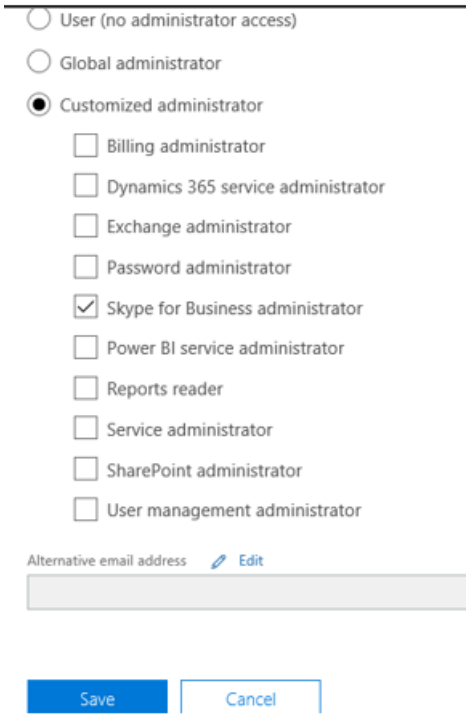
Now we'll enable the service account to manage Skype for Business Online users.

1. Browse to https://portal.office.com, and sign in with administrative credentials.
2. Navigate to the **Office 365 Admin Center**.
3. Locate and select the service account, on the **Active Users** page to display the user's property sheet.

   Service Account Office 365 Properties



4. Click **Edit** in the **Roles** row.
5. Choose the **Customized administrator** radio button, and then select the **Skype for Business administrator** check box.
6. Click the **Save** button, and then click **Close**.



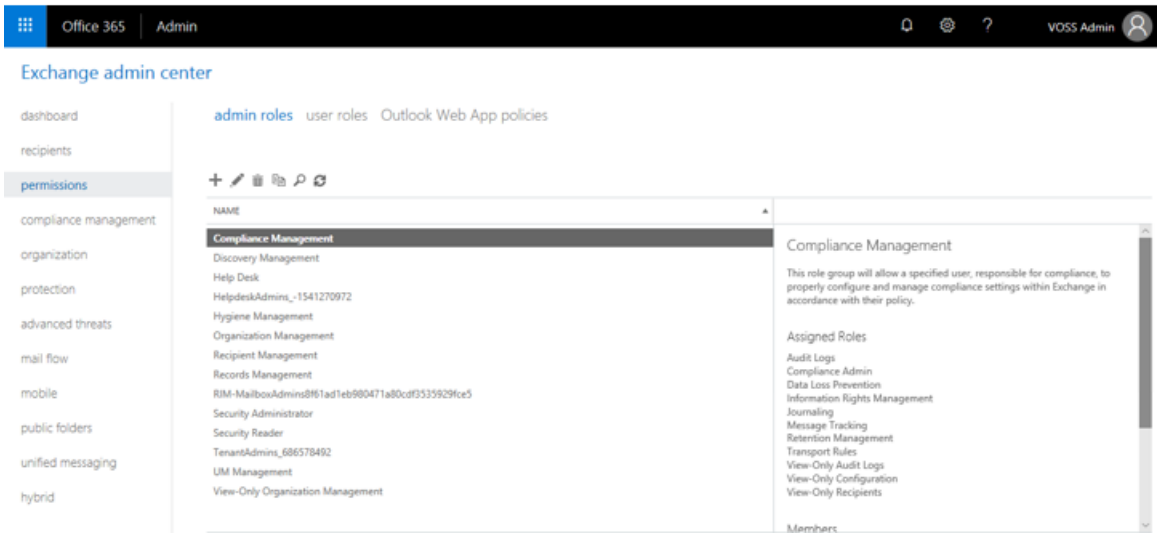
Create Exchange Online Custom Role Group

To assign the least privileges necessary for VOSS-4-UC to manage your Exchange Online mailboxes you will need to create a custom role group in Exchange Online. These steps will walk you through that process.

1. Browse to https://portal.office.com, and sign in with administrative credentials.

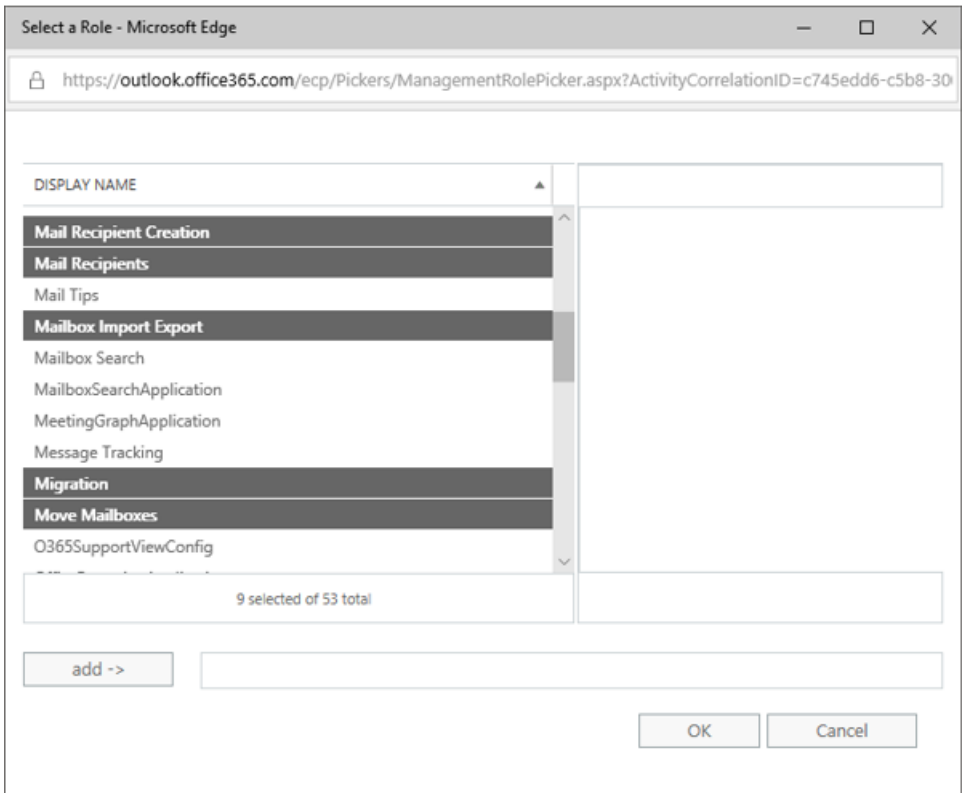
2. Navigate to the **Office 365 Admin Center**.
3. Navigate to the **Exchange Admin Center** and choose **permissions** from the navigation pane.
4. Choose the **admin roles** option at the top of the screen.

   Exchange Online Admin Roles page



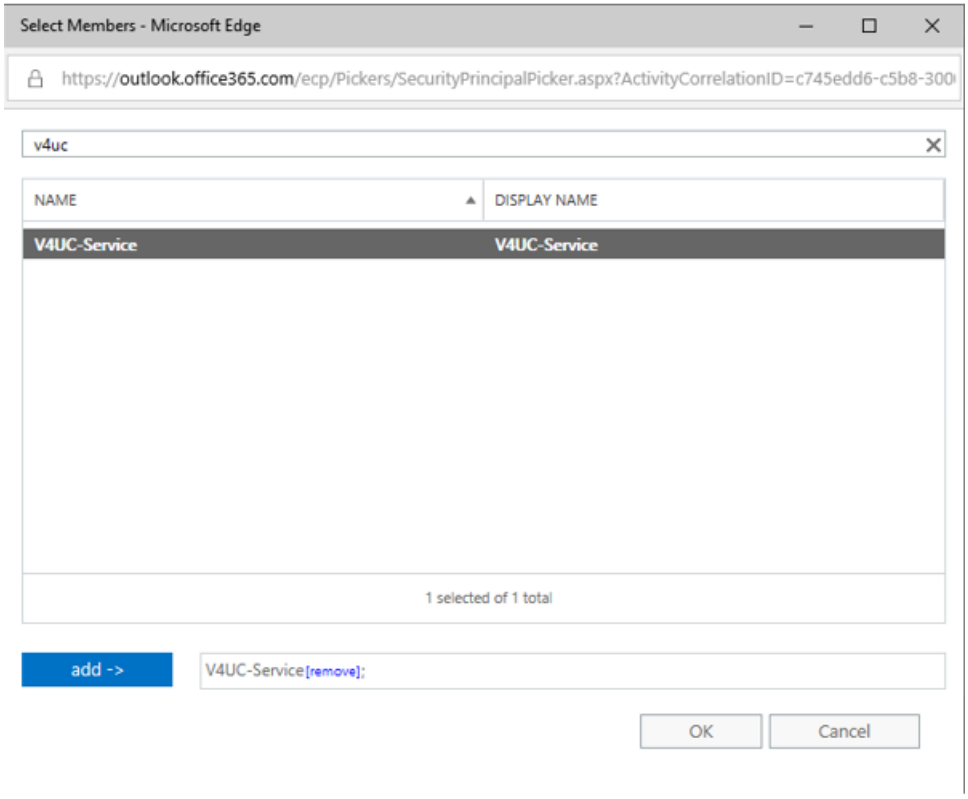
5. Click the **+** icon to add a new role group.
6. Enter a group **Name** and an optional **Description**. Leave the **Write scope** as **Default**.
7. Click the **+** icon under **Roles** to add the following roles. **Ctrl + left mouse click** to select multiple roles. Click **OK** when complete:
   - Address Lists
   - Mail Recipient Creation
   - Mail Recipients
   - Mailbox Import Export
   - Migration
   - Move Mailboxes
   - Reset Password
   - SendMailApplication
   - UM Mailboxes

   Exchange Online Role Group - Role Selection



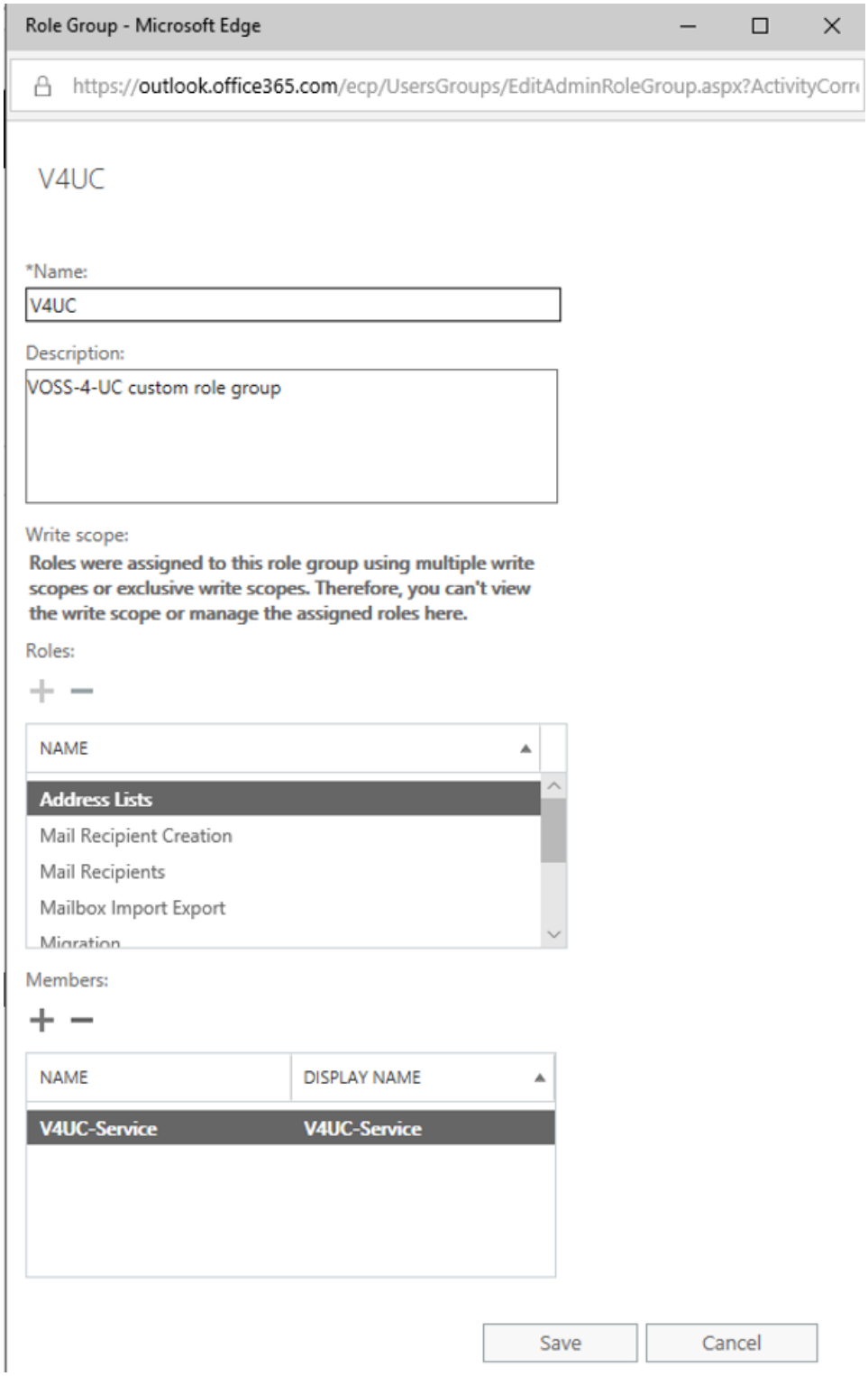
8. Click the **+** icon on the **new role group** sheet, under **Members:** to add the service account to this group.
9. Choose the service account from the list of user accounts, click **Add ->**, and then click **OK**.

   Exchange Online Role Group - Add Members



10. Click **Save** on the new role group sheet.

    Exchange Online Role Group



Add to PS Proxy local administrators group

Repeat these steps on all PS Proxies in your deployment. In this lab we have two PS Proxies, and will complete these steps on both of them.

1. On the PS Proxy launch `lusrmgr.msc`.
2. Choose **Groups** from the navigation pane, right-click **Administrators** and then choose **Properties** from the context menu.
3. Click **Add...**.
4. Enter the name of your domain service account in the **Enter the object names to select** text box. If you have more than one domain service account using this PS Proxy, enter all of them, separated by semicolons.
5. Click **OK** twice.

24.4.7. Example: Provision VOSS-4-UC

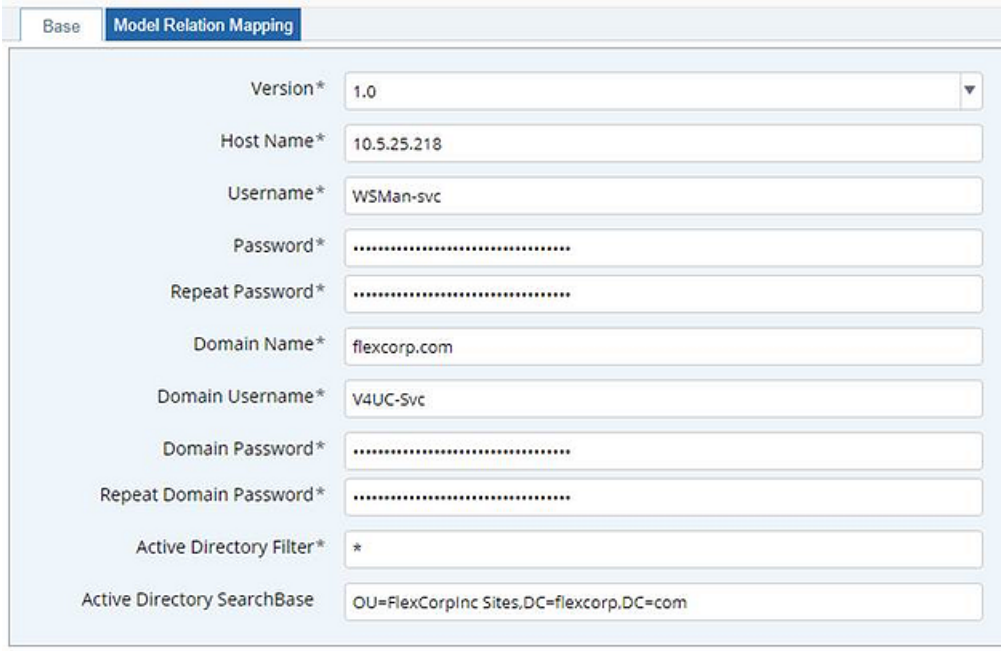
Provision VOSS-4-UC Workflow

1. Sign into VOSS-4-UC as an administrator at a hierarchy level at or above where you will be adding the Microsoft devices. You can add Microsoft devices at the customer level, the provider level, or at any intermediate node above customer.
2. Open the **Device Management** menu.

Active Directory

1. Choose **Active Directory** from the Device Management menu.
2. Choose **AD Server** and click **Add**.

Active Directory Server Configuration Page



3. Enter the following values on the **Base** tab:

   Sample Active Directory Configuration Parameters

Parameter	Example Value	Comments
Version	`1.0`	This is the only version currently supported
Host Name	`10.5.25.240`	The IP address of the PS Proxy handling Active Directory connections. We could have also entered `psproxy01.flexcorp.com`, which is the FQDN of that proxy.
Username	`WSMan-svc`	The local service account that we created in the Remote Management Service Account section.[1]
Password / Repeat		The local service account's password.
Domain Name	`flexcorp.com`	The domain portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[2]
Domain Username	`V4UC-Svc`	The user name portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[3]
Domain Password / Repeat		The domain service account's password.
Active Directory Filter	`*`	We will use a simple wildcard that filters nothing - all results are returned.
Active Directory Search-Base	`OU=FlexCorp Sites, DC=flexcorp, DC=com`	This is the Distinguished Name of the Organizational Unit containing the users and contacts that VOSS-4-UC will manage. Note that this is the OU for which we granted write privileges to the domain service account in the Grant Access to the Users' OU section.

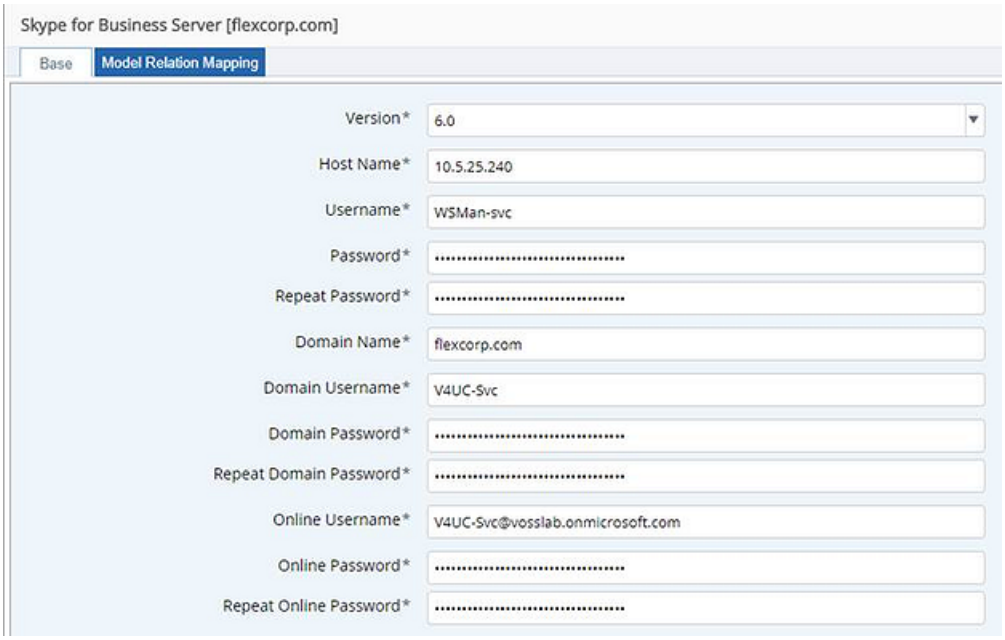
4. Choose **Test Connection** from the **Action** menu.
5. Check the transaction log and confirm that the test was successful.

Skype for Business Server

1. Choose **Skype for Business** from the **Device Management** menu.
2. Choose the **Skype for Business Server** and click **Add**.

Skype for Business Server Configuration Page

[1] See: *Remote Management Service Account*
[2] See: *Create the Domain Service Account*
[3] See: *Create the Domain Service Account*



3. Enter the following values on the **Base** tab:

   Sample Skype for Business Server Configuration Parameters

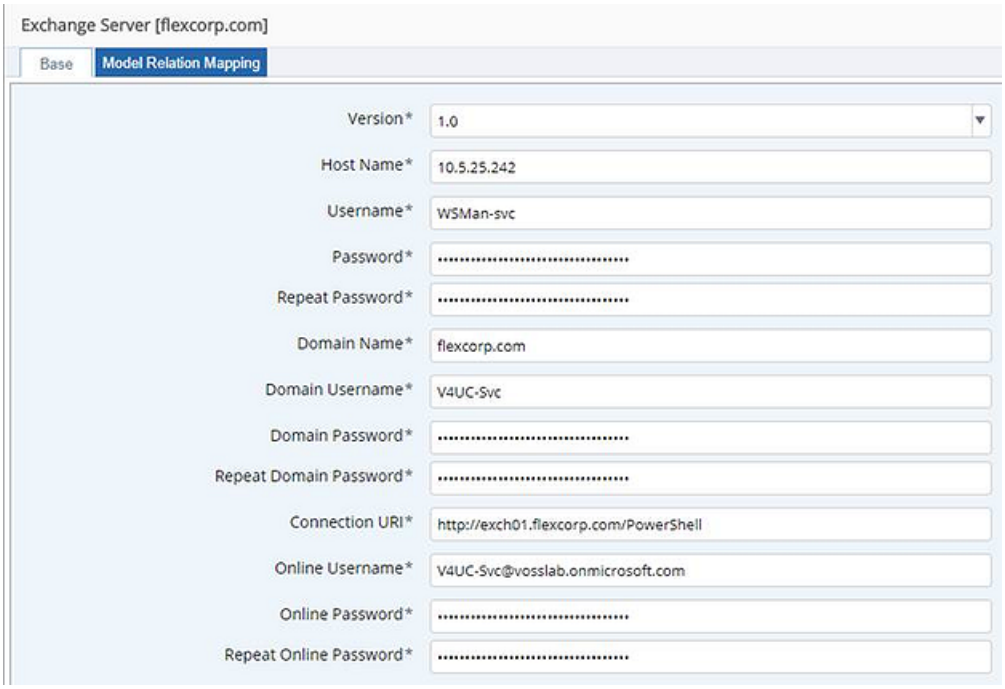
Parameter	Example Value	Comments
Version	`6.0`	This is the only version currently supported
Host Name	`10.5.25.240`	The IP address of the PS Proxy handling Skype for Business Server connections. We could have also entered `psproxy01.flexcorp.com`, which is the FQDN of that proxy.
Username	`WSMan-svc`	The local service account that we created in the Remote Management Service Account section.[1]
Password / Repeat		The local service account's password.
Domain Name	`flexcorp.com`	The domain portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[2]
Domain Username	`V4UC-Svc`	The user name portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[3]
Domain Password / Repeat		The domain service account's password.
Online Username	`V4UC-Svc@vosslab.onmicrosoft.com`	The username of the domain service account as it appears in the Office 365 Admin Center.
Online Password / Repeat		The password for the online service account. This will be the same as "Domain Password", above.

4. Choose **Test Connection** from the **Action** menu.
5. Check the transaction log and confirm that the test was successful.

Exchange Server

1. Choose **Exchange** from the **Device Management** menu.
2. Choose **Exchange Server** and click **Add**.

Exchange Server Configuration Page



3. Enter the following values on the **Base** tab:

Sample Exchange Server Configuration Parameters

[1] See: *Remote Management Service Account*
[2] See: *Create the Domain Service Account*
[3] See: *Create the Domain Service Account*

Parameter	Example Value	Comments
Version	`1.0`	This is the only version currently supported
Host Name	`10.5.25.240`	The IP address of the PS Proxy handling Exchange Server connections. We could have also entered `psproxy01.flexcorp.com`, which is the FQDN of that proxy.
Username	`WSMan-svc`	The local service account that we created in the Remote Management Service Account section.[1]
Password / Repeat		The local service account's password.
Domain Name	`flexcorp.com`	The domain portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[2]
Domain Username	`V4UC-Svc`	The user name portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[3]
Domain Password / Repeat		The domain service account's password.
Connection URI	`http://exch01.flexcorp.com/PowerShell`	The URI starts with the FQDN of an on-premises Exchange server that hosts the Exchange Admin Center.
Online Username	`V4UC-Svc@vosslabonmicrosoft.com`	The username of the domain service account as it appears in the Office 365 Admin Center.
Online Password / Repeat		The password for the online service account. This will be the same as "Domain Password", above.

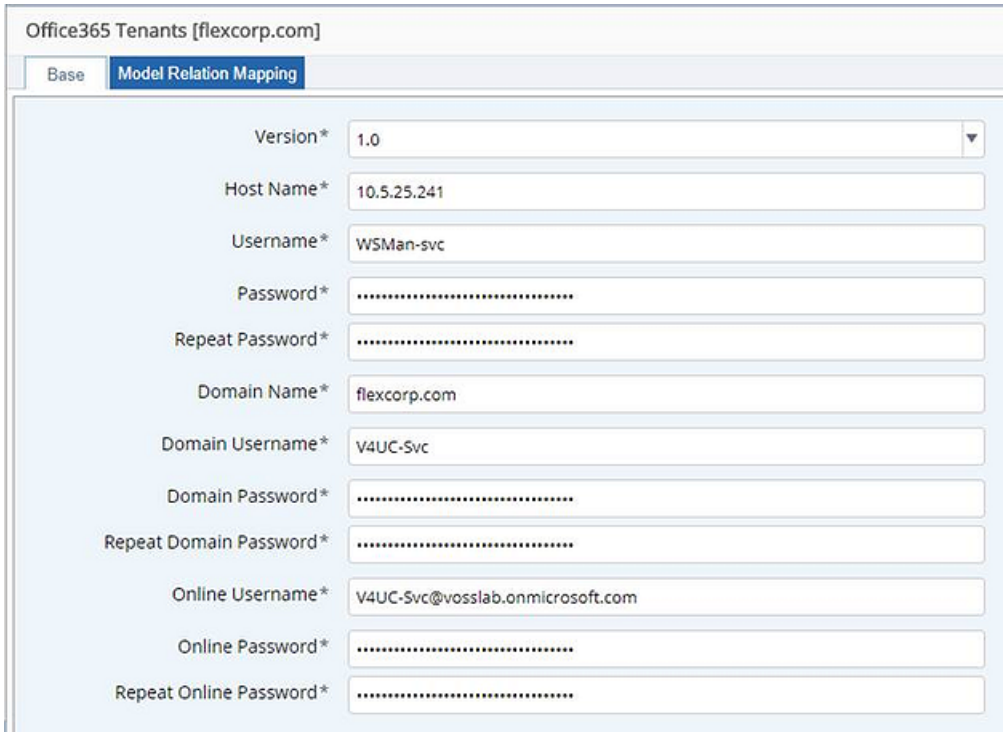
4. Choose **Test Connection** from the **Action** menu.
5. Check the transaction log and confirm that the test was successful.

Microsoft Online

1. Choose **Microsoft Online** from the **Device Management** menu.
2. Choose **Office365 Tenants** and click **Add**.

Microsoft Online (Office 365 Tenant) Configuration Page

[1] See: *Remote Management Service Account*
[2] See: *Create the Domain Service Account*
[3] See: *Create the Domain Service Account*



3. Enter the following values on the **Base** tab:

   Sample Microsoft Online Configuration Parameters

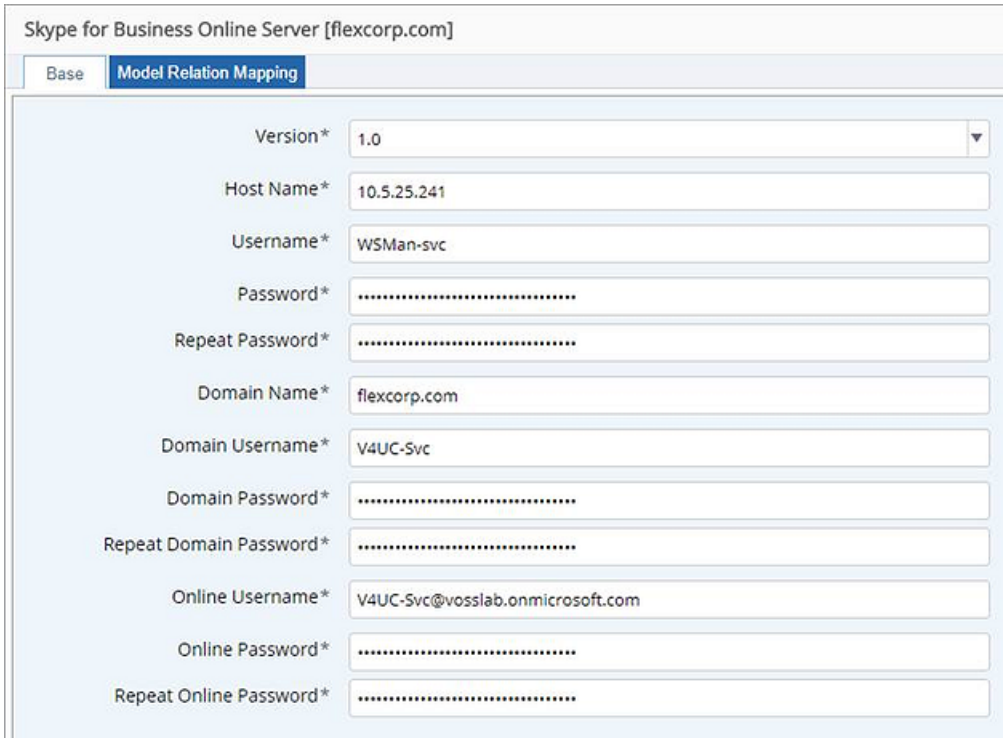
Parameter	Example Value	Comments
Version	`6.0`	This is the only version currently supported
Host Name	`10.5.25.241`	The IP address of the PS Proxy handling Office 365 connections. We could have also entered `psproxy02.flexcorp.com`, which is the FQDN of that proxy.
Username	`WSMan-svc`	The local service account that we created in the Remote Management Service Account section.[1]
Password / Repeat		The local service account's password.
Domain Name	`flexcorp.com`	The domain portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[2]
Domain Username	`V4UC-Svc`	The user name portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[3]
Domain Password / Repeat		The domain service account's password.
Online Username	`V4UC-Svc@vosslab.onmicrosoft.com`	The username of the domain service account as it appears in the Office 365 Admin Center.
Online Password / Repeat		The password for the online service account. This will be the same as "Domain Password", above.

4. Choose **Test Connection** from the **Action** menu.
5. Check the transaction log and confirm that the test was successful.

Skype for Business Online

1. Choose **Skype for Business Online** from the **Device Management** menu.
2. Choose **Skype for Business Online Server** and click **Add**.

Skype for Business Online Configuration Page



3. Enter the following values on the **Base** tab:

Sample Skype for Business Online Configuration Parameters

[1] See: *Remote Management Service Account*
[2] See: *Create the Domain Service Account*
[3] See: *Create the Domain Service Account*

Parameter	Example Value	Comments
Version	`1.0`	This is the only version currently supported
Host Name	`10.5.25.241`	The IP address of the PS Proxy handling Skype for Business Online connections. We could have also entered `psproxy02.flexcorp.com`, which is the FQDN of that proxy.
Username	`WSMan-svc`	The local service account that we created in the Remote Management Service Account section.[1]
Password / Repeat		The local service account's password.
Domain Name	`flexcorp.com`	The domain portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[2]
Domain Username	`V4UC-Svc`	The user name portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[3]
Domain Password / Repeat		The domain service account's password.
Online Username	`V4UC-Svc@vosslab onmicrosoft.com`	The username of the domain service account as it appears in the Office 365 Admin Center.
Online Password / Repeat		The password for the online service account. This will be the same as "Domain Password", above.

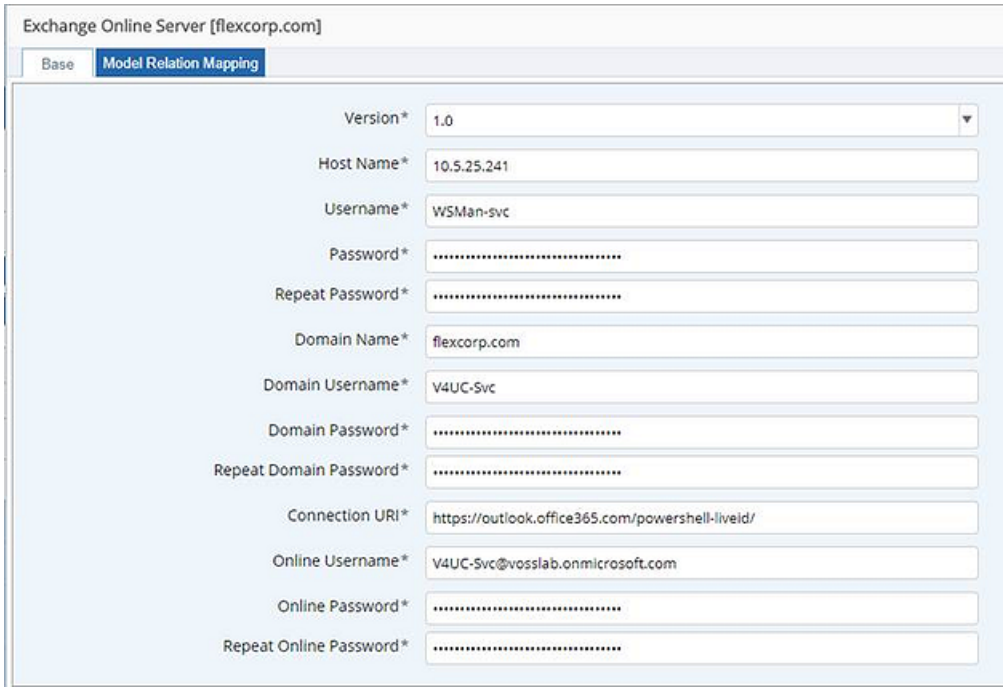
4. Choose **Test Connection** from the **Action** menu.
5. Check the transaction log and confirm that the test was successful.

Exchange Online

1. Choose **Exchange Online** from the **Device Management** menu.
2. Choose **Exchange Online Server** and click **Add**.

Exchange Online Configuration Page

[1] See: *Remote Management Service Account*
[2] See: *Create the Domain Service Account*
[3] See: *Create the Domain Service Account*



3. Enter the following values on the **Base** tab:

   Sample Exchange Online Configuration Parameters

Parameter	Example Value	Comments
Version	`1.0`	This is the only version currently supported
Host Name	`10.5.25.241`	The IP address of the PS Proxy handling Exchange Online connections. We could have also entered `psproxy02.flexcorp.com`, which is the FQDN of that proxy.
Username	`WSMan-svc`	The local service account that we created in the Remote Management Service Account section.[1]
Password / Repeat		The local service account's password.
Domain Name	`flexcorp.com`	The domain portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[2]
Domain Username	`V4UC-Svc`	The user name portion of the domain service account's account name. We created this account in the Create the Domain Service Account section.[3]
Domain Password / Repeat		The domain service account's password.
Connection URI	`https://outlook.office365.com/powershell-liveid/`	Use this URI literally - it is the same for all Office 365 tenants.
Online Username	`V4UC-Svc@vosslab.onmicrosoft.com`	The username of the domain service account as it appears in the Office 365 Admin Center.
Online Password / Repeat		The password for the online service account. This will be the same as "Domain Password", above.

4. Choose **Test Connection** from the **Action** menu.
5. Check the transaction log and confirm that the test was successful.

[1] See: *Remote Management Service Account*
[2] See: *Create the Domain Service Account*
[3] See: *Create the Domain Service Account*

25 Appendix: Business Admin Portal Configuration

25.1. Business Admin Portal Configuration Overview

In VOSS-4-UC version 19.1.1 (or higher), a number of mechanisms are introduced to allow the Business Admin Portal (BAP) to be customized for different customers and even different roles within an organization.

The following aspects of the portal can be customized

- Role based access control (see: *Business Admin Portal Profiles*)
  - Access to features (menu items)
  - Access to MACDs / Day 2 functions
  - Access to dashboard widgets (charts etc.)
- Look and feel (see: *Custom Business Admin Themes and Branding*)
  - Branding / theming
  - Field visibility, order, title and help text
- Configuration Templates
  - Subscriber Profiles (service profiles) (see: *Subscriber Profiles*)
  - Available phone types with related configuration (see: *Phone Configuration Mapping*)
  - Line templates
- User level customization
  - Saved searches
  - UI user preferences

For all of the above, default profiles and templates have been created and will be added to the system during an upgrade to 19.1.1 (or higher).

In previous versions of VOSS-4-UC, BAP was disabled by default and needed to be enabled. In 19.1.1 (or higher) however, BAP will be enabled by default and must specifically be disabled if so required.

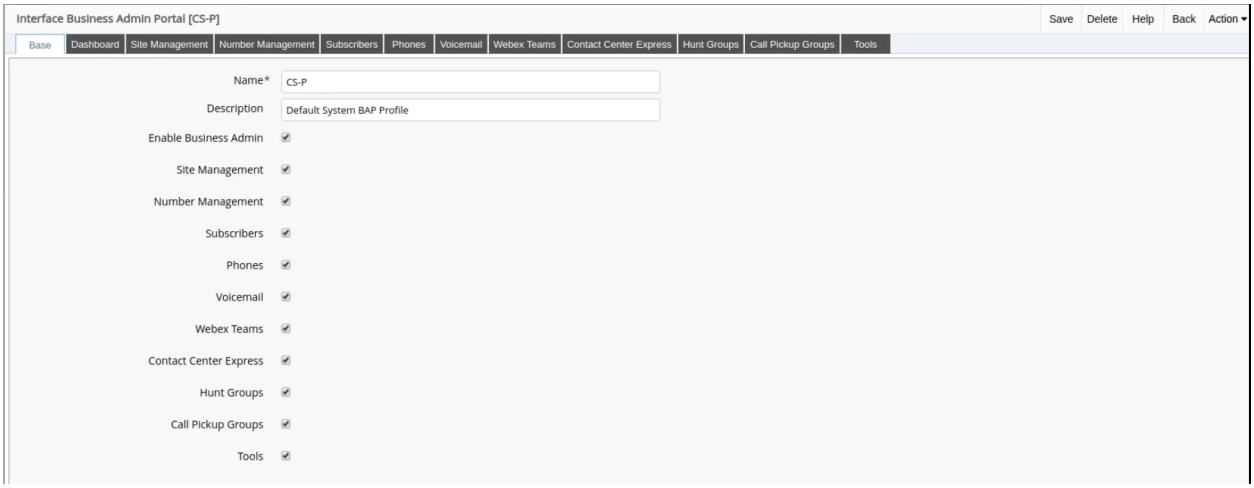
It is important that the defaults are reviewed and if required, be cloned (overridden) and amended to fit the requirements of the deployment.

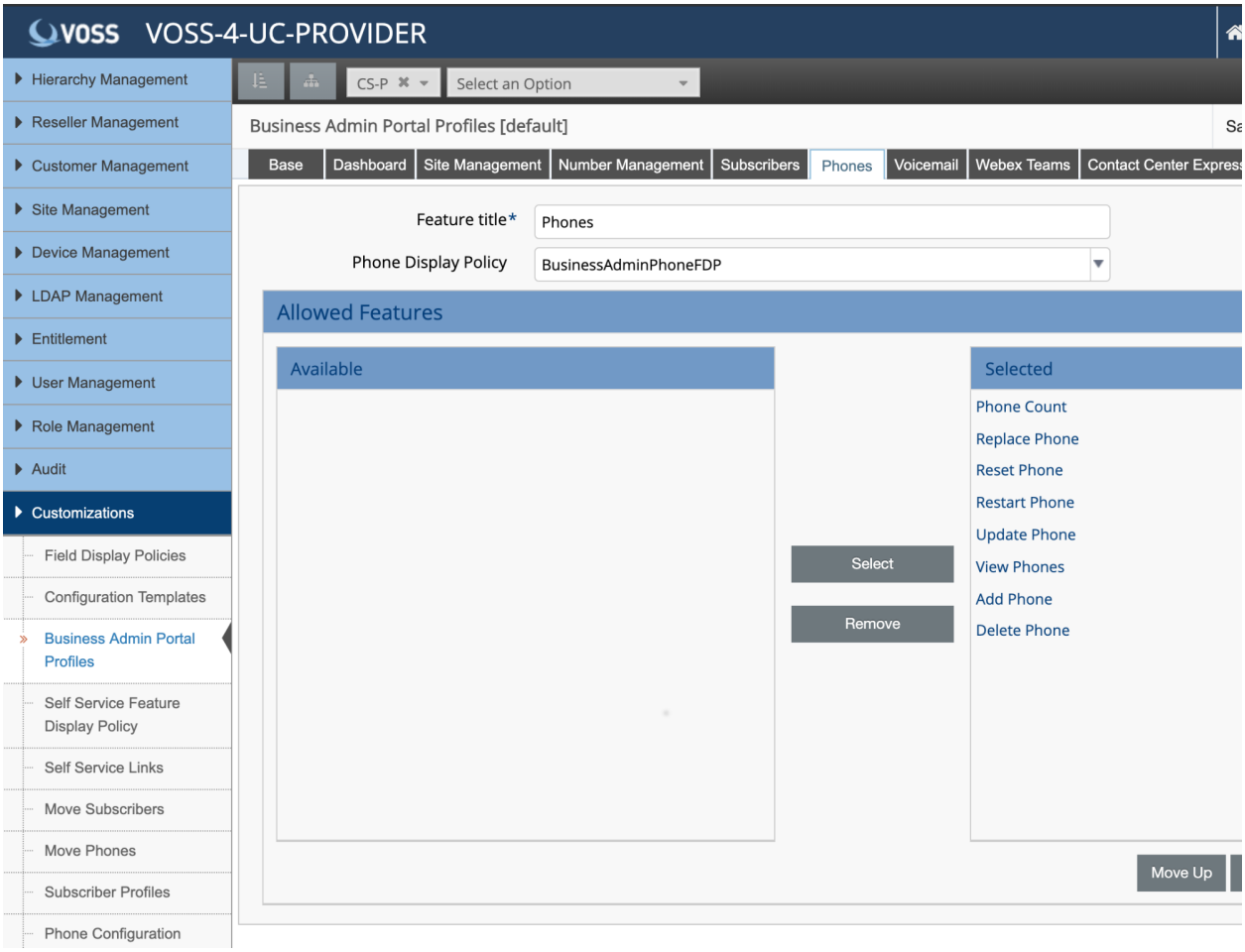
25.2. Business Admin Portal Profiles

BAP Profiles combine the controls of many of the customization aspects mentioned above into a single place.

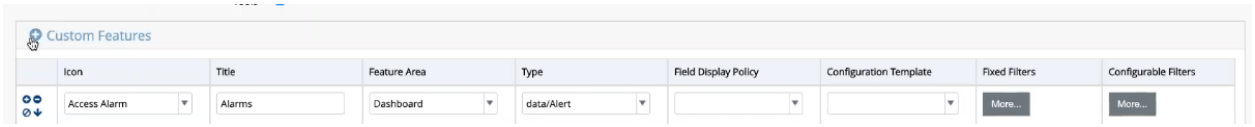
The profile allows a higher level administrator to

- enable or disable the Business Admin Portal for the target administrator user by checking / unchecking the **Enable Business Admin** checkbox on the **Base** tab
- select the features the target administrator user will have access to
- check / uncheck the checkboxes on the **Base** tab of the profile to turn features on / off
- On the **Base** tab: if custom features are needed to be added to the **Quick Actions** card for a Feature Area, use the **Custom Features** list:
  - Choose an **Icon** title. For a list icons corresponding to the titles, see *Business Admin Portal Interface Custom Icon Names Reference*.
  - Enter a title and choose the Feature Area.
  - Similar to Menu Layout configuration options, choose a model type and set up any further configuration associated with the model type. Note that the model type needs to be exposed in a user's Access Profile if the custom interface is associated with a user. Refer to the Custom Feature example image.
- change the titles that will be used for each of the enabled features
- select a custom Field Display Policy for relevant features
- select all MACDs / functions that the target administrator will have access to

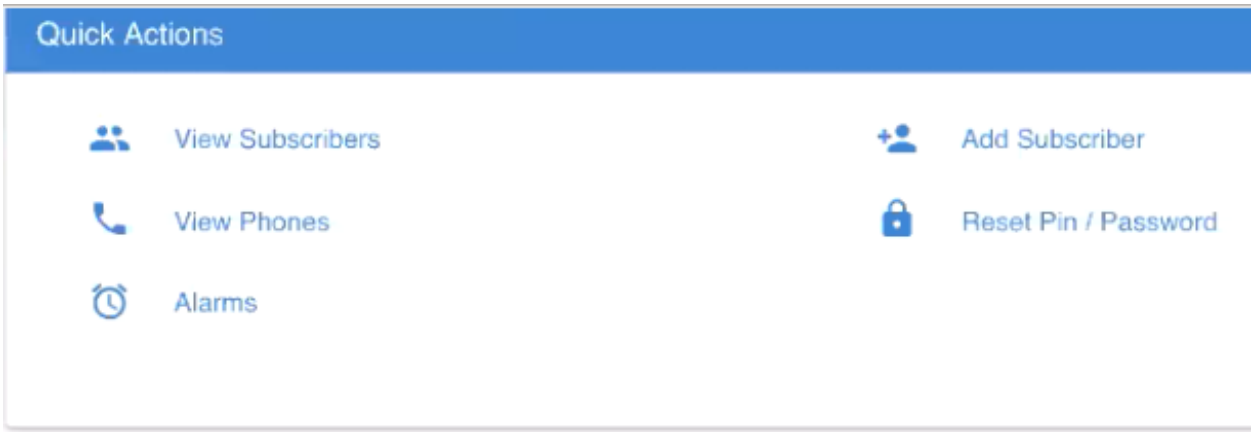




Custom Feature example:



Custom Feature example on Dashboard: Quick Action Alarms



Upon installation, the Business Admin Portal Interface Type provides the profile instances below.

When upgrading to Release 19.1.2 or higher, only the roles at the `sys.hcs` level are updated.

- `default`

  This instance is used when creating a role, in other words, it is applied to users if their role has not assigned any Business Admin Profile.

  The name “default” at the user’s hierarchy level or first level upwards is applied.

  The default profile has the following properties:

  - No access the Business Admin Portal Menus: site management, tools.
  - Only view access to data from other Business Admin Portal Menus, including example model counts and charts.

  The system level administrator can clone the instance down the hierarchy and modify it to create custom default instances of the interface type.

- `Disabled`

  Available, but not applied. Used to prevent access to the Business Admin Portal.

- `Read Only`

  This instance:

  - has the same properties as the `default` instance
  - is applied to all Operator administrator user roles by default

- `Full Access`

  This instance is a profile with full access to all Business Admin Portal Menus menus and features.

  The profile is added to the ProviderAdmin Roles upon new installation.

The Field Display Policies (FDP) associated with the `default` profile are

- `BusinessAdminPhoneFDP`
- `BusinessAdminLineFDP`
- `BusinessAdminVoicemailFDP`
- `BusinessAdminWebexTeamsUserFDP`
- `BusinessAdminUccxAgentFDP`
- `BusinessAdminUccxTeamFDP`
- `BusinessAdminUccxContactServiceQueueFDP`
- `BusinessAdminHuntGroupFDP`
- `BusinessAdminCallPickupGroupFDP`

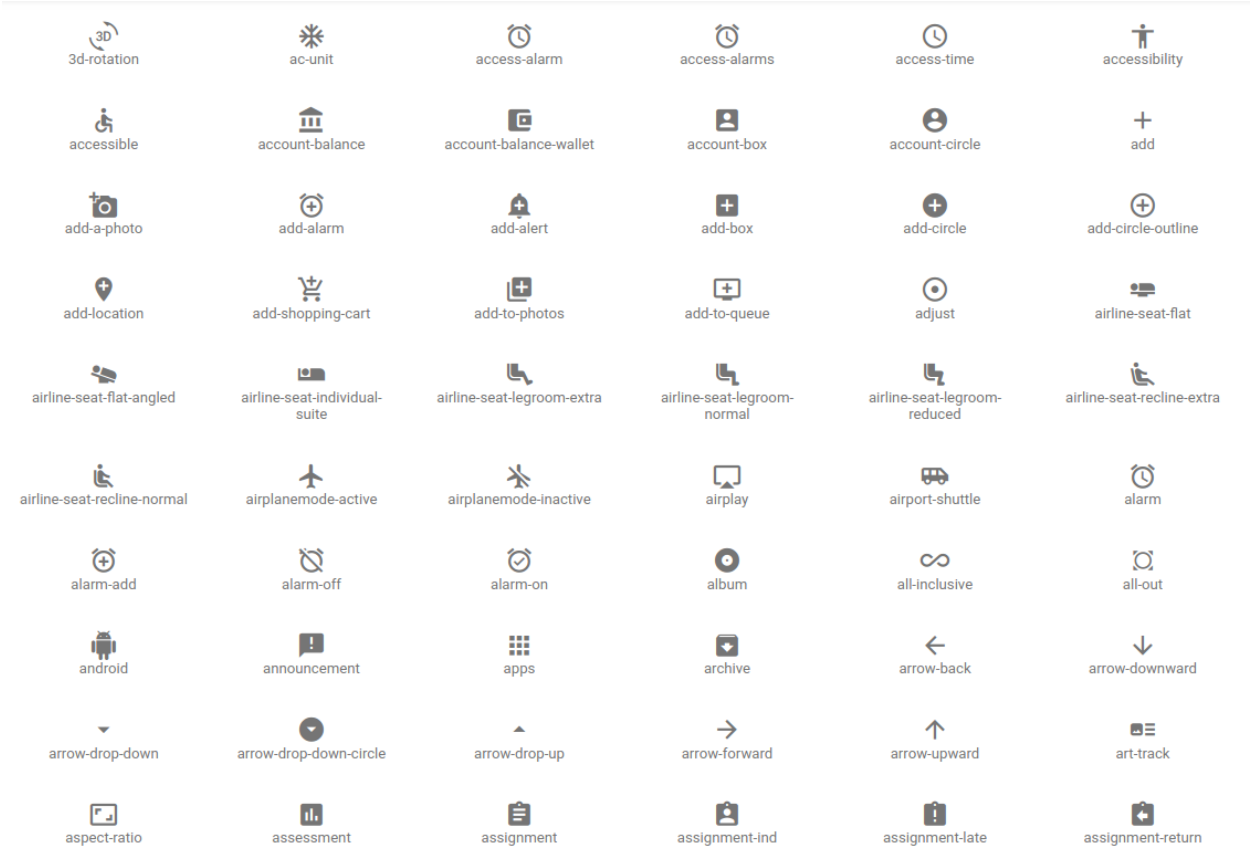
These can be cloned and overridden or custom FDPs can also be configured on the BAP profile.

25.3. Business Admin Portal Interface Custom Icon Names Reference

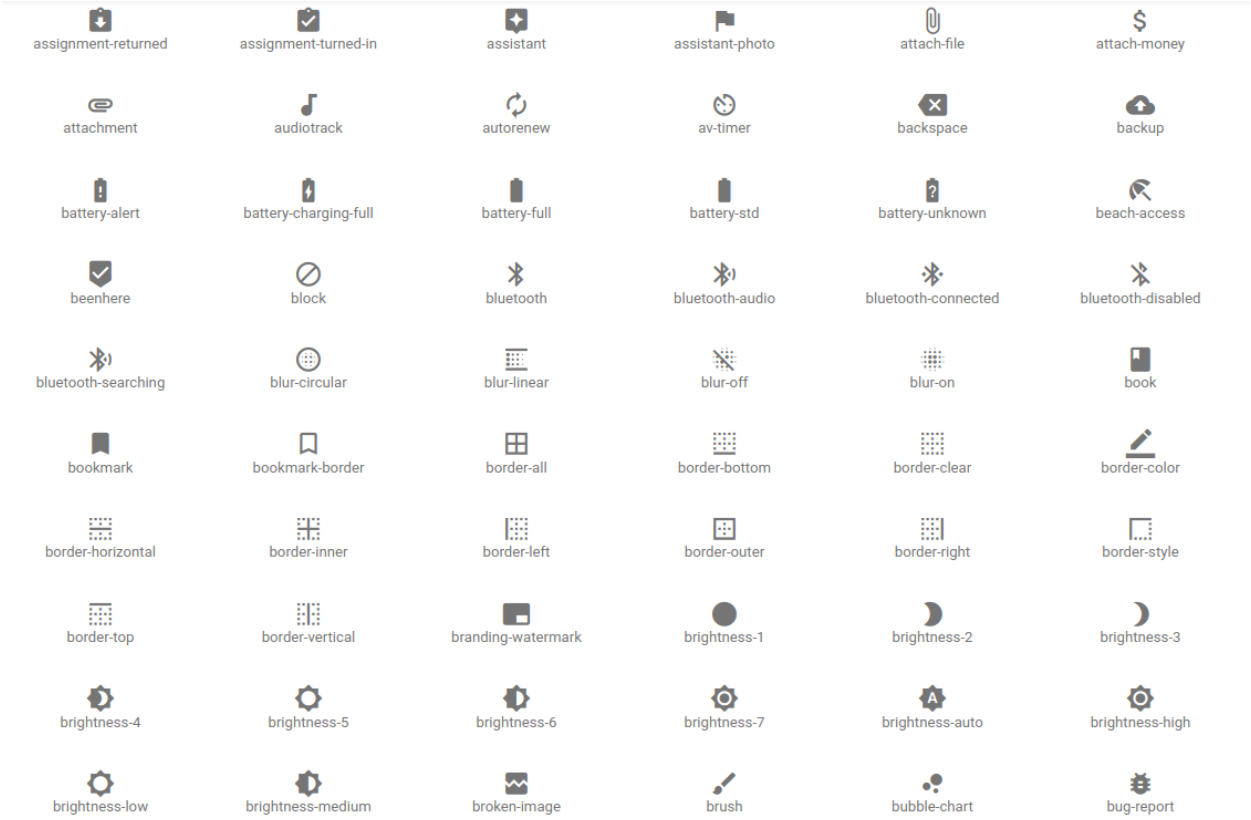
This reference shows the icons associated with the **Icon** name drop-down on the **Custom Features** input list of the **Business Admin Portal Interface**. See: *Business Admin Portal Custom Interface*.

To associate the icon of the in the drop-down, inspect the titles below, remove the title hyphens and capitalize the first letter of each word. The section headings below show the first and last icon names in each section.

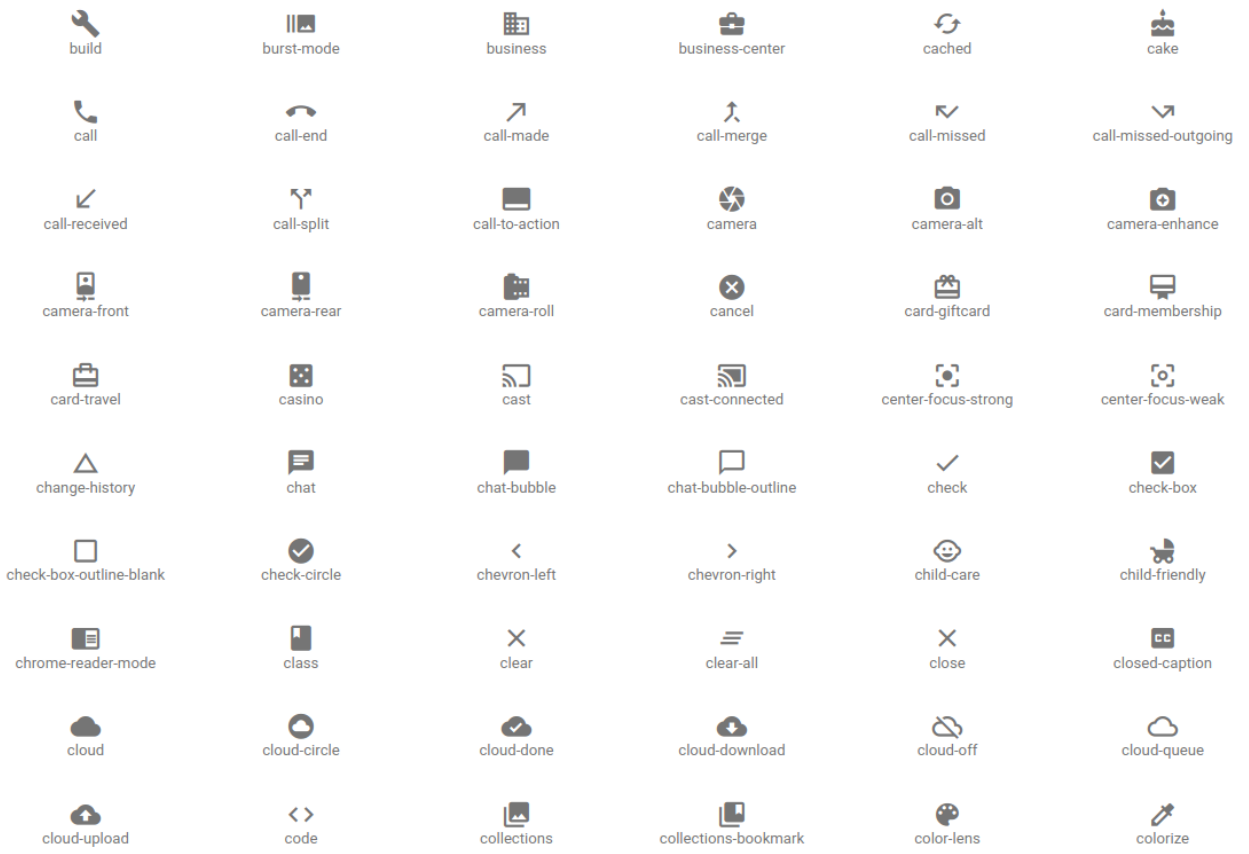
25.3.1. “3d Rotation” to “Assignment Return”



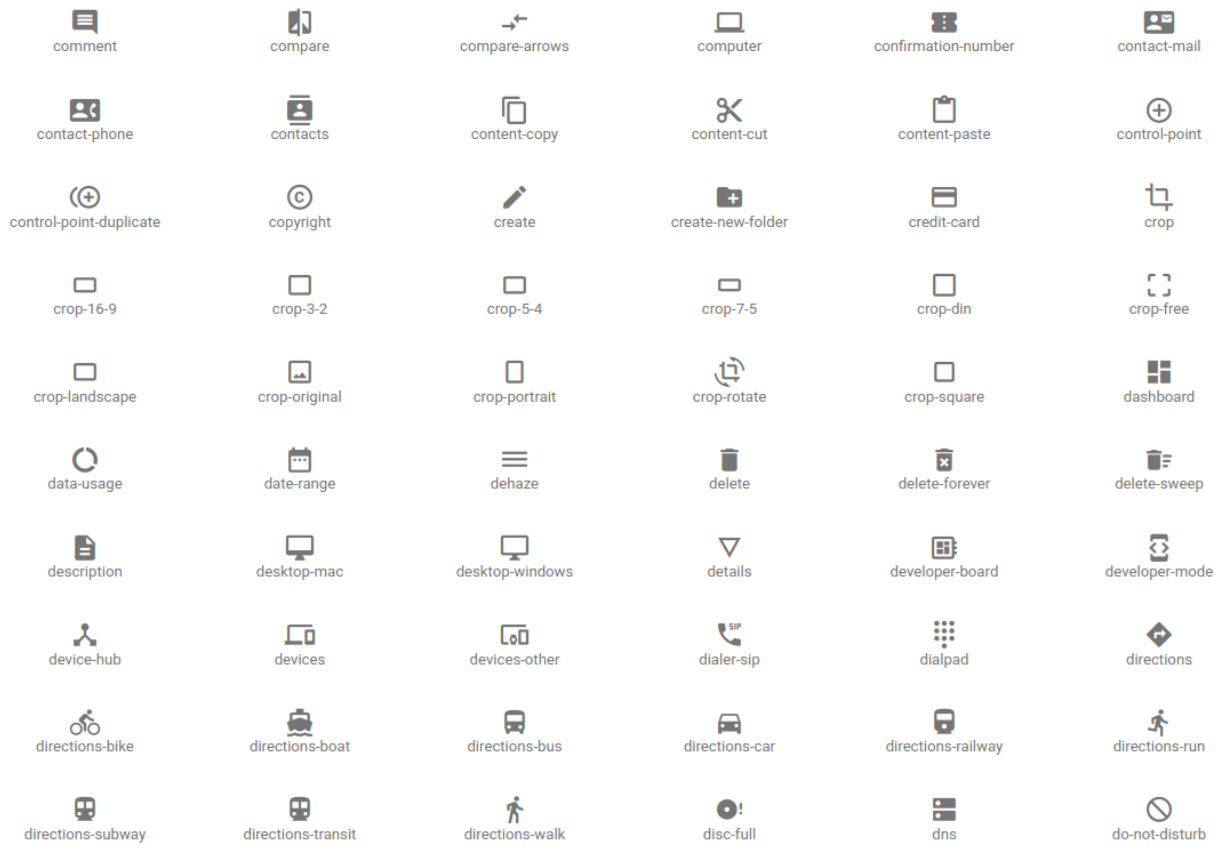
25.3.2. “Assignment Returned” to “Bug Report”



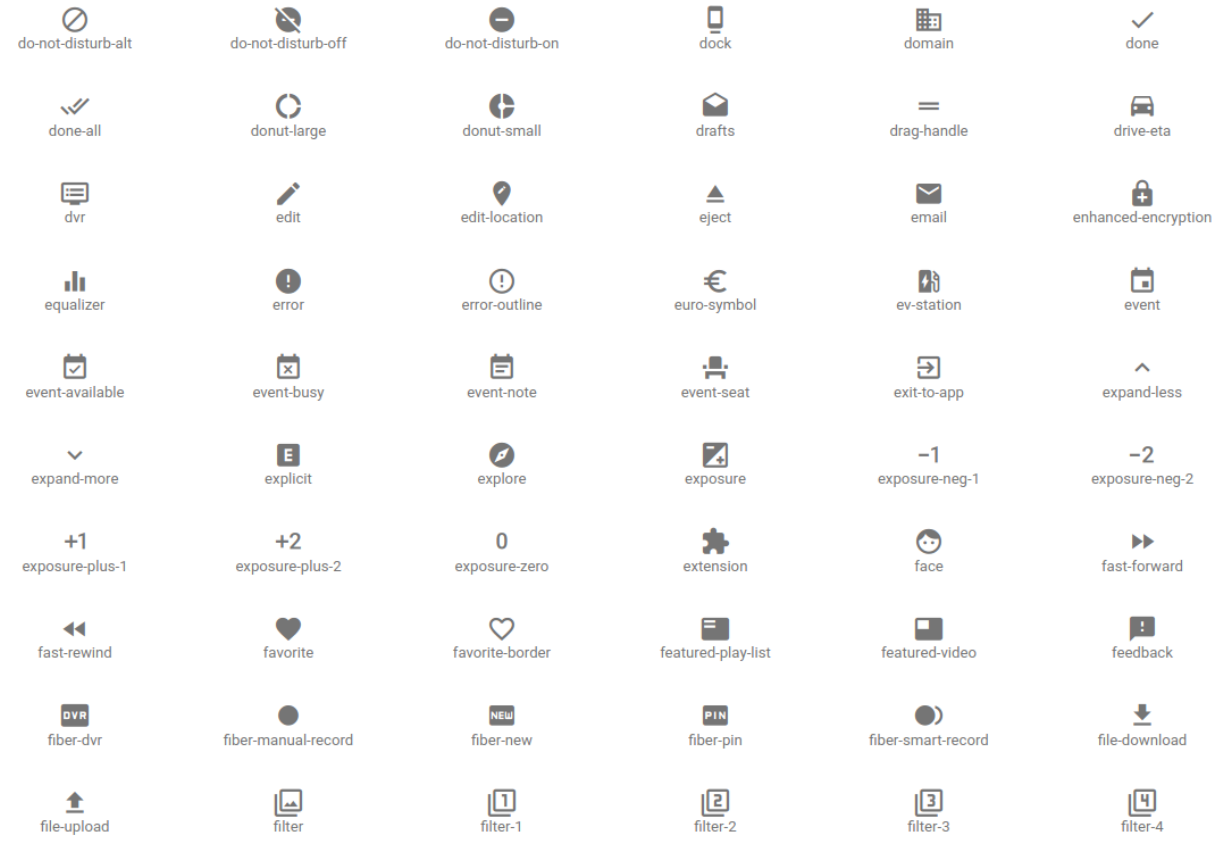
25.3.3. “Build” to “Colorize”



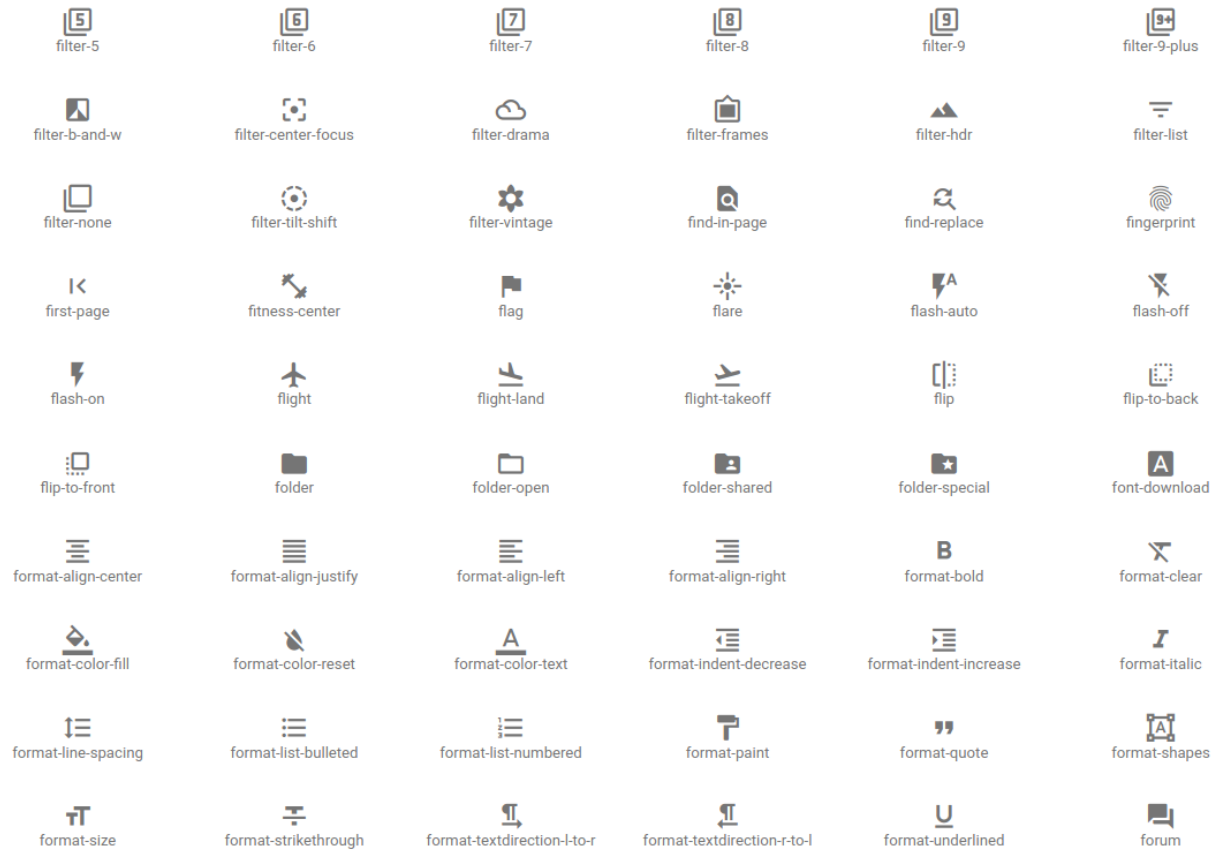
25.3.4. “Comment” to “Do Not Disturb”



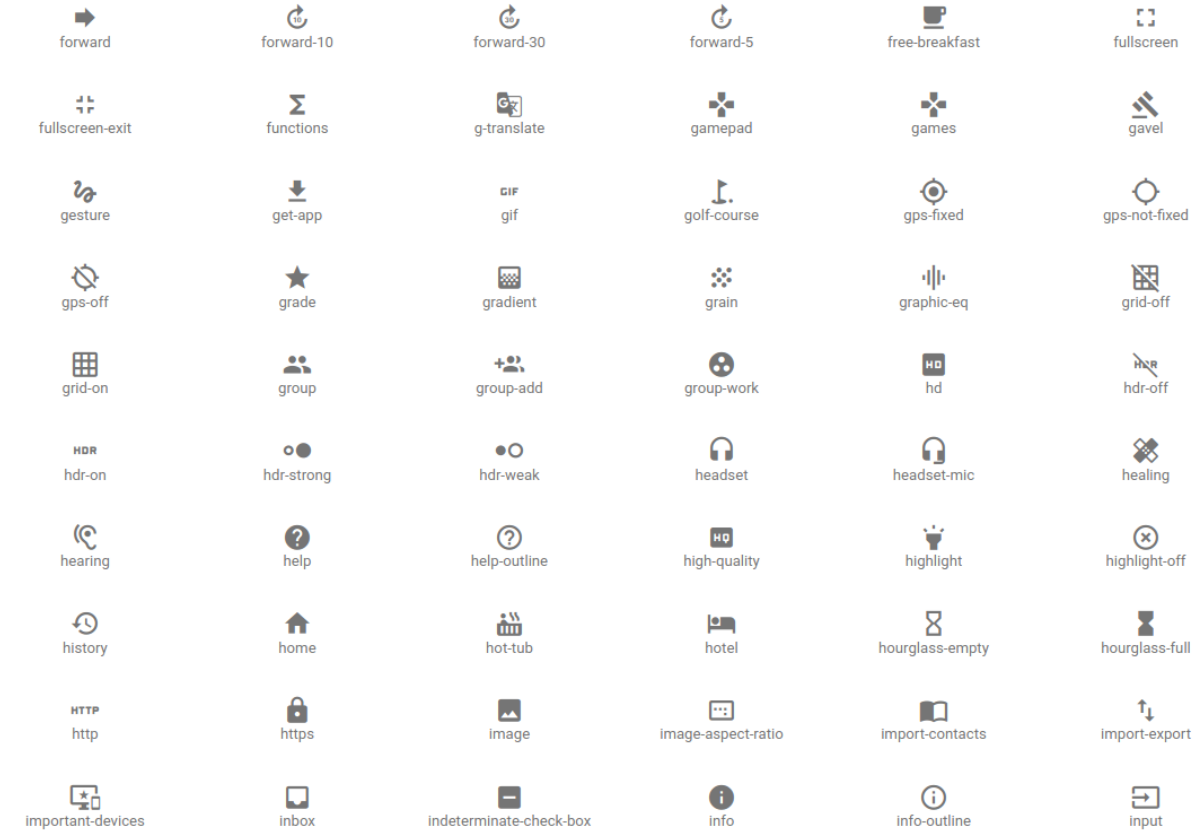
25.3.5. “Do Not Disturb Alt” to “Filter 4”



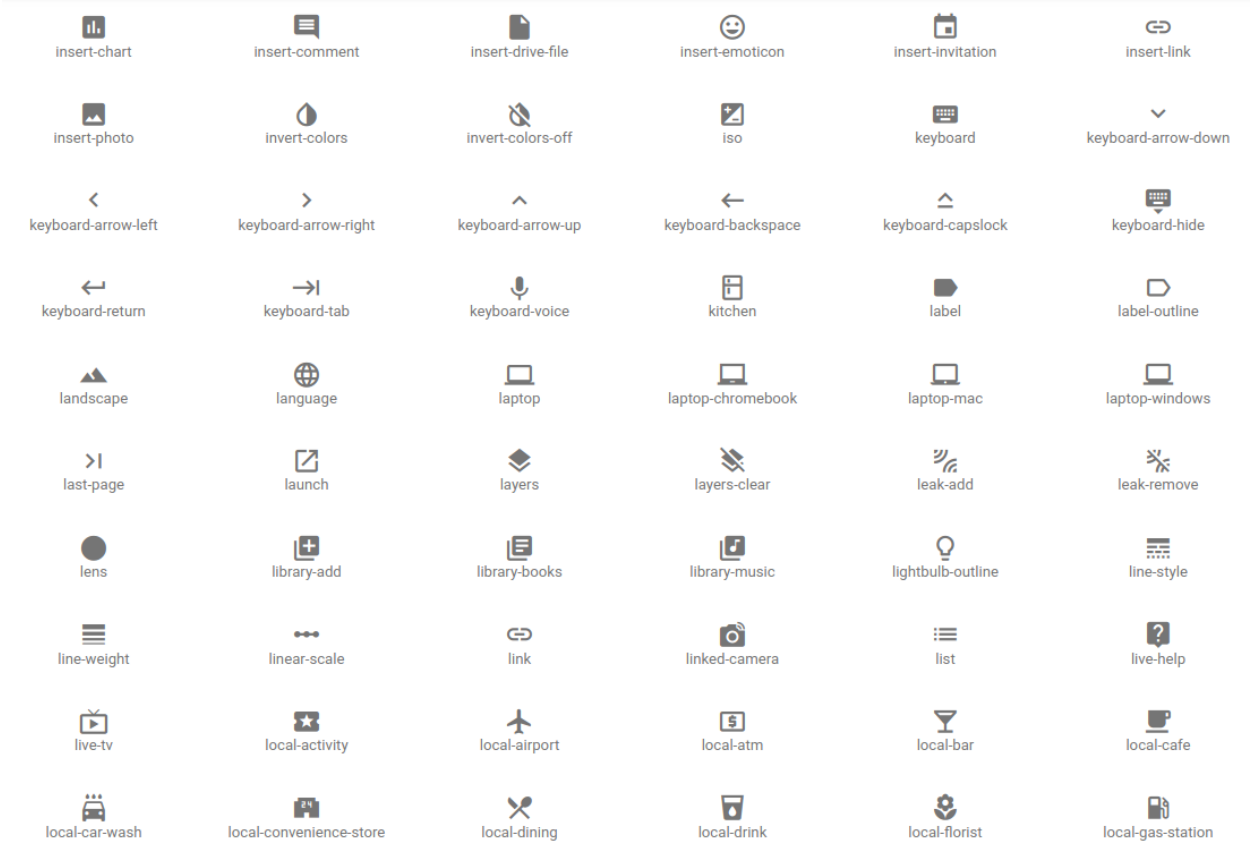
25.3.6. “Filter 5” to “Forum”



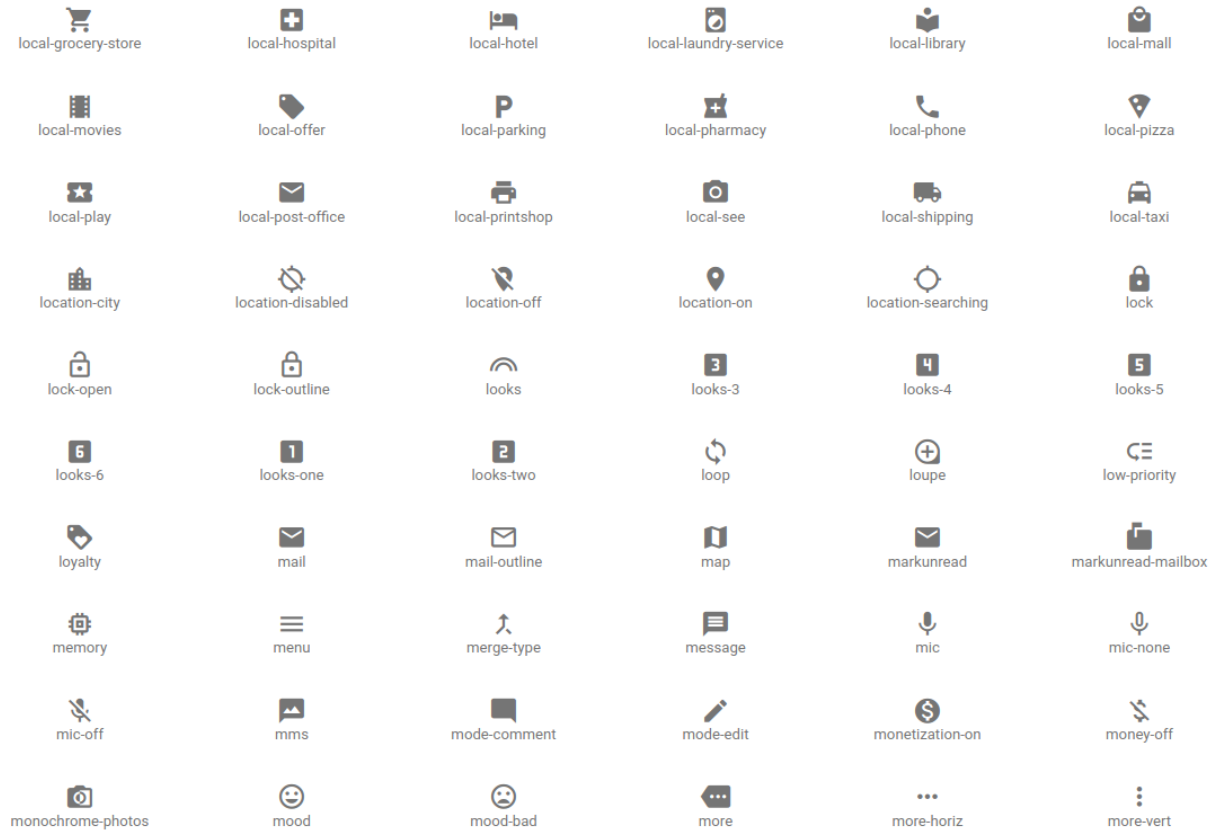
25.3.7. “Forward” to “Input”



25.3.8. “Insert Chart” to “Local gas Station”



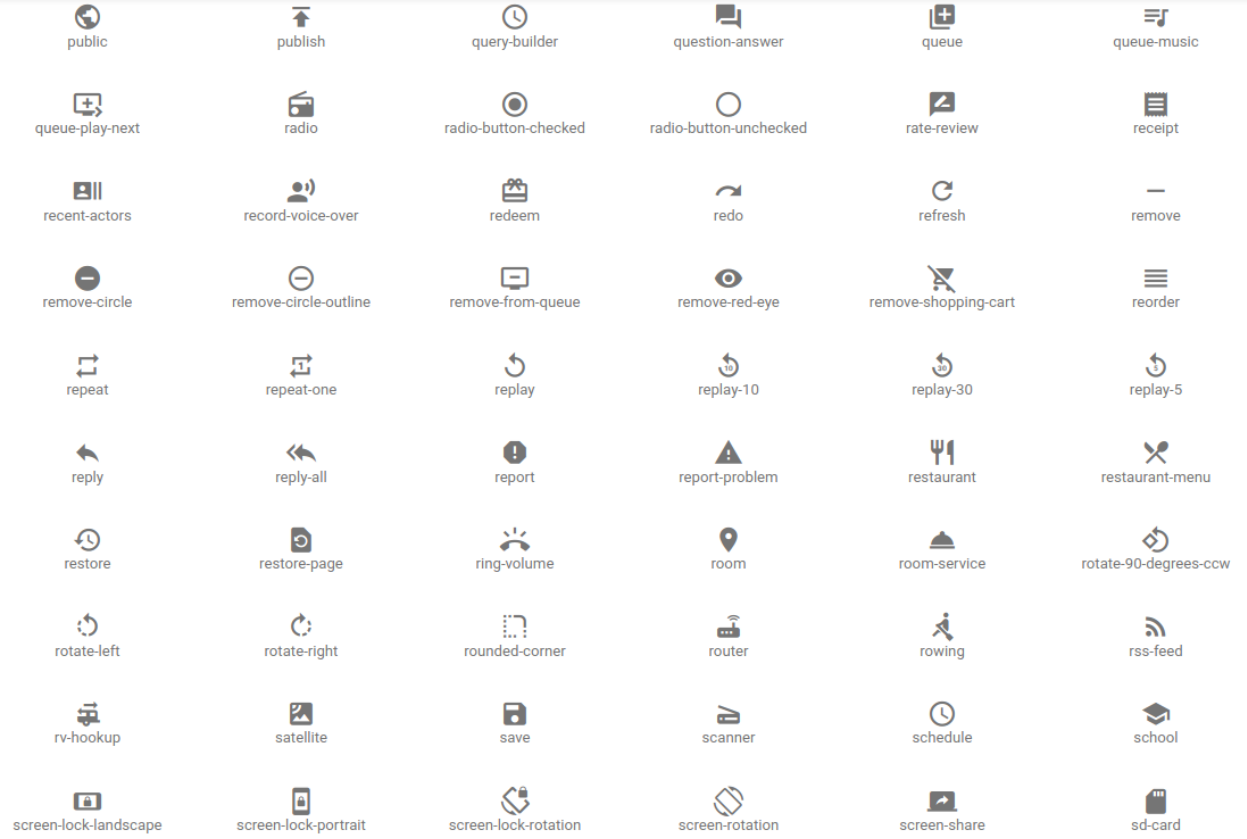
25.3.9. “Local Grocery Store” to “More Vert”



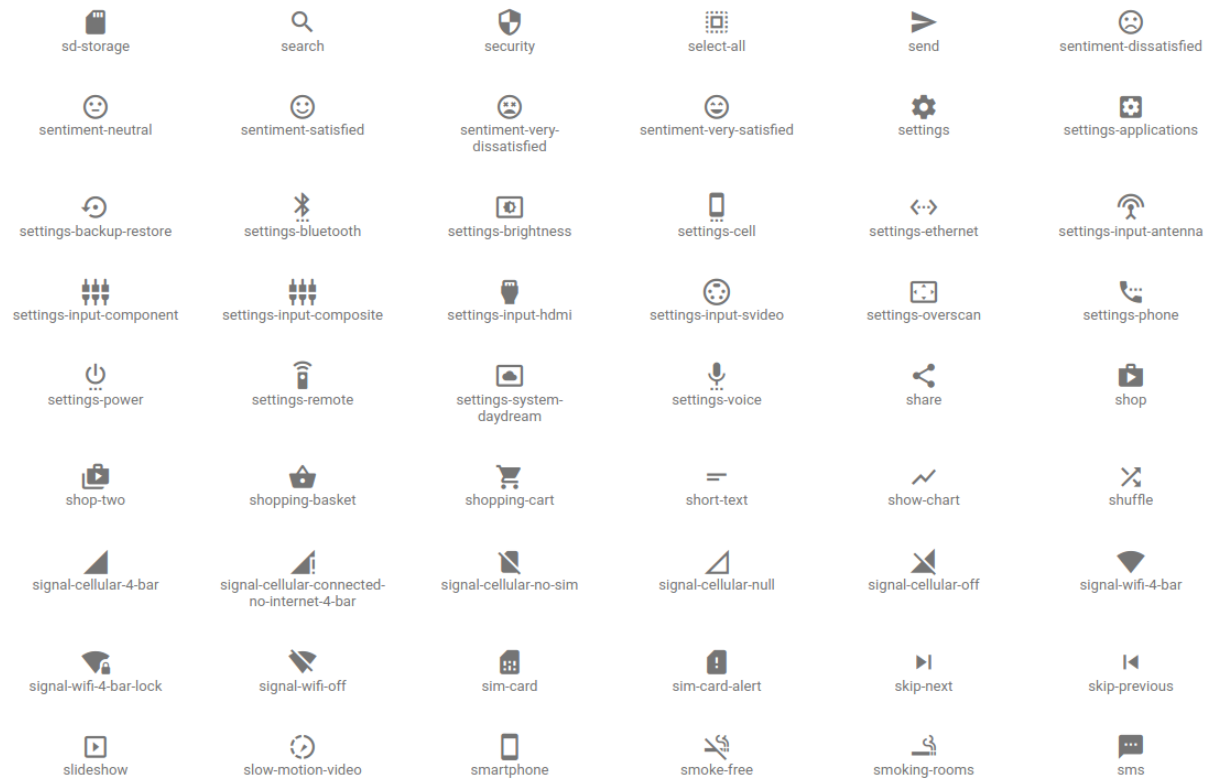
25.3.10. “Motorcycle” to “Perm Identity”

25.3.11. “Perm Media” to “Priority High”

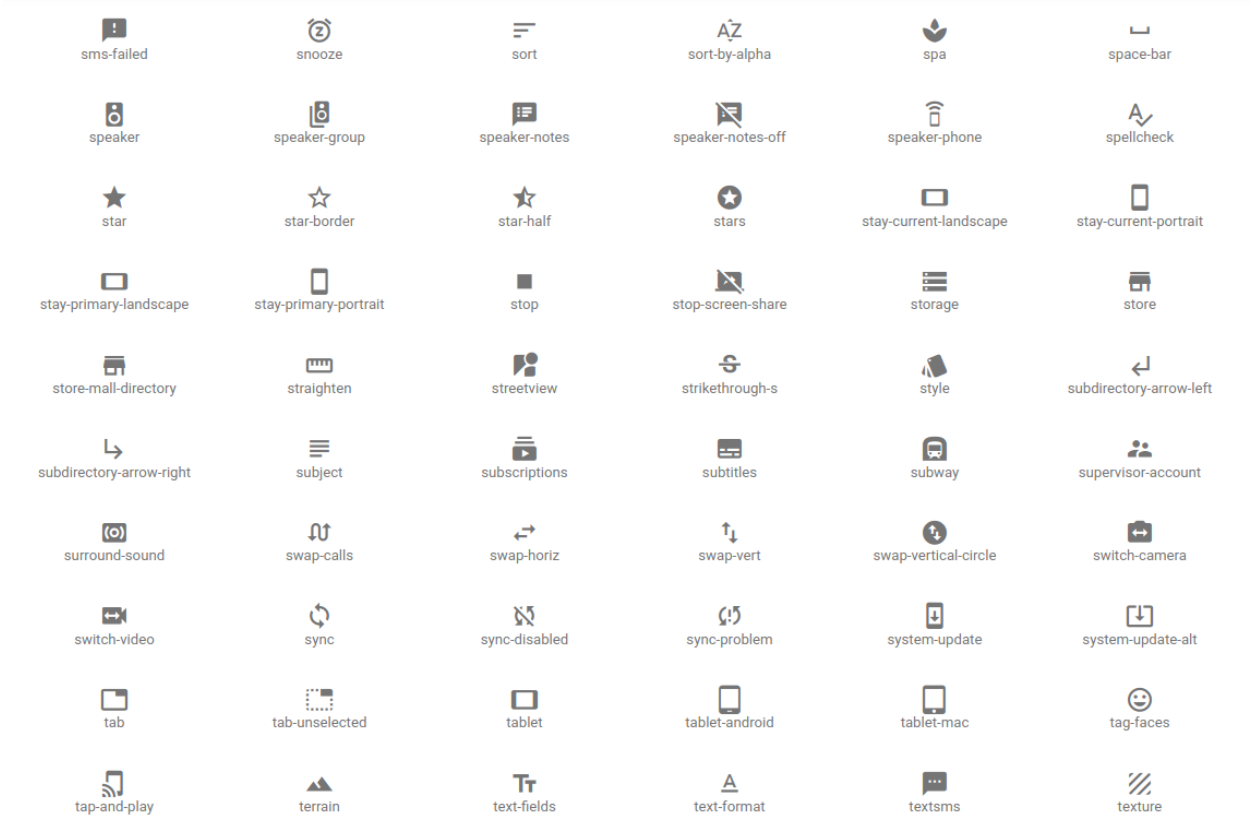
25.3.12. “Public” to “Sd Card”



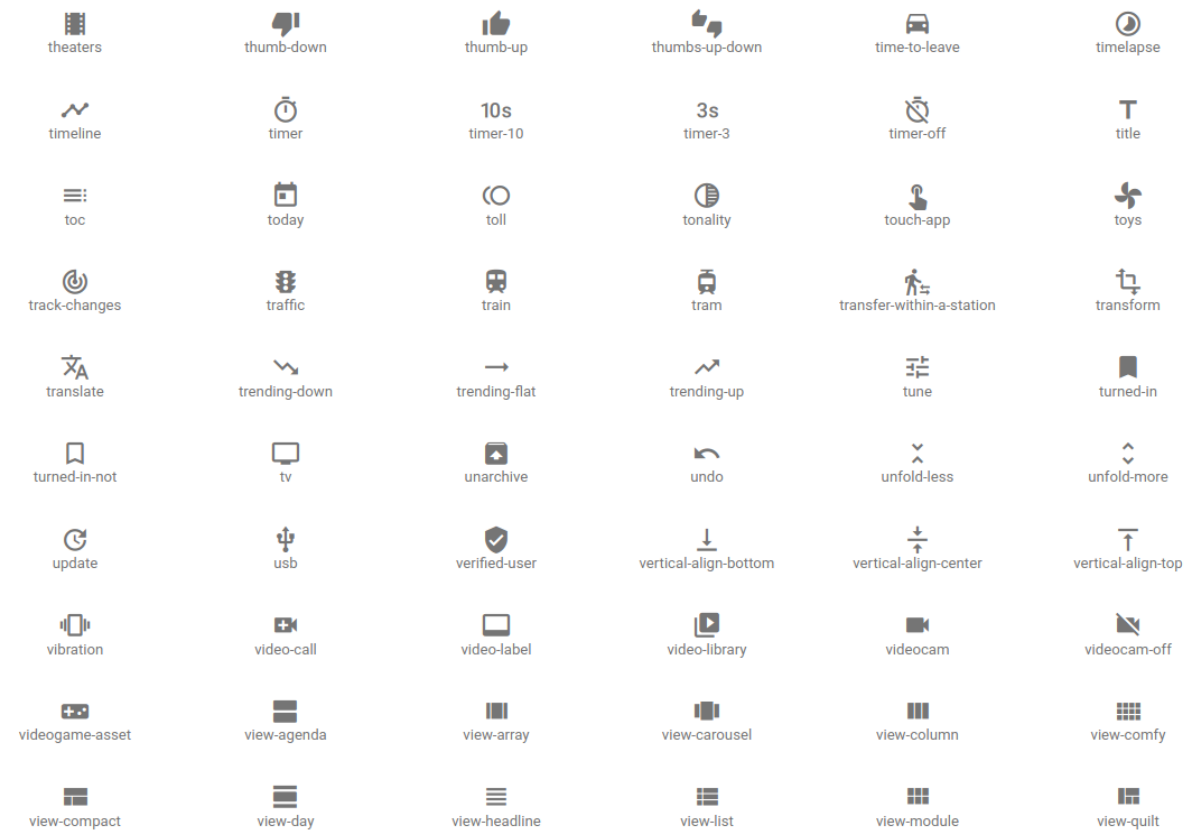
25.3.13. “Sd Storage” to “Sms”



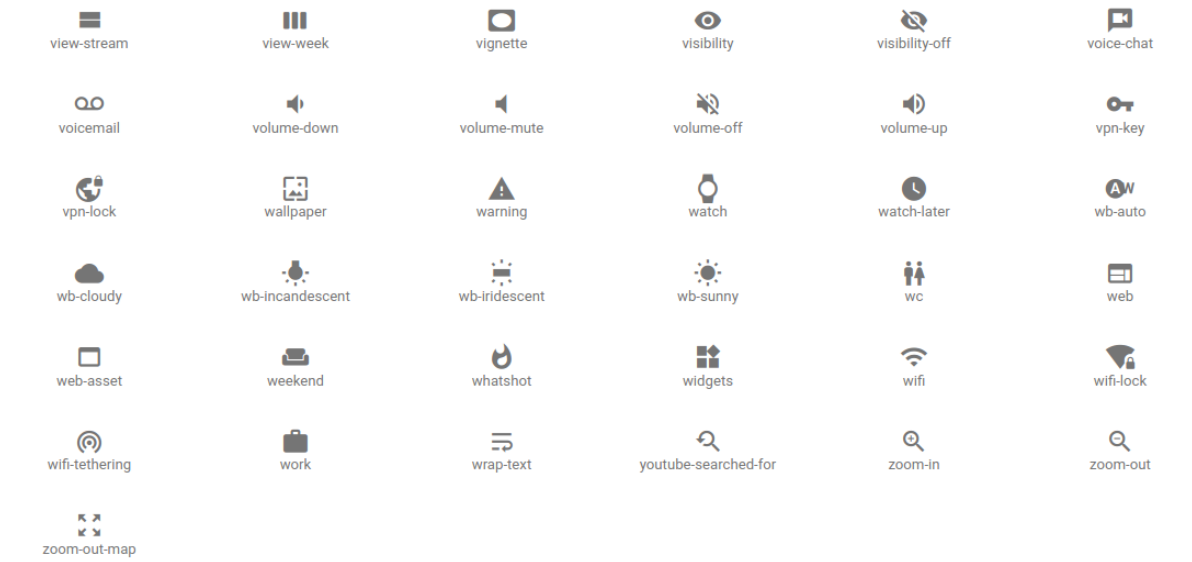
25.3.14. “Sms Failed” to “Texture”



25.3.15. “Theaters” to “View Quilt”



25.3.16. “View Stream” to “Zoom Out Map”

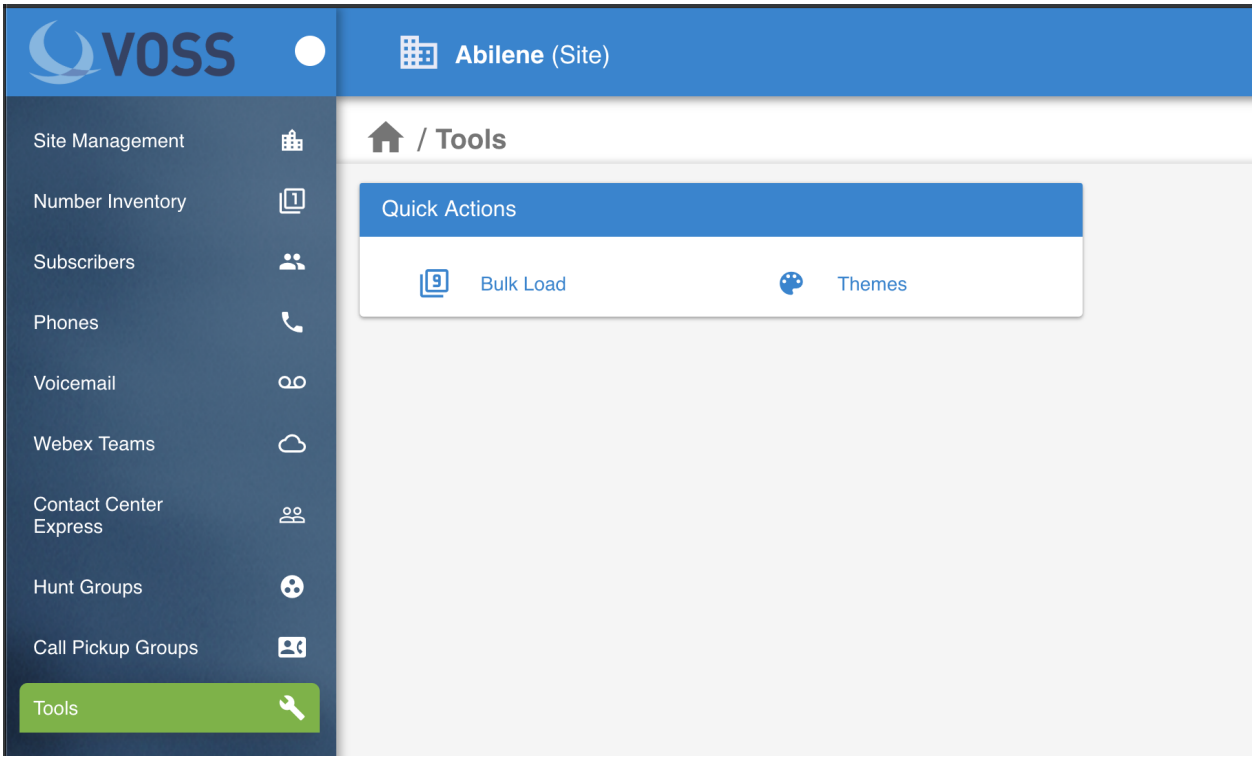


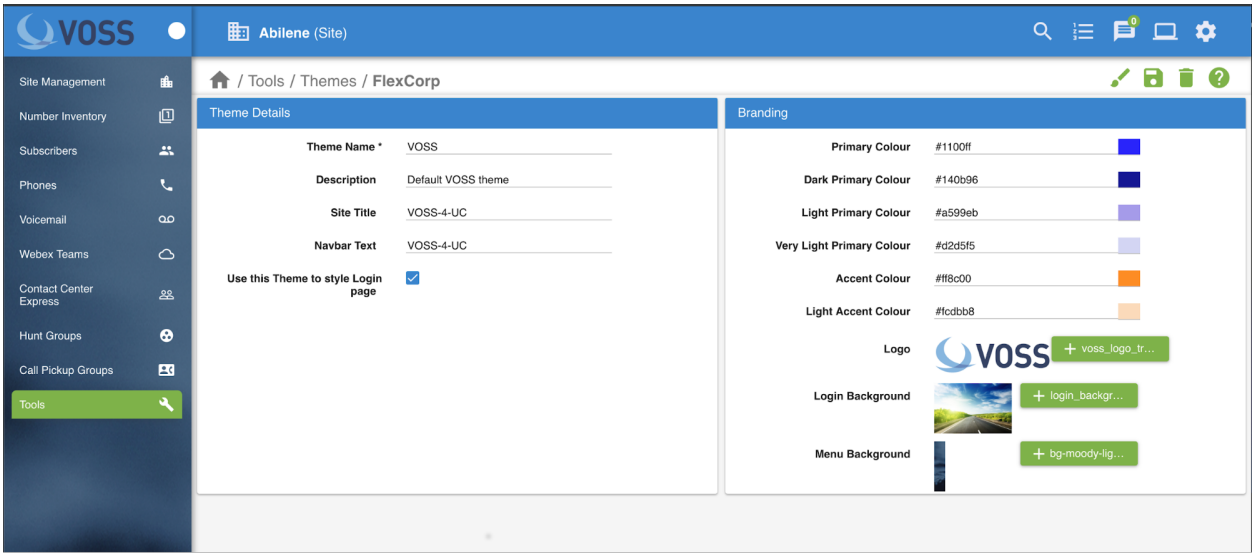
25.4. Custom Business Admin Themes and Branding

It is possible to create a custom theme which changes the following properties of the Business Admin Portal:

- Primary and accent colors
- Logo image
- Login screen background image
- Background image for menu
- Browser tab title

See “Create a Theme in the Business Admin Portal” in the Core Feature Guide for details.

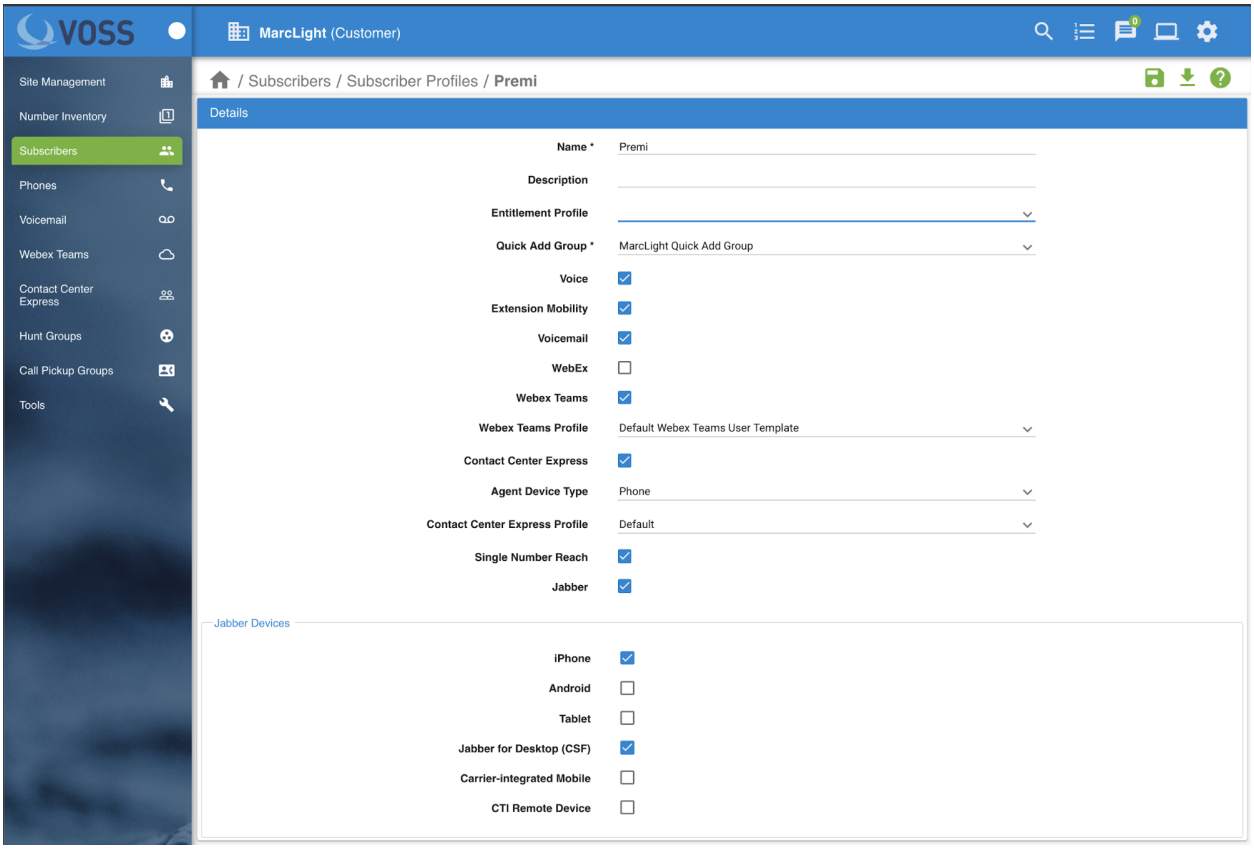




25.5. Subscriber Profiles

A subscriber profile allows for quick provisioning of subscribers in the Business Admin Portal (BAP) with the same (or similar) set of features and services.

Subscriber profiles can be created by an administrator using either the Administration GUI or the Business Admin Portal (BAP). These subscriber profiles will be available in the BAP **Subscriber Profile** drop-down when adding a subscriber at that hierarchy level (and below) only.



A subscriber profile allows an administrator to pre-configure the following:

- Entitlement Profile to use:
  - This determines which features a subscriber is allowed to have.
- Quick Add Group:
  - This captures all configuration templates to be used during service provisioning.
  - These are the same quick add groups used in the quick add subscriber feature (refer to the Core Feature Guide).
- Voice:
  - This will create a desk phone.
  - Phone type is determined by the phone template in the quick add group.
- Extension Mobility:
  - Settings are driven from template in the quick add group.
- Voicemail
- WebEx
- Webex Teams:
  - It is possible to select a Webex Team user profile.
  - This user profile determines the actual Webex Teams services that will be provisioned.
- Contact Center Express:

  - It is possible to select an Agent profile.
  - Must select what device type must be used as the agent's controlled device.
- Single Number Reach
- Jabber:
  - Can select one or more Jabber device types.

Important: A **Default** subscriber profile is created at sys (System) level, but can be deleted by a system administrator *only*.

Best practice is to clone and override an existing subscriber profile in order to use a working quick add group.

25.6. Theme Management

25.6.1. Create a Theme in the Business Admin Portal

The **Themes** interface can be used to create a theme that applies to the Business Admin Portal as well as the VOSS-4-UC Administration GUI.

Note:

- A theme created in the Business Admin Portal will also show and can be edited from the VOSS-4-UC Administration GUI (see under "Themes" in the Core Feature Guide for details).
- Since two themes are now compiled when saving a new theme on the Business Admin Portal, this takes slightly longer than theme compilation on the VOSS-4-UC Administration GUI.
- Themes created in the Business Admin Portal:
  - cannot be exported in full from the Business Admin Portal, so that it can be imported
  - will show in the VOSS-4-UC Administration GUI, where they can be exported

---

Use the **Preview** button  to preview the saved theme before it is applied to the user interface by assigning it to a user role.

Theme Details

Note: If the Business Admin Portal Theme interface is to be used for full Administration GUI theme configuration, a Custom Admin GUI File should be uploaded.

- **Custom Admin GUI File**:
  - If a *theme file is added*:

    the theme file will apply the VOSS-4-UC Administration GUI, while the theme customization updates made in the **Branding** group of controls will *only* apply to the Business Admin Portal.

- If *no theme file is added*:

  the theme updates made in the **Branding** group of controls are applied to VOSS-4-UC Administration GUI *and* the Business Admin Portal. The **Custom Admin GUI File** upload control is then *not* available for theme modification.

Branding

- Color selection:
  - Select a color using either the color picker control or by typing in the color hex value. The color picker control is only available on the Business Admin Portal theme interface.

    Refer to:
  - *Business Admin Theme Color Reference*.
  - *Administration GUI Theme Customization Color Reference*
- Image upload:
  - Note the file size and *width x height* pixel dimension size restrictions (shown on the context sensitive help) for images. A warning message will also show if selected images are too large.

    The **Logo** image format must be PNG format. Other images can be PNG or JPEG.
  - The **Menu Background** image does not apply to the VOSS-4-UC Administration GUI.

25.6.2. Business Admin Theme Color Reference

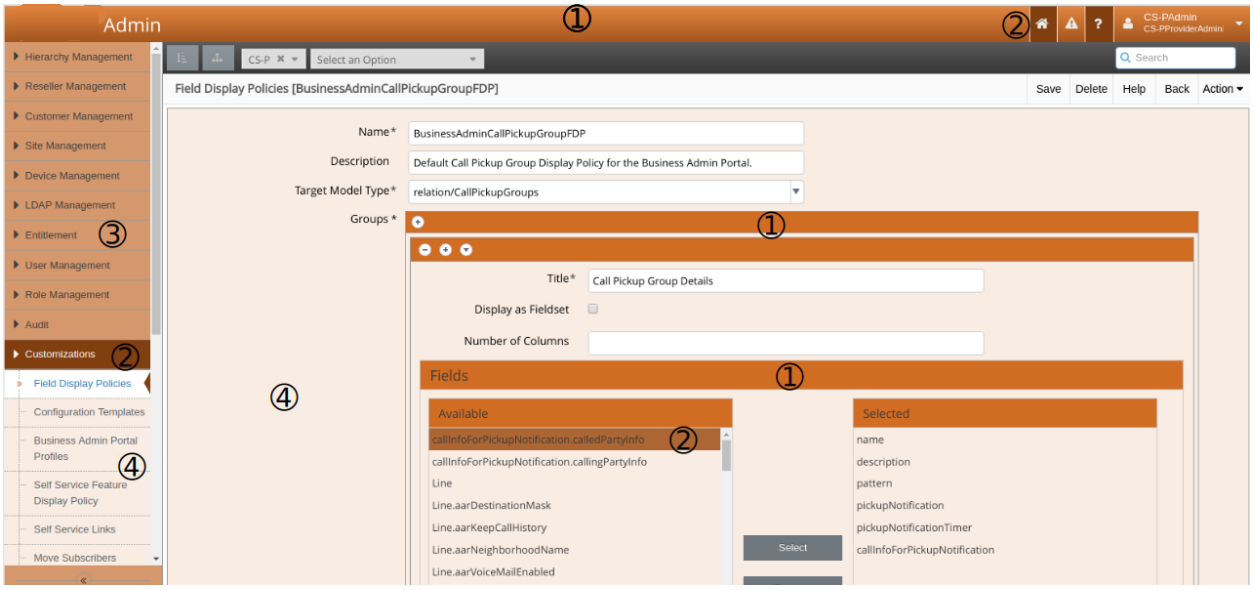
The Element variable below is a descriptive name of the GUI element that will be affected by the Color variable, which corresponds with the color name on the Theme design form.

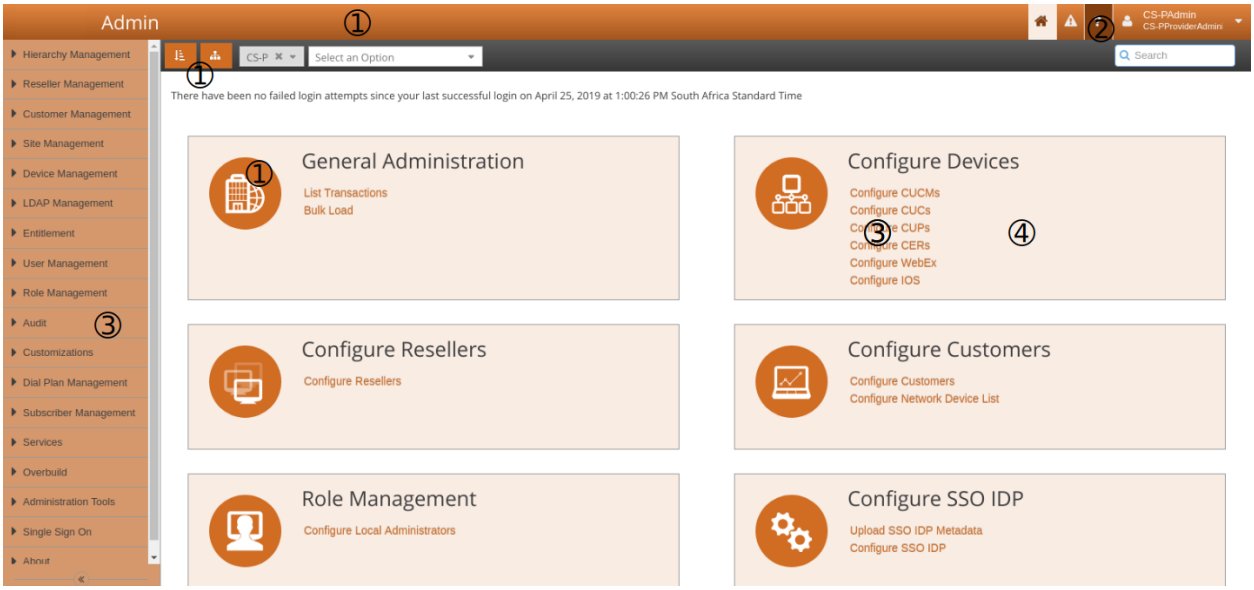
Element	Color
$sidebarLogoBgColor	$primaryColor
$sidebarBgColor	$primaryColor
$topbarTextColor	$primaryLightestColor
$topbarIconColor	$primaryLightestColor
$submenuBgColor	$primaryColor
$darkSubmenuBgColor	$primaryDarkColor
$horizontalSubmenuBgColor	$primaryColor
$horizontalSubmenuitemHoverBgColor	$primaryColor
$horizontalSubmenuitemDarkHoverBgColor	$primaryColor
$menuitemActiveBgColor	$accentColor
$subMenuitemActiveTextColor	$accentLightColor
$subMenuitemActiveIconTextColor	$accentLightColor
$darkMenuitemActiveBgColor	$accentColor
$darksubMenuitemActiveTextColor	$accentLightColor
$darksubMenuitemActiveIconTextColor	$accentLightColor

25.6.3. Administration GUI Theme Customization Color Reference

The Theme Customization Color names and the corresponding Administration GUI controls that are affected, are listed below:

1. Primary Colour
   - main window top bar
   - landing page icon background
   - hierarchy and tree view button
   - form heading bars
2. Dark Primary Colour
   - home and help buttons on main window top bar
   - selected side menu item
3. Light Primary Colour
   - hyperlink text
   - side menu background
4. Very Light Primary Colour
   - landing page card background
   - detail form background
   - sub menu backgrond
5. Accent Colour
   - login button
6. Light Accent Colour





26 Appendix: Optional Features

26.1. Dial Plan Management

26.1.1. Introduction

Important: Contact your dedicated VOSS support representative for details on how to set up and configure the next generation dial plan management feature.

Note: If this feature is not exposed in the Admin GUI menu layout, refer to the Optional Features Appendix: Dial Plan Management - Menu Layout Changes and Access Profile Changes.

The VOSS-4-UC next generation dial plan management feature:

- Offers dial plan management that is independent of the hierarchy schema approach of the first generation dial plan management. However, the feature can also be used in together with schema-based dial plan management.
- Enables senior administrators to define complete complex dial plans and to allow the application of these to lower level administrators without the need to understand the complete dial plan.
- Can be used in place of the schema or schema group approach or in tandem with this approach, for example to add elements in an additional dial plan in an ad-hoc manner.
- All the available functionality of schemas are covered by the models of the feature, as well as call routing via route filters.
- Provides additional benefits:
  - More configuration options
  - A repeatable process to manage Cisco Call manager elements
  - Dial plan can be provisioned in a modular manner
  - A structure to store dial plan models

Scope

The following areas of Cisco Dial Plan deployment are covered by this feature:

- Device Pools - Regions - Locations -SRST

- Transcoders
- Conference Bridge
- Media Resource Groups
- Media Resource Group Lists
- Route Groups
- SIP Trunks
- CTI Route Points *with Lines* (Lines are not supported in schemas)
- Time Periods
- Time Schedules
- Partitions
- CSSs
- Route Patterns
- Transition Patterns
- Called Party Transformation Patterns
- Calling Party Transformation Patterns
- SIP Route Patterns

The entire group of dial plan elements is referred to as a “Dial Plan Model”. Each dial plan element is broken into its own container or model for storage in VOSS-4-UC. This allows for simple management of the dial plan model as a whole. The dial plan models may be bulk loaded into VOSS-4-UC and managed via the GUI.

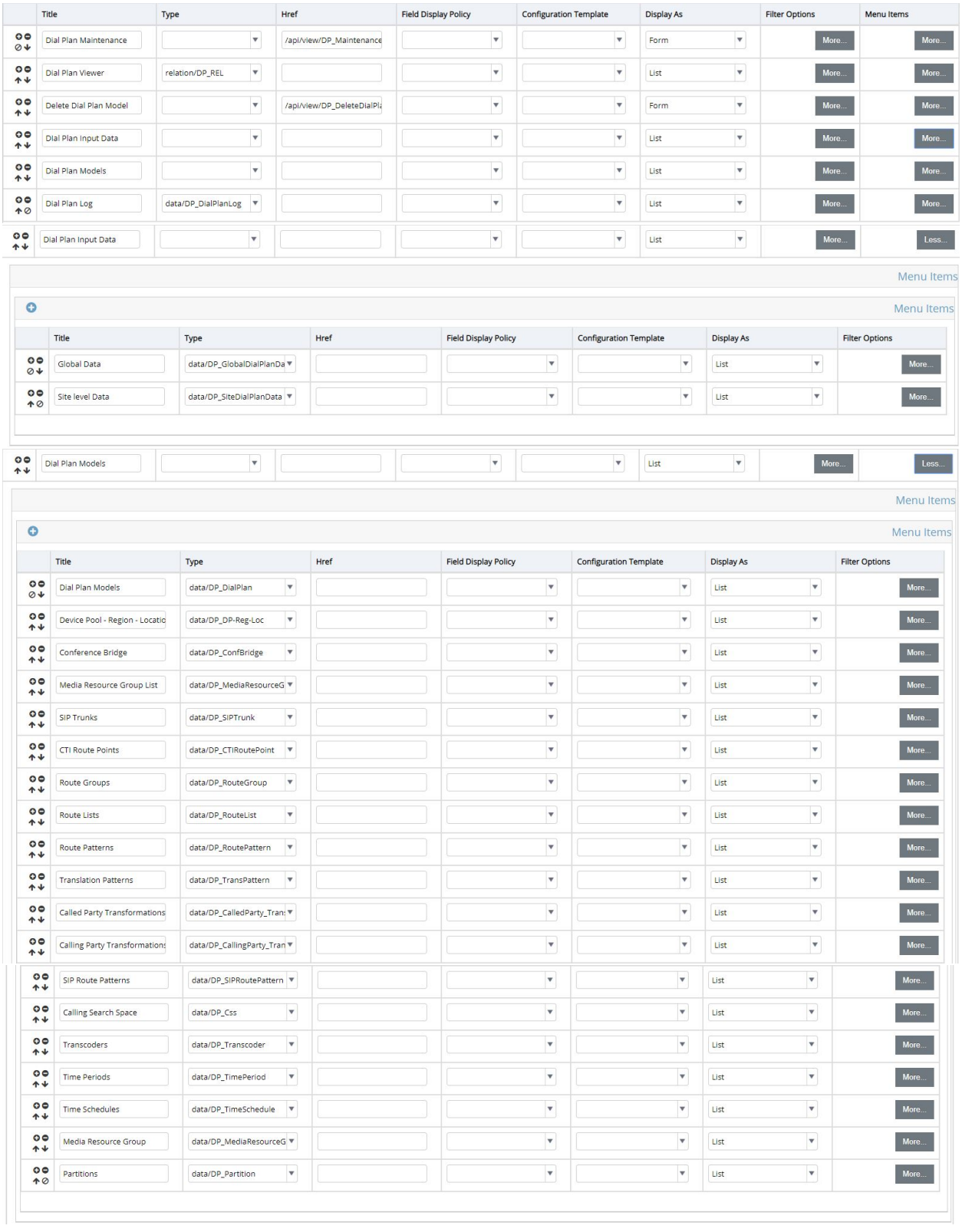
26.1.2. Menu Layout Changes

1. Login as an administrator with sufficient rights to change menu layouts.
2. Click **Role Based Access > Menu Layouts**.
3. Select the required menu.
4. Configure the menu layout as shown below under **Dial Plan Management**.
5. Click **Save**.

Title	Type	Href	Display As
Dial Plan Management			List
Dial Plan Maintenance		/api/view/DP_MaintenanceVIEW/add	Form
Dial Plan Viewer	relation/DP_REL		List
Delete Dial Plan Model		/api/view/DP_DeleteDialPlanModel/add	Form
Dial Plan Input Data			List
• Global Data	data/DP_GlobalDialPlanData		List
• Site Level Data	ata/DP_SiteDialPlanData		List
Dial Plan Models			List
• Dial Plan Models	data/DP_DialPlan		List
• Device Pool-Region -Location-SRST	data/DP_DP-Reg-Loc		List
• Conference Bridge	data/DP_ConfBridge		List
• Media Resource Group List	data/DP_MediaResourceGroupList		List
• SIP Trunks	data/DP_SIPTrunk		List
• CTI Route Points	data/DP_CTIRoutePoint		List
• Route Groups	data/DP_RouteGroup		List
• Route Lists	data/DP_RouteList		List
• Route Patterns	data/DP_RoutePattern		List
• Translation Patterns	data/DP_TransPattern		List
• Called Party Transformations	data/DP_Called_Party_Transformation		List

Title	Type	Href	Display As
Dial Plan Models (Continued)			List
• Calling Party Transformations	data/DP_Calling_Party_Transformation		List
• SIP Route Patterns	data/DP_SIPRoutePattern		List
• Calling Search Space	data/DP_Css		List
• Transcoders	data/DP_Transcoder		List
• Time Periods	data/DP_TimePeriod		List
• Time Schedules	data/DP_TimeSchedule		List
• Media Resource Group	data/DP_MediaResourceGroup		List
• Partitions	data/DP_Partition		List
Dial Plan Log	data/DP_DialPlanLog		List

See also **Dial Plan Management Menu Layout** illustration:



26.1.3. Access Profile Changes

1. Login as an administrator with sufficient rights to change access profiles.
2. Click **Role Based Access > Access Profiles**.
3. Select the required administrator name, for example ProviderAdminAP.
4. Configure the provider access profiles as shown in step 5.
5. Under **Type Specific Permissions** add the following new **Permitted Type** entries and **Permitted Operations**:
    - Permitted Type: view/DP_MaintenanceVIEW
    - Permitted Operations: Create, Field Display Policy, Read
    - Permitted Type: relation/DP_REL
    - Permitted Operations: Create, Read
    - Permitted Type: view/DP_DeleteDialPlanModel
    - Permitted Operations: Create, Read
    - Permitted Type: data/DP_GlobalDialPlanData
    - Permitted Operations: Create, Delete, Export, Export Bulk Load, Read, Tag, Update
    - Permitted Type: data/DP_SiteDialPlanData
    - Permitted Operations: Create, Delete, Export, Export Bulk Load Template, Read, Tag, Update
    - Permitted Types:
        - data/DP_CalledParty_Transformation
        - data/DP_CallingParty_Transformation
        - data/DP_ConfBridge
        - data/DP_Css
        - data/DP_CTIRoutePoint
        - data/DP_DialPlan
        - data/DP_DialPlanLog
        - data/DP_DP-Reg-Loc
        - data/DP_MediaResourceGroup
        - data/DP_MediaResourceGroupList
        - data/DP_Partition
        - data/DP_RouteGroup
        - data/DP_RouteList
        - data/DP_RoutePattern
        - data/DP_SIPRoutePattern
        - data/DP_SIPTrunk
        - data/DP_TimePeriod

  - data/DP_TimeSchedule
  - data/DP_Transcoder
  - data/DP_TransPattern
- Permitted Operations: Create, Delete, Export, Export Bulk Load Template, Read, Tag, Update

6. Click **Save**.

26.1.4. Overview of Dialplan Management Menus and Workflow

Overview

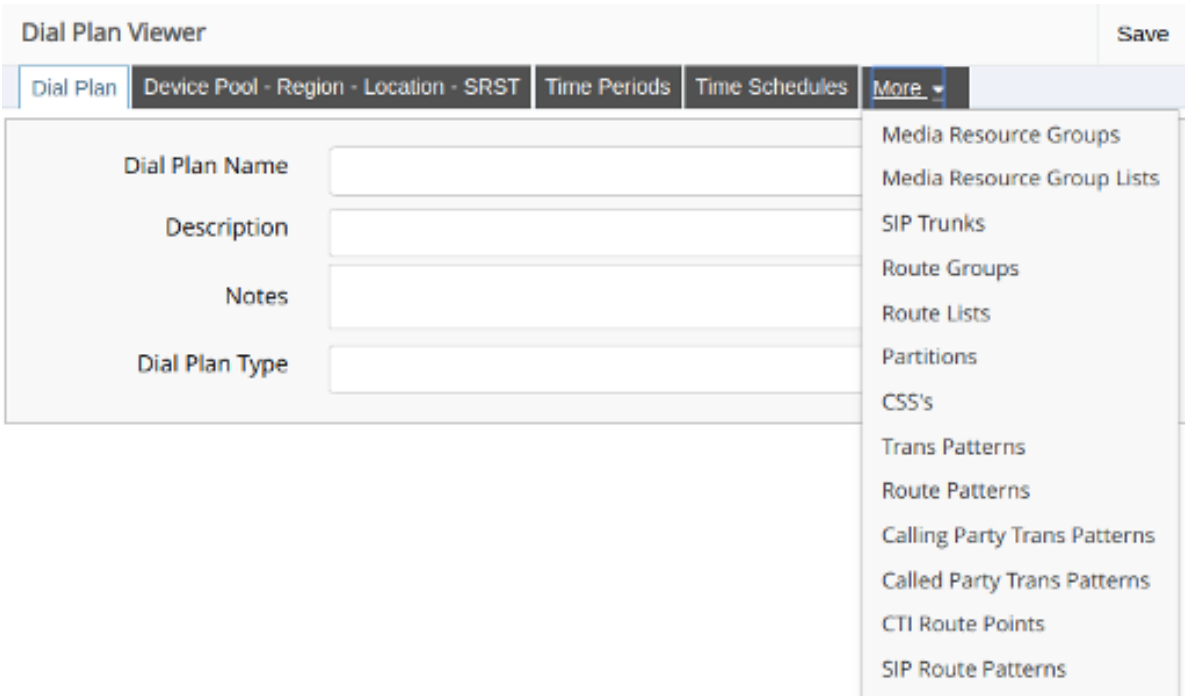
When the Next Generation Dial Plan Management Feature is installed for an administrator, the **Dial Plan Management** menu offers menu items for enhanced dial plan management. The list below provides an overview of the sub-menus:

- **Dial Plan Maintenance** - an interface for the created dial plan to be push to or removed from a chosen, **Target Call Manager Cluster**.

  The hierarchy on which this operation is carried out will filter the list of dial plans - according to the chosen **Dial Plan Type** when it was created on the **Dial Plan Models** menu.

  This utility can also be used to push a dial plan to the cluster for inspection and then to remove it again, as long as no elements were added to the Call Manager cluster that rely on the dial plan elements (for example, adding phones on the Call Manager that would lock CSSs and partitions).

- **Dial Plan Viewer** - a tabbed form view of all the dial plan elements of a selected dial plan created from this feature. The contents of this view corresponds with the view of a dial plan schema, but in a format that is easier to inspect. Note that the viewer does not allow for any changes to be made to the dial plan. See also “Dial Plan Models” for details of each specific dial plan element.



- **Delete Dial Plan Model** - from this menu, an entire dial plan created in this feature can be deleted with a single action, in other words, all dial plan model elements associated with the selected dial plan model are removed, as well as the dial plan model itself.

- **Dial Plan Input Data** - an interface allowing lower level administrators to easily set up data to be added to either global or site level dial plan types. Custom dial plan data can also be included.

  In the individual dial plan elements, the values entered here are then referenced with macros, so that shared dial plan data can be managed efficiently.

- **Dial Plan Models** - a list of menus to manage elements of dial plans created with the feature. Individual elements such as Route Patterns, SIP Trunks, and Translation Patterns each have a menu item from which it can be managed.

- **Dial Plan Log** - a record of Push and Remove operations carried out from the **Dial Plan Maintenance** menu. Details such time and hierarchy of operation, target Call Manager and dial plan name are recorded.

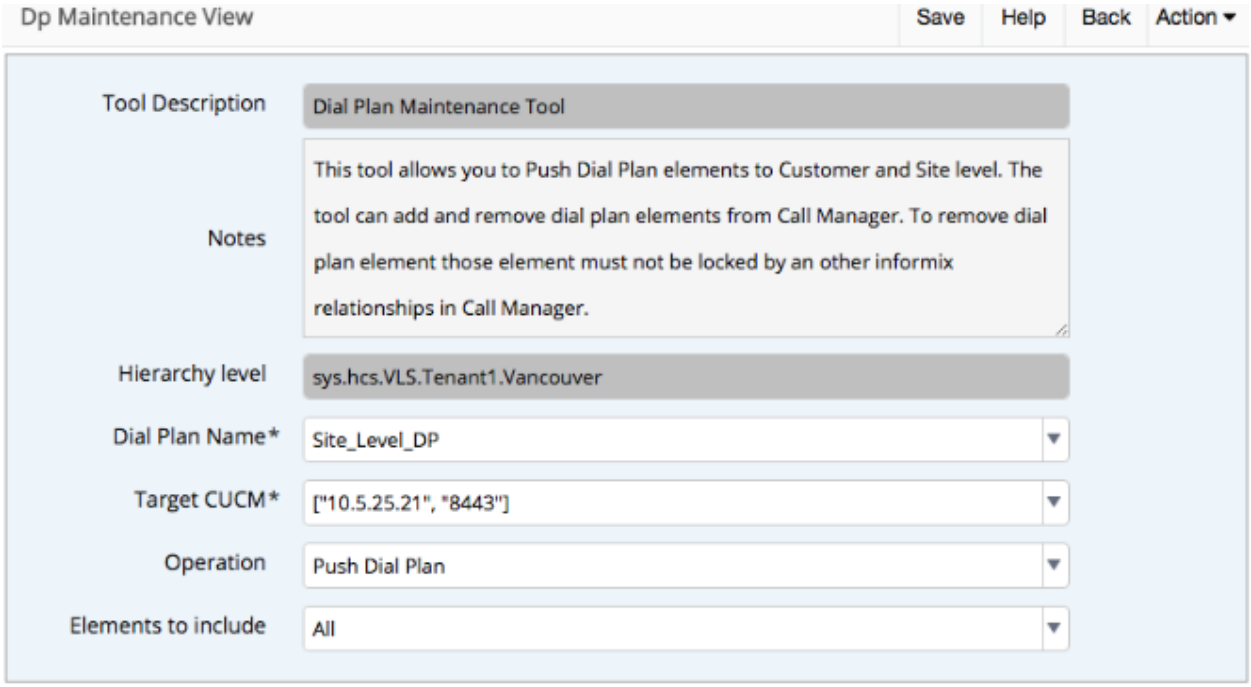
  This interface provides an overall view and does not allow any editing of the dial plan.

26.1.5. Dial Plan Maintenance

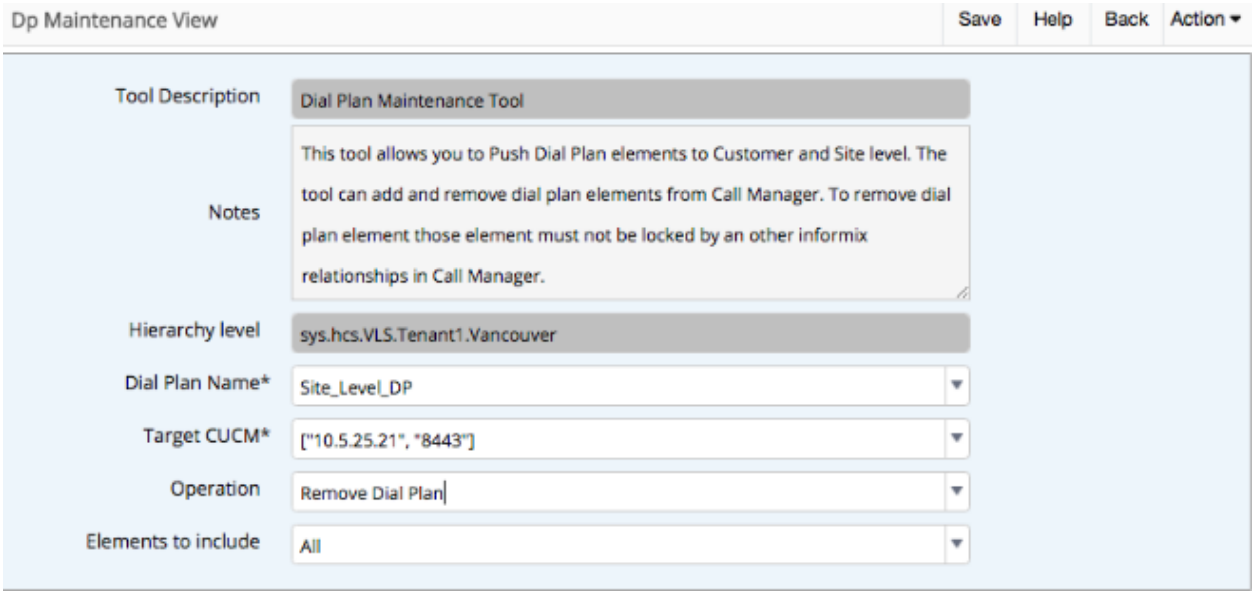
The Dial Plan Maintenance View is the mechanism by which dial plan is manipulated on Call Manager instances. There are no restrictions on the use of this tool from a hierarchy perspective. The naming of the dial plans should indicate at what level the dial plans may be used. There is an enhancement in place to tag dial plans in the dial plan model with Global/Site/No Specific Type so that a small amount of error checking can be introduced into this tool.

The dial plan tag allows only dial plans meant for a specific hierarchy use to be shown in the dial plan maintenance tool. For example, If an administrator is at customer level in VOSS-4-UC and uses the dial plan drop-down, the list of available dial plans are only those tagged “Global”. We do this to ensure the dial plan models with hierarchy specific macros are executed at the correct hierarchy levels.

Push Dial Plan Mode



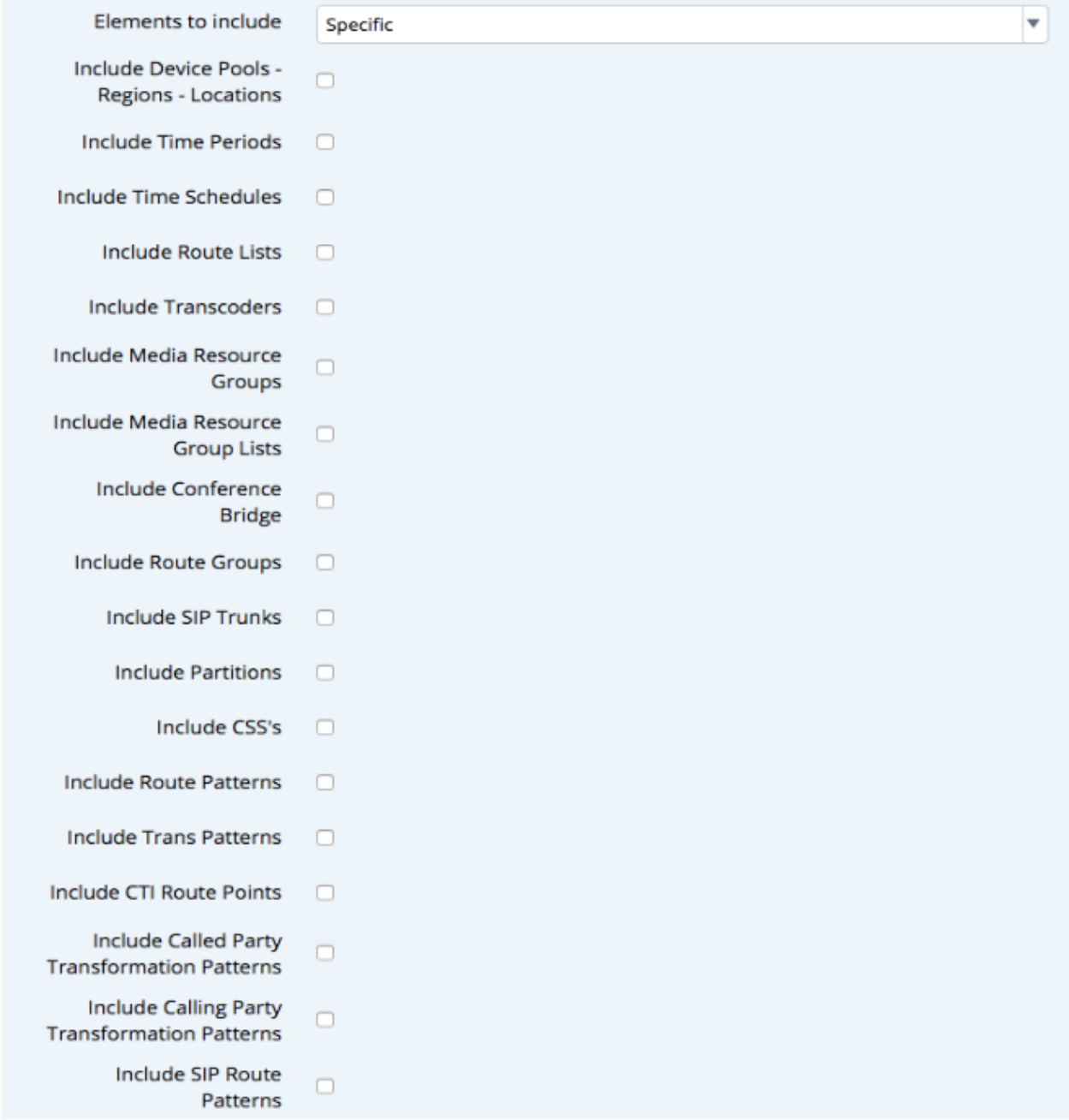
Remove Dial Plan Mode



Both modes of the tool work in the same manner:

1. A dial plan model is chosen from the **Dial Plan Name** drop-down.
2. A target CUCM is chosen from the **Target Call Manager Cluster** drop-down.
3. A operation is chosen from the **Operation** drop-down.
4. Elements to include are chosen from the elements drop-down.

If specific is chosen from the Elements to include field a list of check boxes are exposed to choose individual models:



26.1.6. Dial Plan Input Data and Macros

Overview

The input forms from the **Dial Plan Input Data** simplifies the update of dial plan data by exposing a set of values that can be provided to and then easily applied by lower level administrators.

No values are mandatory, and Field Display Policies can be used to hide unused fields if needed (for example, **Secondary SIP Trunk Destination IP** and **Secondary SIP Trunk Destination Port**.

In addition, a set of custom values can be added and macros are available so that these can be referenced in dial plan elements. (A Field Display Policy can then be used to rename the input field label if needed.)

Two types of dial plan input data can be defined, each corresponding to a dial plan type:

- **Global Data**: applies to Global dial plan type (customer)
- **Site level Data**: applies to Site dial plan type

Input data may be used in combinations to build patterns dynamically, because the pattern itself is a macro.

For example, site level translation patterns for 7 or 10 digit dialing can use the Customer Level macro for PSTN access (or External Breakout Number), then followed by a "." , then the macro for Area Code or Exchange:

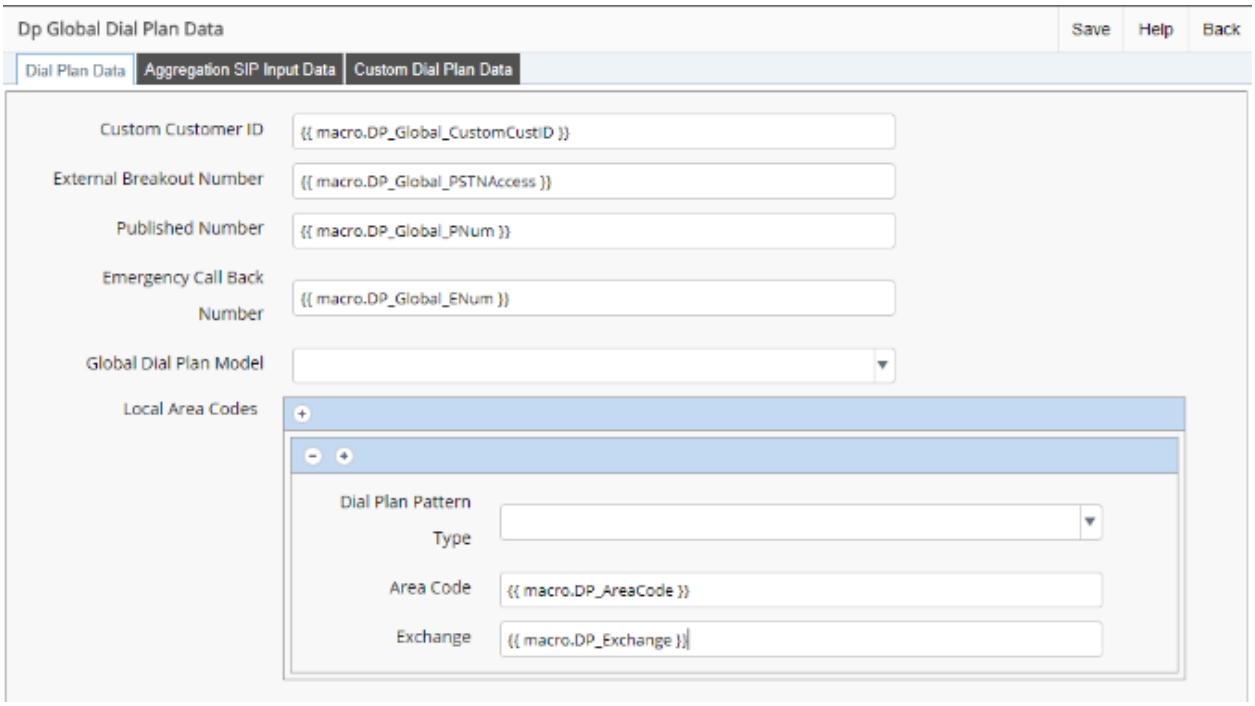
```
{{ macro.DP_Global_PSTNAccess }}.{{ macro.DP_AreaCode }}XXXXXXX
```

when applied, could be inserted to Call Manager as `9.214XXXXXXX` for 10 digit dialing.

```
{{ macro.DP_Global_PSTNAccess }}.{{ macro.DP_Exchange }}XXXX
```

when applied, could be inserted to Call Manager as `9.256XXX` for 7 digit dialing.

Global Dial Plan Data Single Instance

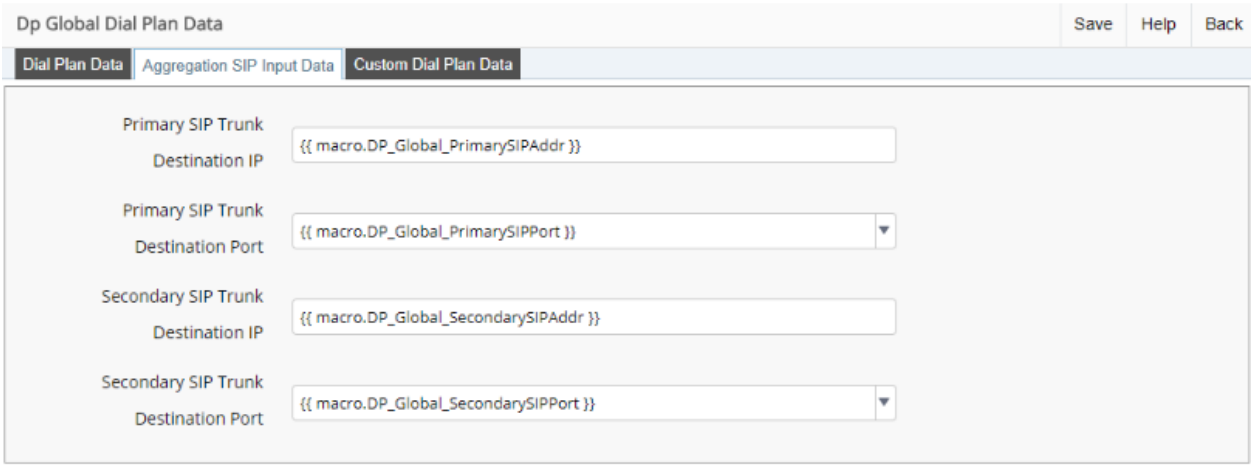


Data from the provided fields may be referenced with the provided macros:

- Custom Customer ID: `{{ macro.DP_Global_CustomCustID }}`
- External Breakout Number: `{{ macro.DP_Global_PSTNAccess }}`
- Published Number: `{{ macro.DP_Global_PNum }}`
- Emergency Call Back Number: `{{ macro.DP_Global_ENum }}`
- Area Code: `{{ macro.DP_AreaCode }}`

- Exchange: `{{ macro.DP_Exchange }}`

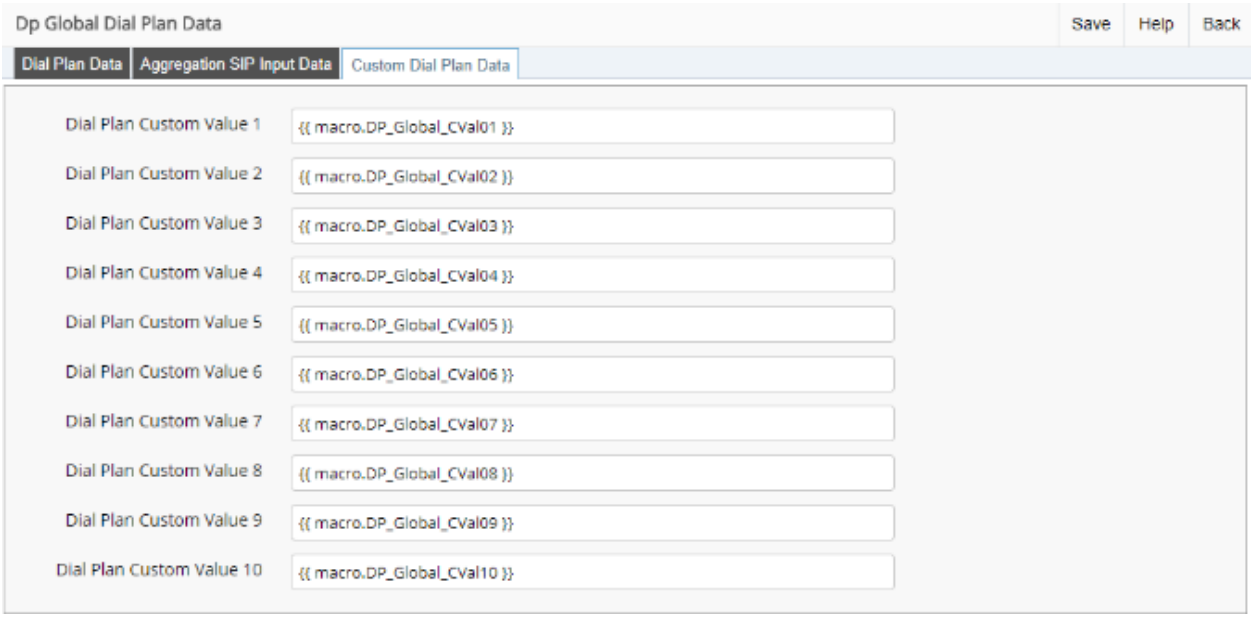
Global Aggregation SIP Input Data Tab



Data from the provided fields may be referenced with the provided macros:

- Primary SIP Trunk Destination IP: `{{ macro.DP_Global_PrimarySIPAddr }}`
- Primary SIP Trunk Destination Port: `{{ macro.DP_Global_PrimarySIPPort }}`
- Secondary SIP Trunk Destination IP: `{{ macro.DP_Global_SecondarySIPAddr }}`
- Secondary SIP Trunk Destination Port: `{{ macro.DP_Global_SecondarySIPPort }}`

Global Custom Dial Plan Data Tab

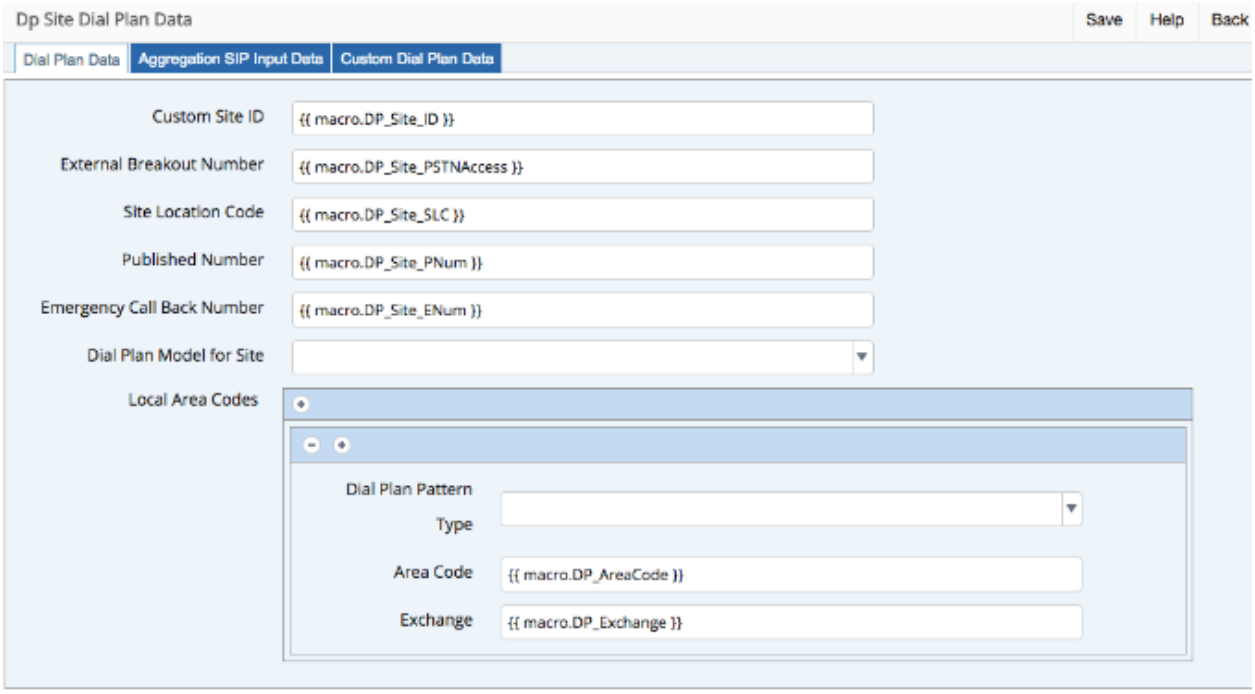


Data from the provided fields may be referenced with the provided macros:

- Dial Plan Custom Value 1: `{{ macro.DP_Global_CVal01 }}`

- Dial Plan Custom Value 2: `{{ macro.DP_Global_CVal02 }}`
- Dial Plan Custom Value 3: `{{ macro.DP_Global_CVal03 }}`
- Dial Plan Custom Value 4: `{{ macro.DP_Global_CVal04 }}`
- Dial Plan Custom Value 5: `{{ macro.DP_Global_CVal05 }}`
- Dial Plan Custom Value 6: `{{ macro.DP_Global_CVal06 }}`
- Dial Plan Custom Value 7: `{{ macro.DP_Global_CVal07 }}`
- Dial Plan Custom Value 8: `{{ macro.DP_Global_CVal08 }}`
- Dial Plan Custom Value 9: `{{ macro.DP_Global_CVal09 }}`
- Dial Plan Custom Value 10: `{{ macro.DP_Global_CVal10 }}`

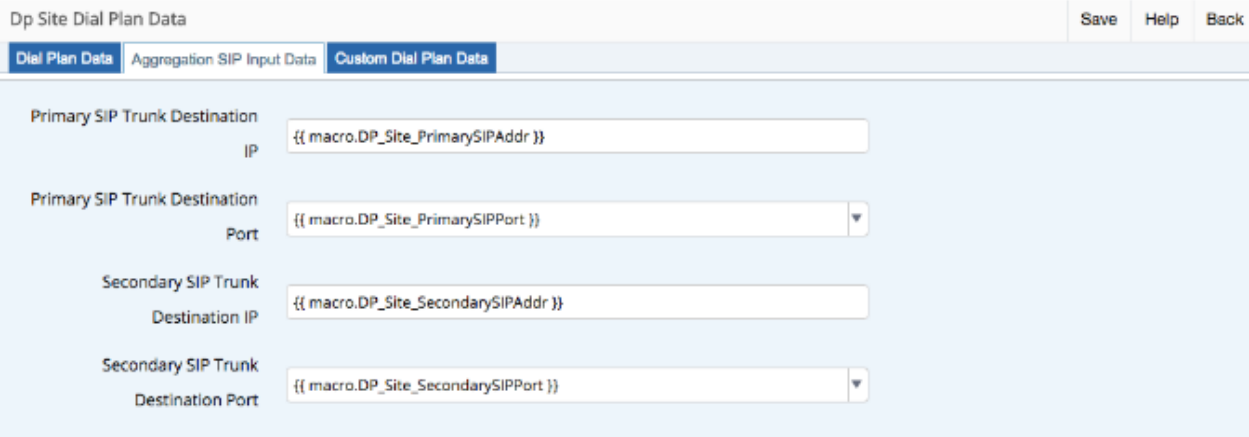
Site Dial Plan Data Single Instance



Data from the provided fields may be referenced with the provided macros:

- Custom Site ID: `{{ macro.DP_Site_ID }}`
- External Breakout Number: `{{ macro.DP_Site_PSTNAccess }}`
- Site Location Code: `{{ macro.DP_Site_SLC }}`
- Published Number: `{{ macro.DP_Site_PNum }}`
- Emergency Call Back Number: `{{ macro.DP_Site_ENum }}`
- Area Code: `{{ macro.DP_AreaCode }}`
- Exchange: `{{ macro.DP_Exchange }}`

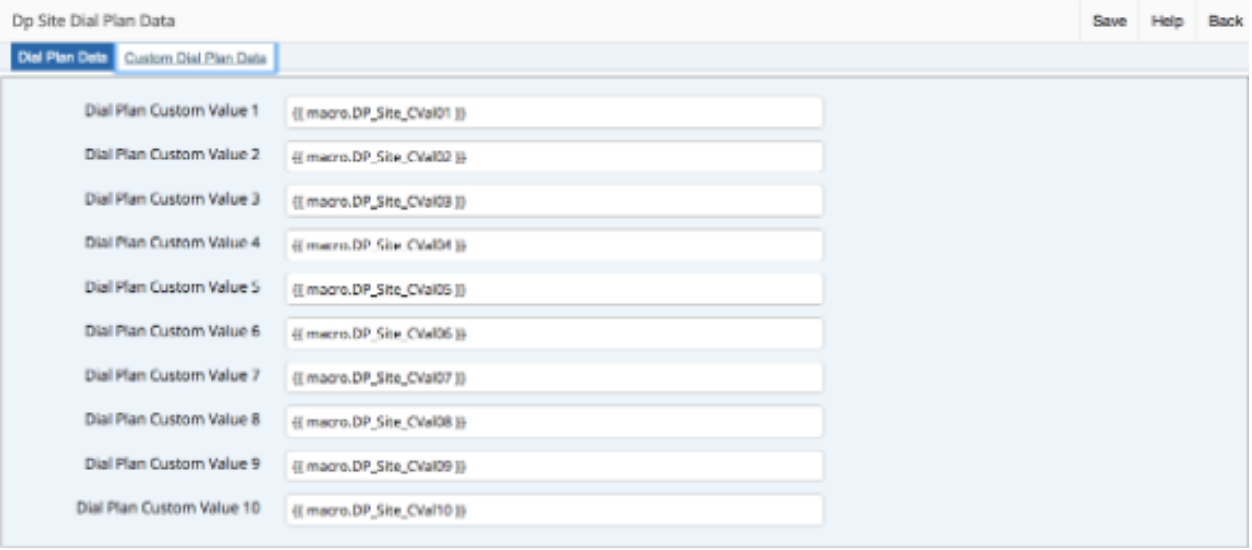
Site Aggregation SIP Input Data



Data from the provided fields may be referenced with the provided macros:

- Primary SIP Trunk Destination IP: `{{ macro.DP_Site_PrimarySIPAddr }}`
- Primary SIP Trunk Destination Port: `{{ macro.DP_Site_PrimarySIPPort }}`
- Secondary SIP Trunk Destination IP: `{{ macro.DP_Site_SecondarySIPAddr }}`
- Secondary SIP Trunk Destination Port: `{{ macro.DP_Site_SecondarySIPPort }}`

Site Custom Dial Plan Data Tab



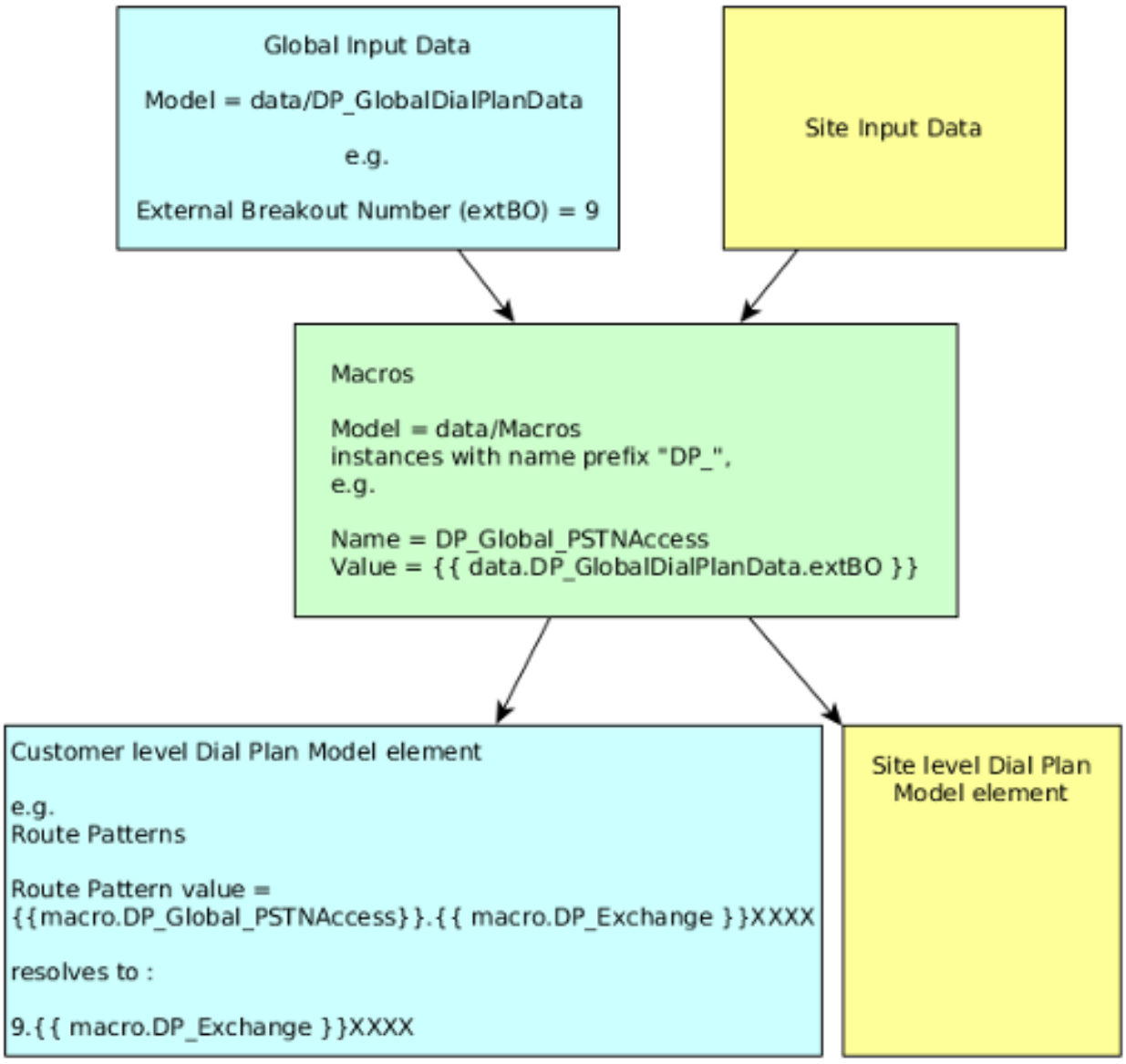
Data from the provided fields may be referenced with the provided macros:

- Dial Plan Custom Value 1: `{{ macro.DP_Site_CVal01 }}`
- Dial Plan Custom Value 2: `{{ macro.DP_Site_CVal02 }}`
- Dial Plan Custom Value 3: `{{ macro.DP_Site_CVal03 }}`
- Dial Plan Custom Value 4: `{{ macro.DP_Site_CVal04 }}`
- Dial Plan Custom Value 5: `{{ macro.DP_Site_CVal05 }}`

- Dial Plan Custom Value 6: `{{ macro.DP_Site_CVal06 }}`
- Dial Plan Custom Value 7: `{{ macro.DP_Site_CVal07 }}`
- Dial Plan Custom Value 8: `{{ macro.DP_Site_CVal08 }}`
- Dial Plan Custom Value 9: `{{ macro.DP_Site_CVal09 }}`
- Dial Plan Custom Value 10: `{{ macro.DP_Site_CVal10 }}`

Diagram Example

The diagram below provides an example of the use of a macro in a Global (customer) level dial plan element: **Route Patterns**.



26.1.7. Dial Plan Models

Overview

From the **Dial Plan Models** menu, a sub-menu and base model called **Dial Plan Model** is available to define the dial plan and to enter a name and type to group its elements.

The Dial Plan Type drop-down is used to tag it with its hierarchy, so that available dial plans to push or remove are filtered when using the Dial Plan Maintenance menu:

- Multi-tenant / Shared Architecture - provider hierarchy
- Global - customer hierarchy
- Site - site hierarchy

Note: If no Dial Plan Type tag is added to a dial plan, a new “in-progress” or “staging” dial plan can be created that will not show up to be pushed or removed on the Dial Plan Maintenance menu.

A description and notes for the Dial Plan Model definition can be added on the input form.

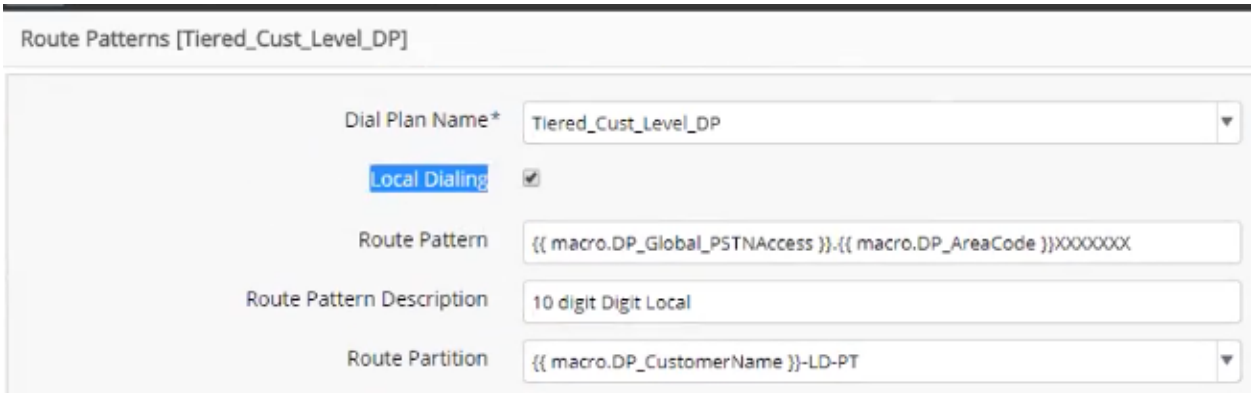
Dial Plan Model Elements

The remaining list of menus manage elements of dial plans created with the feature. Individual elements such as Route Patterns, SIP Trunks, and Translation Patterns each have a menu item from which it can be associated with a Dial Plan Model and managed.

The feature provides menu items or input fields to extend schema based dial plan management functionality. When a dial plan created with the feature is pushed from the **Dial Plan Maintenance** menu, the transaction log can be inspected to see the extended functionality:

- Device Pools - Regions - Locations -SRST
- Transcoders
- Conference Bridge
- Media Resource Groups
- Media Resource Group Lists
- Route Groups
- SIP Trunks
- CTI Route Points *with Lines* (Lines are not supported in schemas)

When managing these dial plan elements, the installed named macros can be used to refer to data added from the **Dial Plan Input Data** menu.



The list view from each of these menus shows the Dial Plan Name - as defined from the **Dial Plan Model** menu - to which the element belongs. The feature structures the elements as instances of distinct data models.

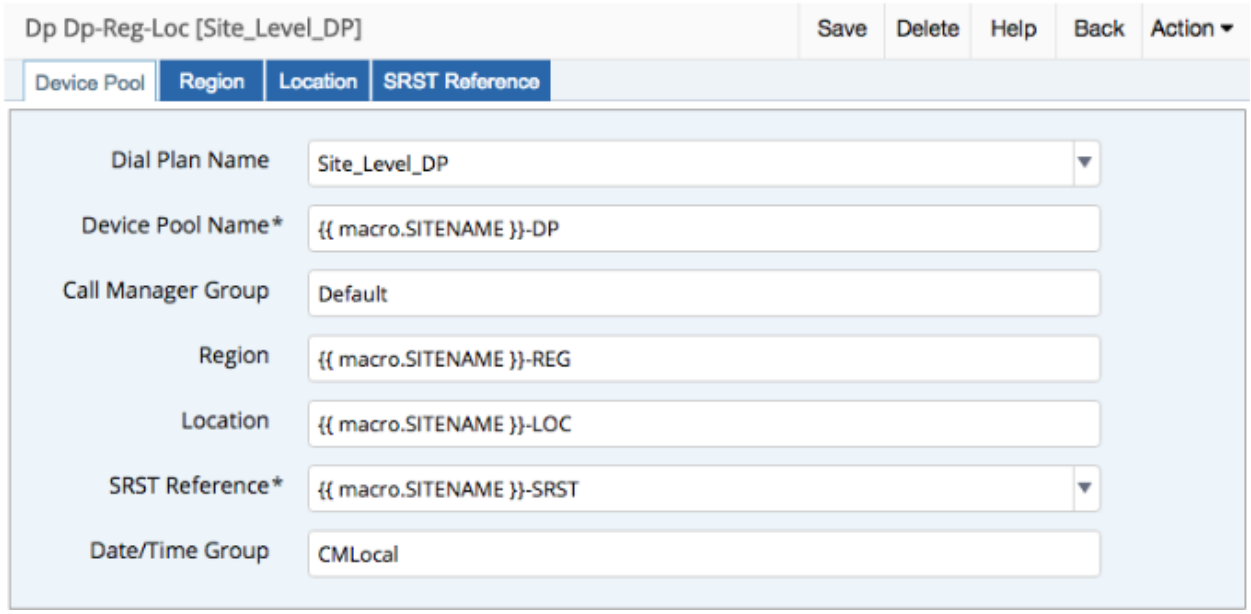
There is an additional flexibility in the **Route Patterns** and **Translation Patterns** dial plan model elements so that a **Local Dialing** check box can be selected here if required when using a simpler or flat dial plan.

Dial Plan elements, such as Calling Search Space, can be cloned and edited to easily add another element to the dial plan by defining an “add-on” dial plan model, associating the cloned CSS element with it and pushing it to the required Call Manager cluster using the **Dial Plan Maintenance** menu. In this way the dial plan can be then be updated - functionality that is not possible in a schema based approach.

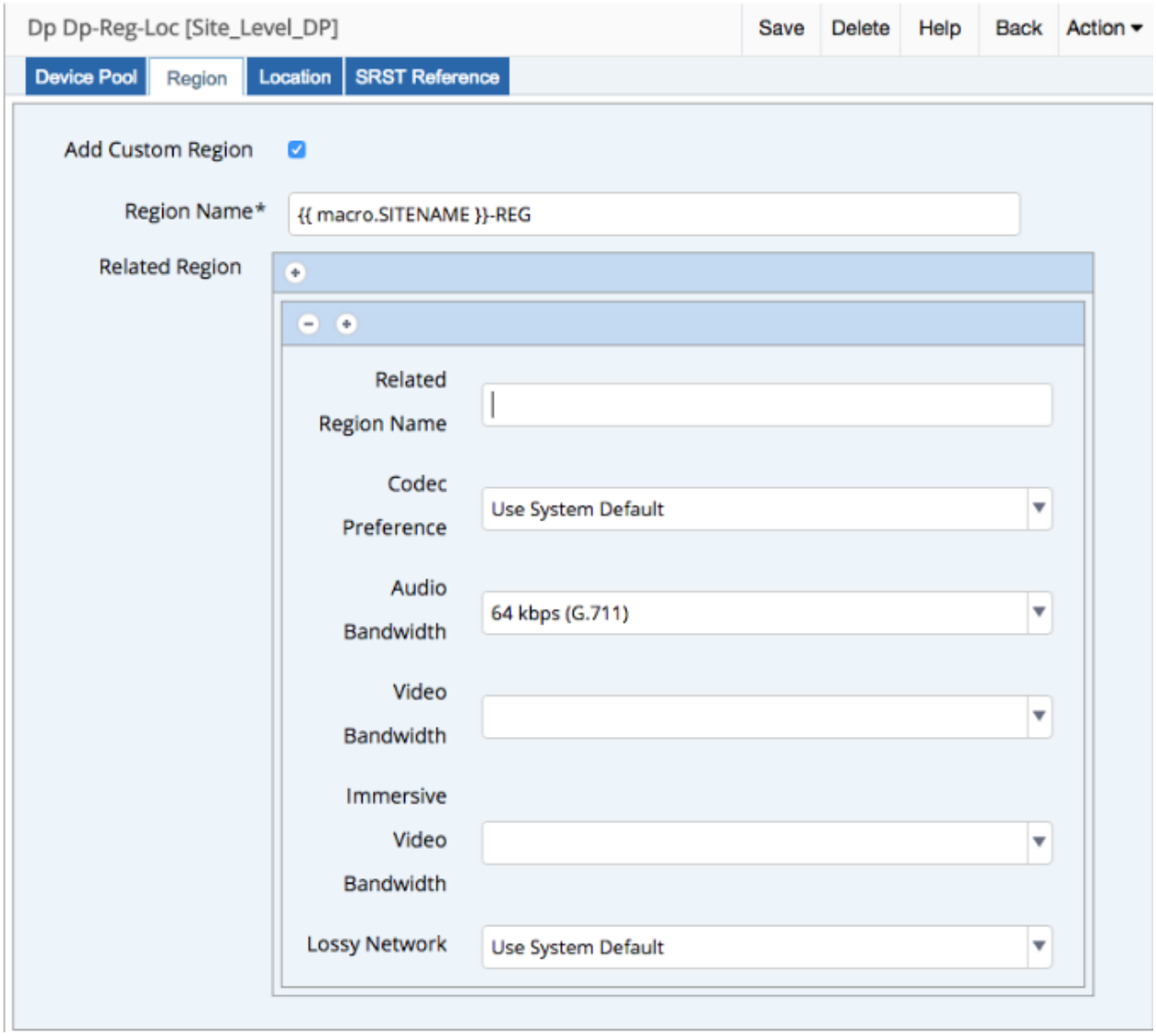
Additional workflows in the feature allow for values (for example MRGL) to be added from for example the **Device Pools - Regions - Locations -SRST** element input form, since the workflow will push to the these to the Call Manager cluster *only after* the prerequisite values become available. Inspect the transaction log to see the required sequence of data carried out with these workflows.

Device Pools - Regions - Locations - SRST

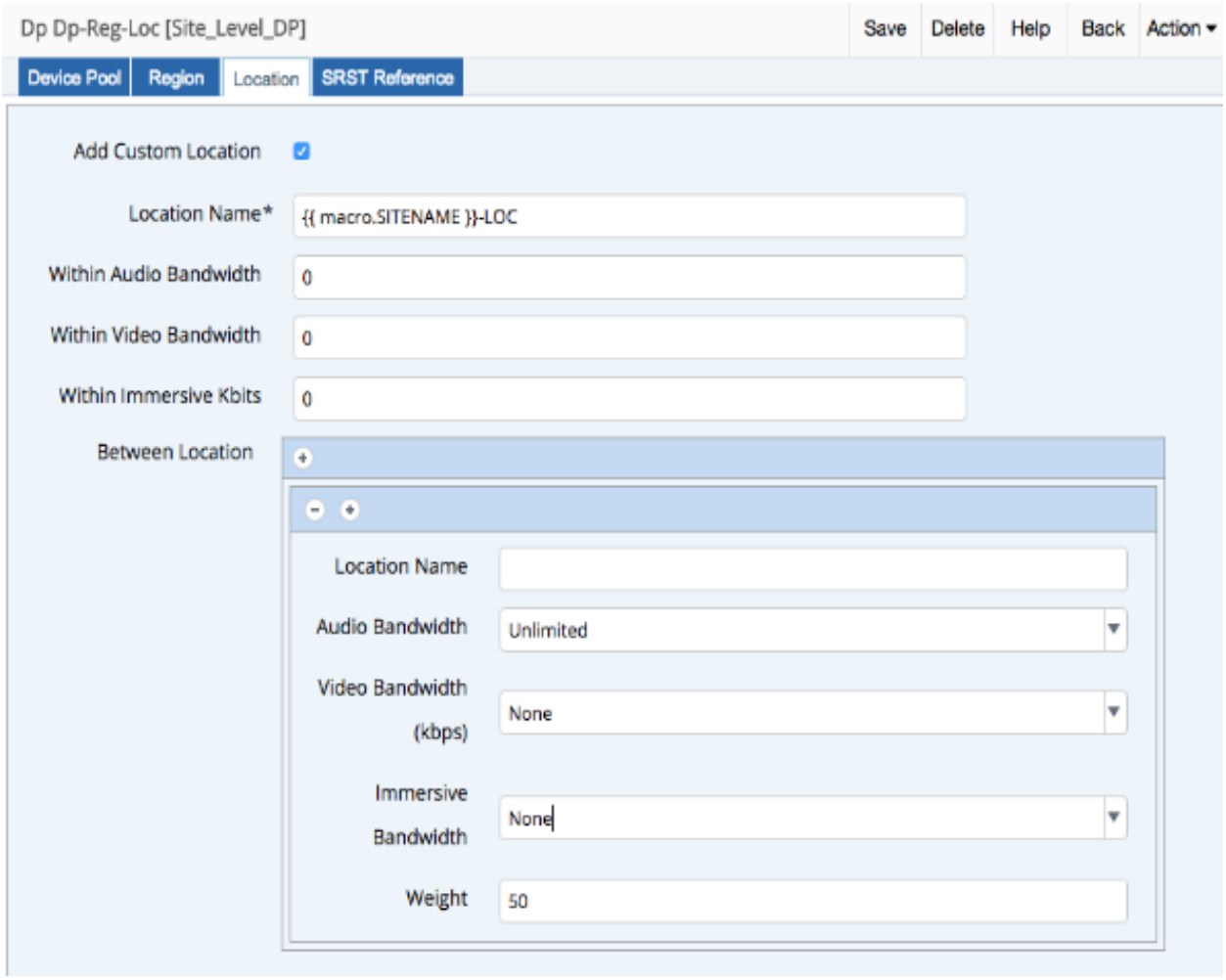
The Device Pool, Region, Location and SRST Reference dial plan model have been combined into one coherent data model for ease of entry into a call manager since the elements are often related.



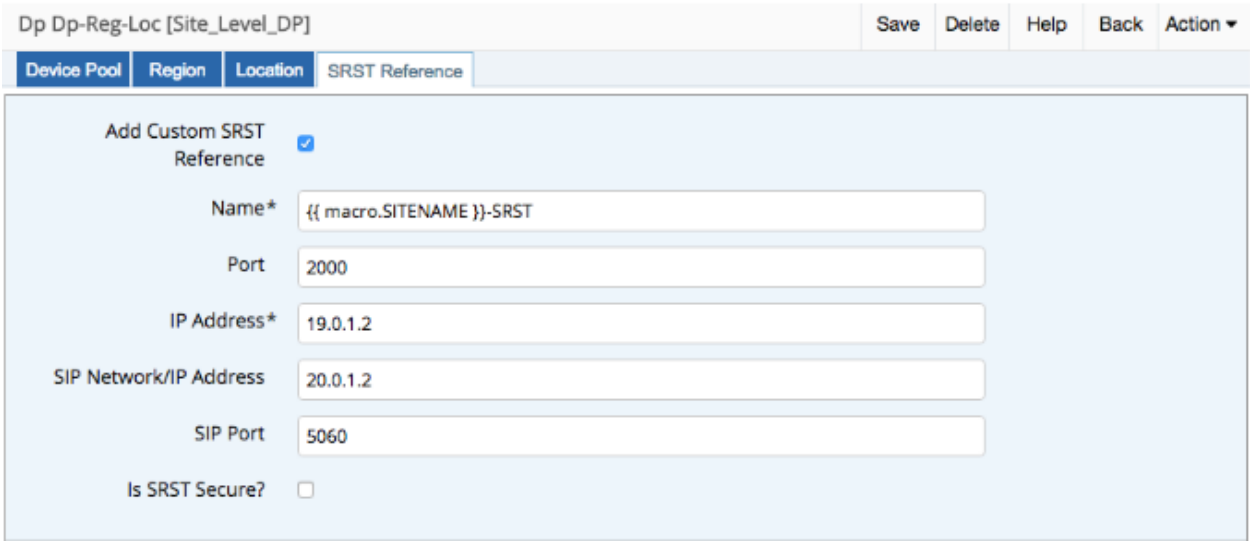
- **Device Pool** tab fields:
  - **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
  - **Device Pool Name**: Free text field to add a device pool name or macro. In this example the name is built using a macro reference and a static extension of `-DP`.
  - **Call Manager Group**: Free text field to add a call manager group name.
  - **Region**: Free text field to enter a call manager existing region to the device pool or the field will automatically update with the name of the custom added region from the **Region** tab.
  - **Location**: Free text field to enter a call manager existing location to the device pool or the field will automatically update with the name of the custom added location from the **Location** tab.
  - **SRST Reference**: Free text field to enter a call manager existing SRST reference to the device pool or the field will automatically update with the name of the custom added SRST reference from the **SRST Reference** tab.
  - **Date/Time Group**: Free text field to add a date time group name.



- **Region** tab fields:
  - **Add Custom Region**: Check box to optionally add a custom region.
  - **Region Name**: Free text field to add a region name. In this example the name is built using a macro reference and a static extension of `-REG`.
  - **Related Region**: Ability to add related regions to the custom region.
    - **Related Region Name**: Free text field to add a related region.
    - **Codec Preference**: Drop-down with choices:
      - Use System Default
      - Factory Default lossy
      - Factory Default low loss
    - **Audio Bandwidth**: Drop-down with choices:
      - Use System Default
      - 7 kbps (GSM-HR, G.723.1)
      - 8 kbps (G.729)
      - 13 kbps (GSM-FR, AMR)
      - 16 kbps (iLBC, G.728)
      - 24 kbps (AMR-WB)
      - 32 kbps (iSAC, G.722.1)
      - 64 kbps (G.711)
      - 128 kbps (AAC-LD [LATM])
      - 256 kbps (L16, AAC-LD)
    - **Video Bandwidth**: Drop-down to choose video bandwidth setting with choices:
      - Use System Default
      - Not Allowed
    - **Immersive Video Bandwidth**: Drop-down to choose immersive video bandwidth with choices:
      - Use System Default
      - Not Allowed
    - **Lossy Network**: Drop-down to choose lossy network setting with choices:
      - Use System Default
      - Keep Current Setting
      - Low Loss
      - Lossy



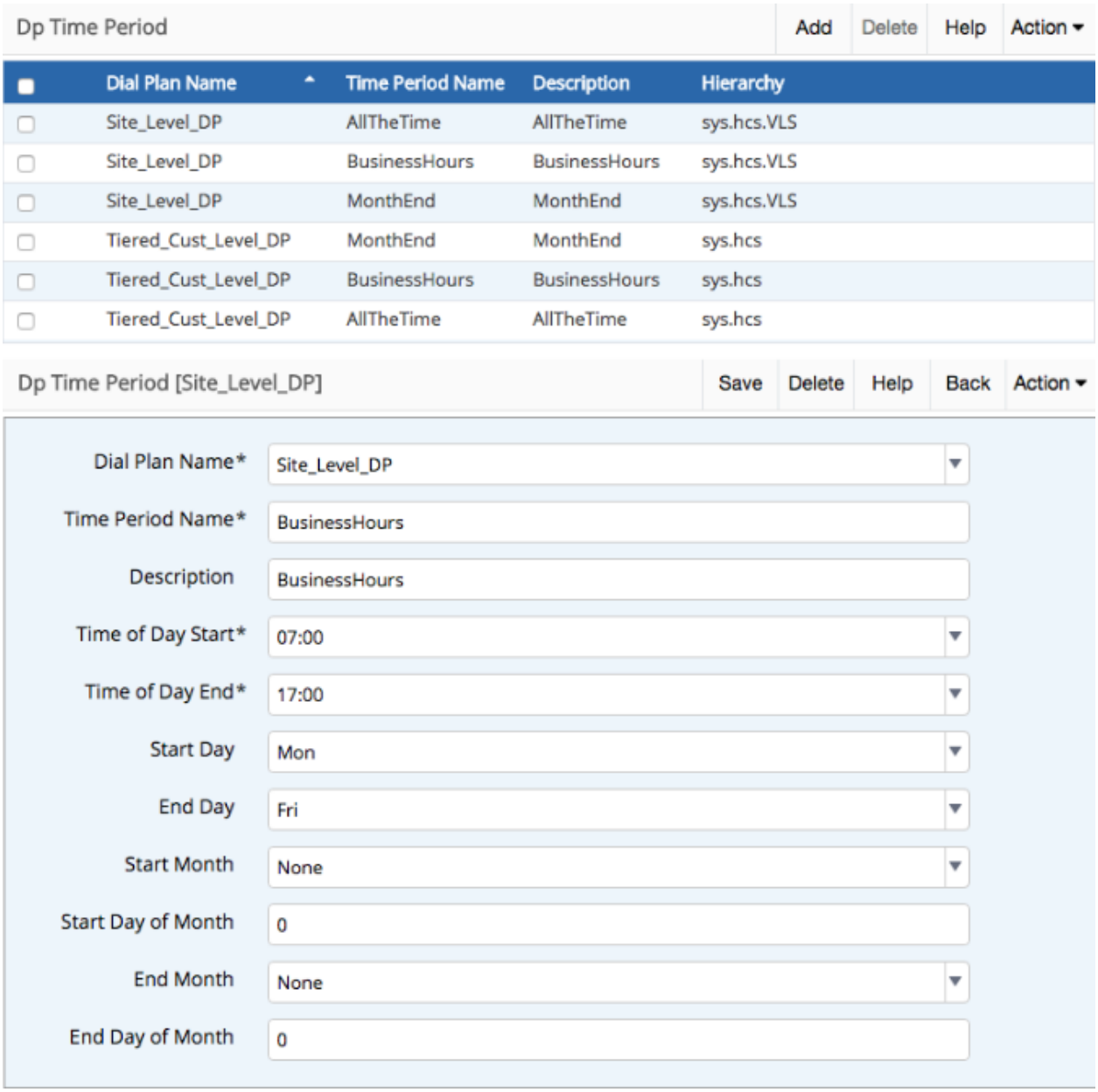
- **Location** tab fields:
  - **Add Location**: Check box to optionally add a custom Location.
  - **Location Name**: Free text field to add a location name. In this example the name is built using a macro reference and a static extension of `-LOC`.
  - **Within Audio Bandwidth**
  - **Within Video Bandwidth**
  - **Within Immersive Kbits**
  - **Between Location** group of fields:
    - **Location Name**
    - **Audio Bandwidth**
    - **Video Bandwidth**
    - **Immersive Bandwidth**
    - **Weight**



- **SRST Reference** tab fields:
  - **Add SRST Reference**: Check box to optionally add a custom SRST Reference.
  - **SRST Reference Name**: Free text field to add a SRST Reference name. In this example the name is built using a macro reference and a static extension of `-SRST`.
  - **Port**
  - **IP Address**
  - **SIP Network/IP Address**
  - **SIP Port**
  - **SRST Secure?**

Time Period Model

This allows the administrator to define an unlimited number of time periods.



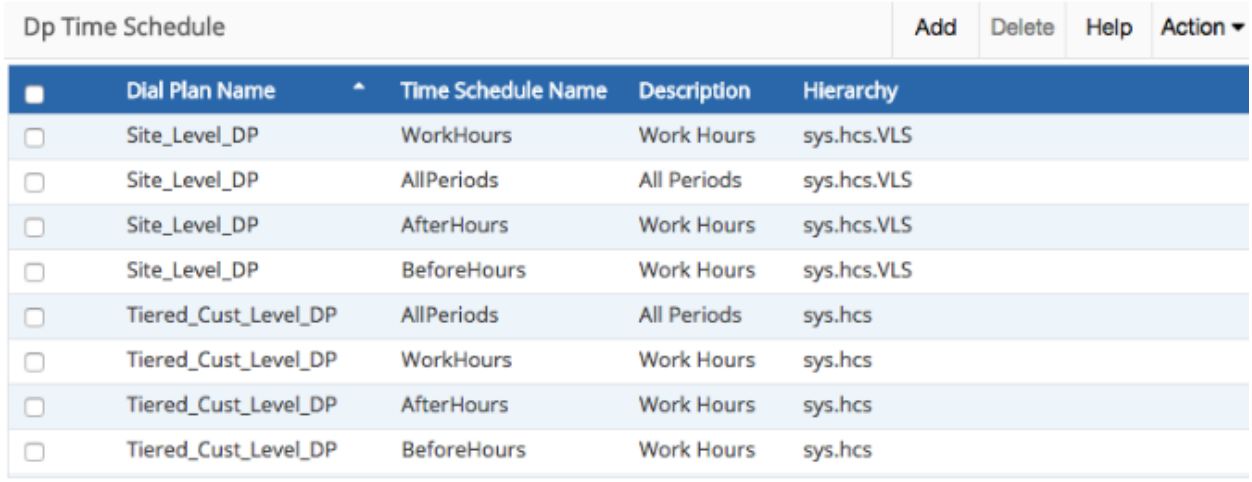
Time Period fields:

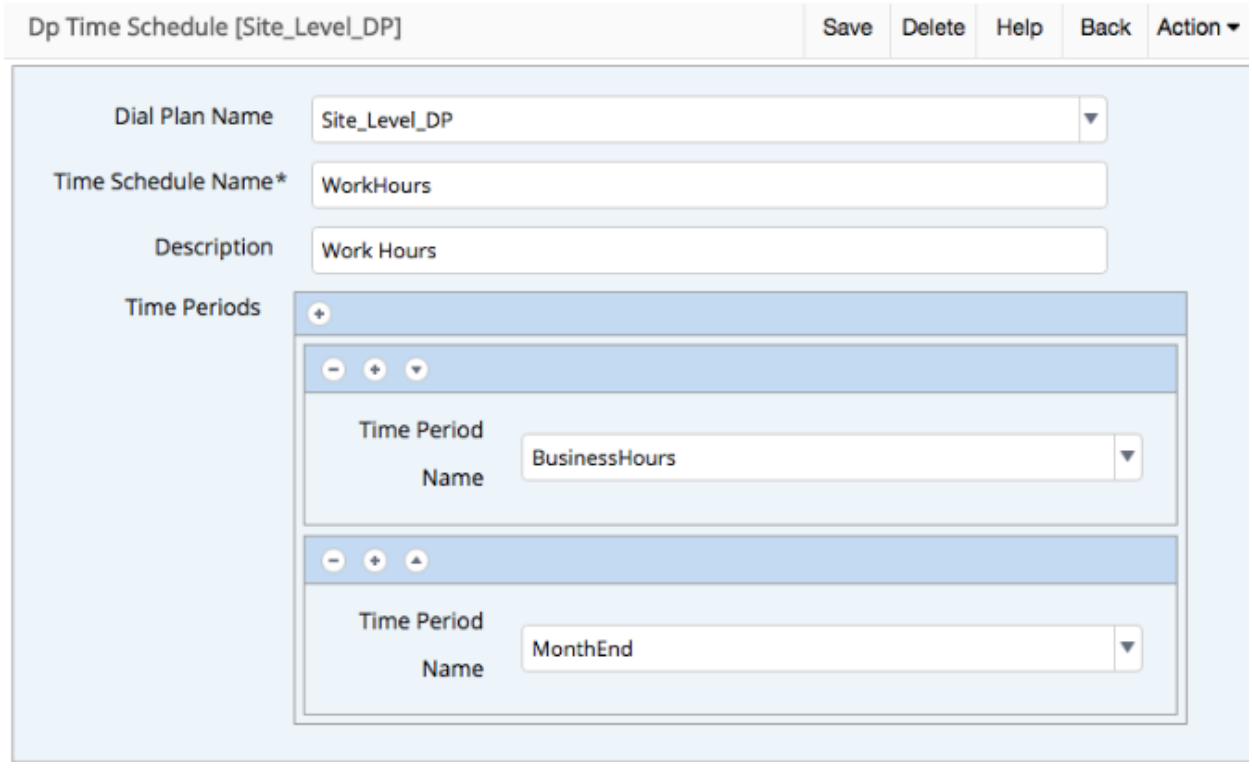
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Time Period Name**: The free text name for desired time period.
- **Description**: Meaningful description of the time period.
- **Time of Day Start**: Drop-down driven field to set start of time period in 15 minute increments.
- **Time of Day End**: Drop-down driven field to set end of time period in 15 minute increments.
- **Start Day**: Drop-down driven field to set start day giving “Mon”-“Fri” and “None” as options.
- **End Day**: Drop-down driven field to set end day giving “Mon”-“Fri” and “None” as options.
- **Start Month**: Drop-down driven field to set start month giving “Jan”-“Dec” and “None” as options.

- **Start Month**: Drop-down driven field to set start month giving “Jan”-“Dec” and “None” as options.
- **Start Day of Month**: Free text field to add integer of start day of the month
- **End Month**: Drop-down driven field to set end month giving “Jan”-“Dec” and “None” as options.
- **End Day of Month**: Free text field to add integer of start day of the month.

Time Schedule Model

This allows the administrator to define an unlimited number of time schedules.



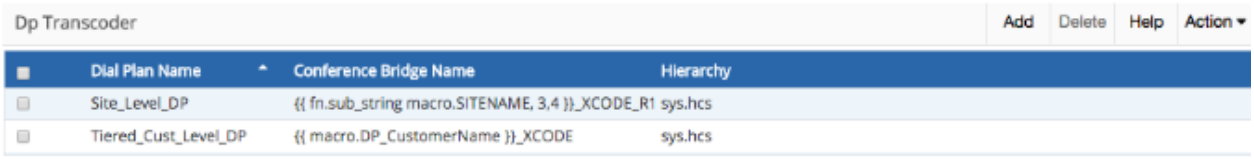


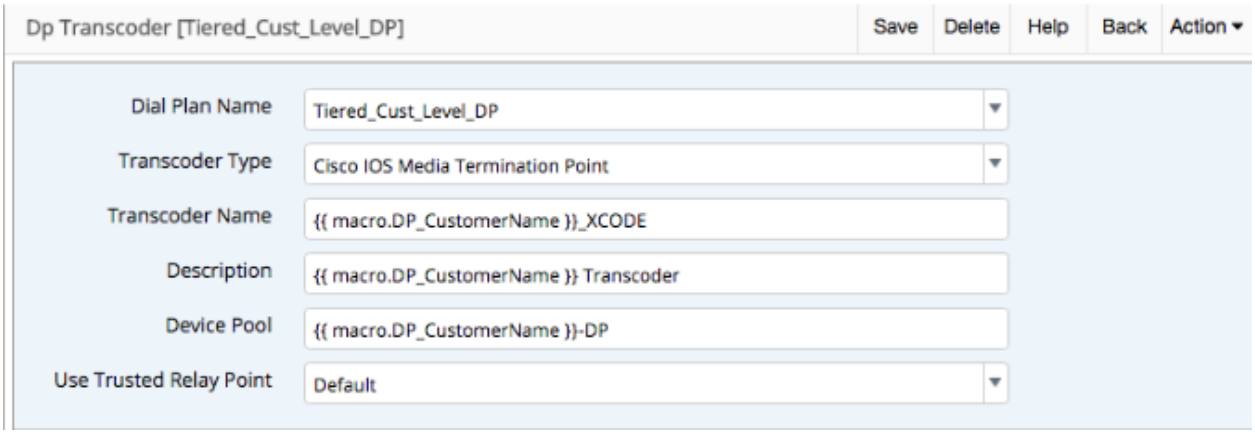
Time Schedule fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Time Schedule Name**: Free text field to enter a unique time schedule name.
- **Description**: Meaningful description of the time schedule.
- **Time Periods**: An array of time periods that provides drop-downs of time periods defined from the Time Period.

Transcoder Model

The transcoder dial plan model allows the administrator to define an unlimited number of transcoders.



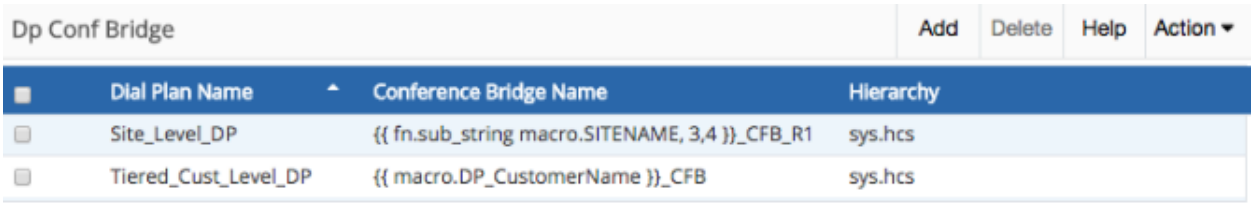


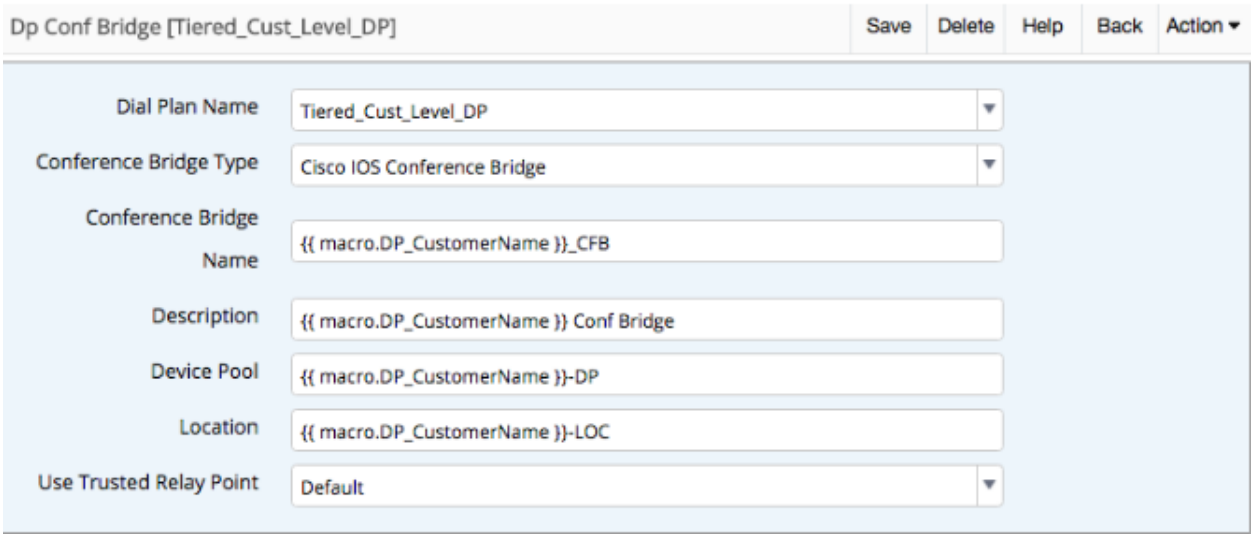
Transcoder fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type
- **Transcoder Type**: Drop-down field to set Transcoder Type. Currently only supports Cisco IOS Media Termination Point but will be expanded based on market input.
- **Transcoder Name**: Free Text field where a unique name should be entered. In the above example the macro will fill the VOSS customer name with `_XCODE` suffix.
- **Description**: Meaningful description of the transcoder
- **Device Pool**: Free text field to identify the proper device pool.
- **Use Trusted Relay Point**: Drop-down with values:
  - Default
  - Off
  - On

Conference Bridge Model

The Conference Bridge dial plan model allows the administrator to define an unlimited number of Conference Bridges.



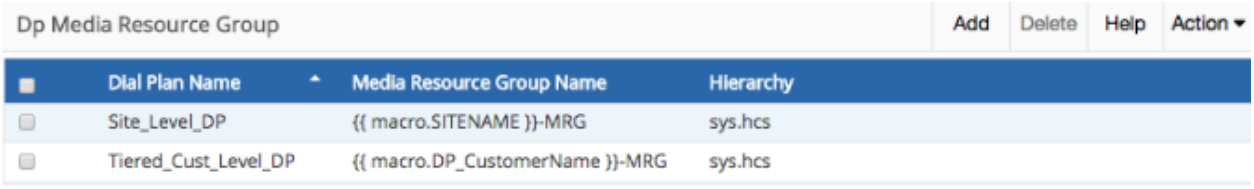


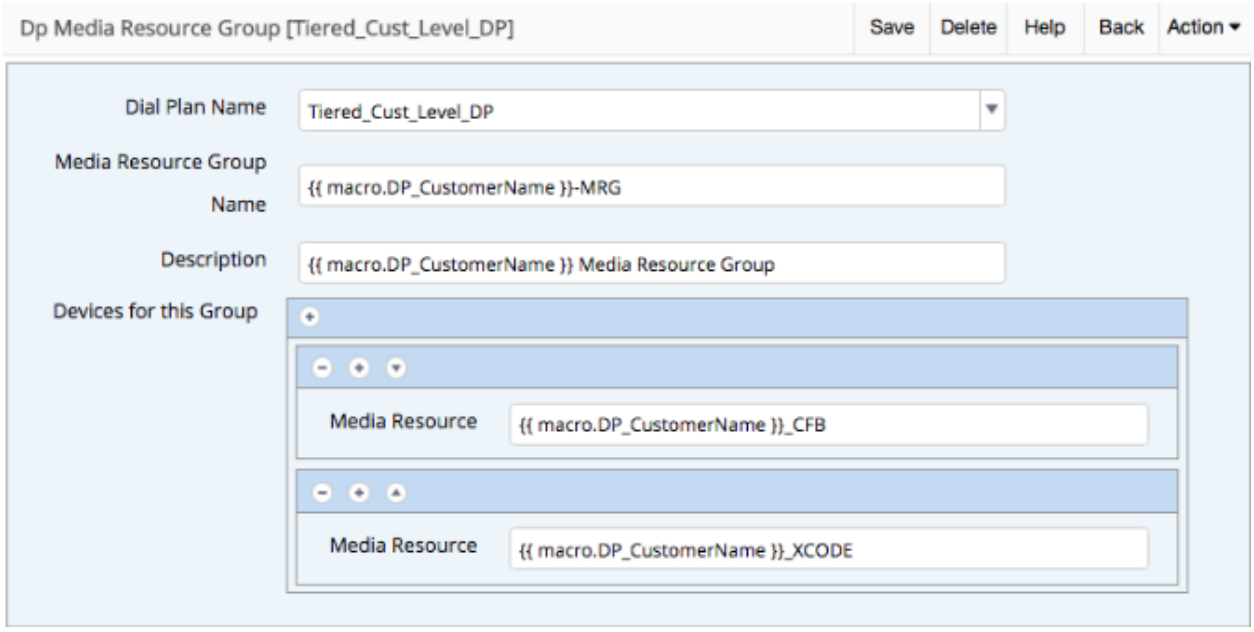
Conference Bridge fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Conference Bridge Type**: Drop-down field to set Transcoder Type. Currently only supports Cisco IOS Conference Bridge but will be expanded based on market input.
- **Conference Bridge Name**: Free Text field where a unique name should be entered. In the above example the macro will fill the VOSS customer name with `_CFB` suffix.
- **Description**: Meaningful description of the Conference Bridge.
- **Device Pool**: Free text field to identify the proper Device Pool.
- **Location**: Free text field to identify the proper Location.
- **Use Trusted Relay Point**: Drop-down with values:
  - Default
  - Off
  - On

Media Resource Group Model

The Media Resource Group dial plan model allows the administrator to define an unlimited number of Media Resource Groups.



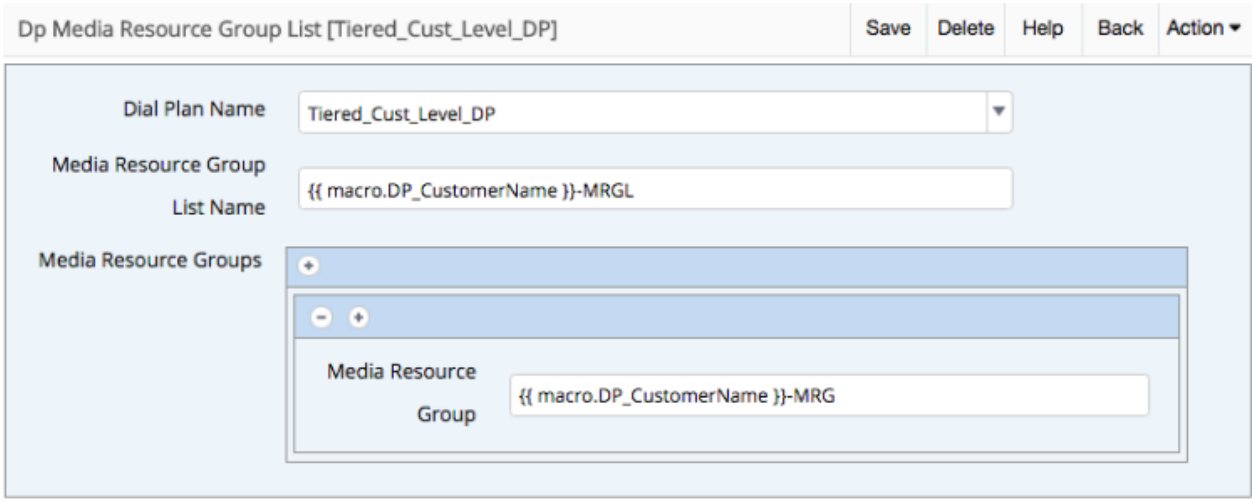


Media Resource Group fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Media Resource Group Name**: Free text field to enter a unique name for the Media Resource Group.
- **Description**: Meaningful description of the Media Resource Group.
- **Devices for this Group**: Array of member media resources for the Media Resource Group. In this instance using macros to enter the two customer level Transcoder and Conference Bridge instances.

Media Resource Group List Model

The Media Resource Group List dial plan model allows the administrator to define an unlimited number of Media Resource Group Lists.

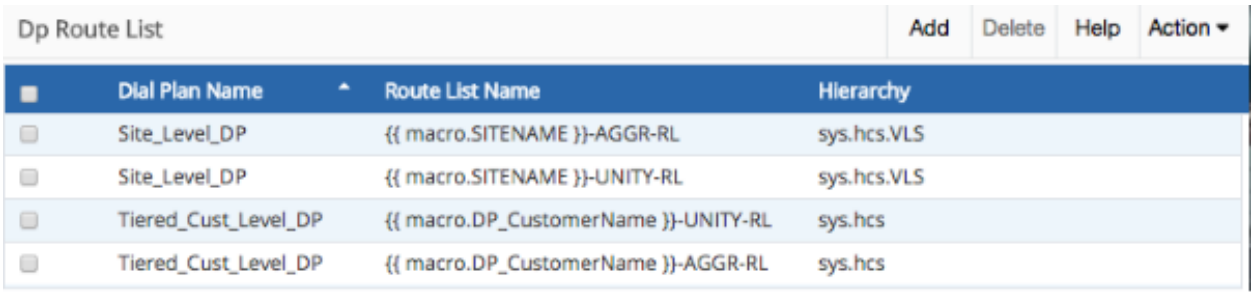


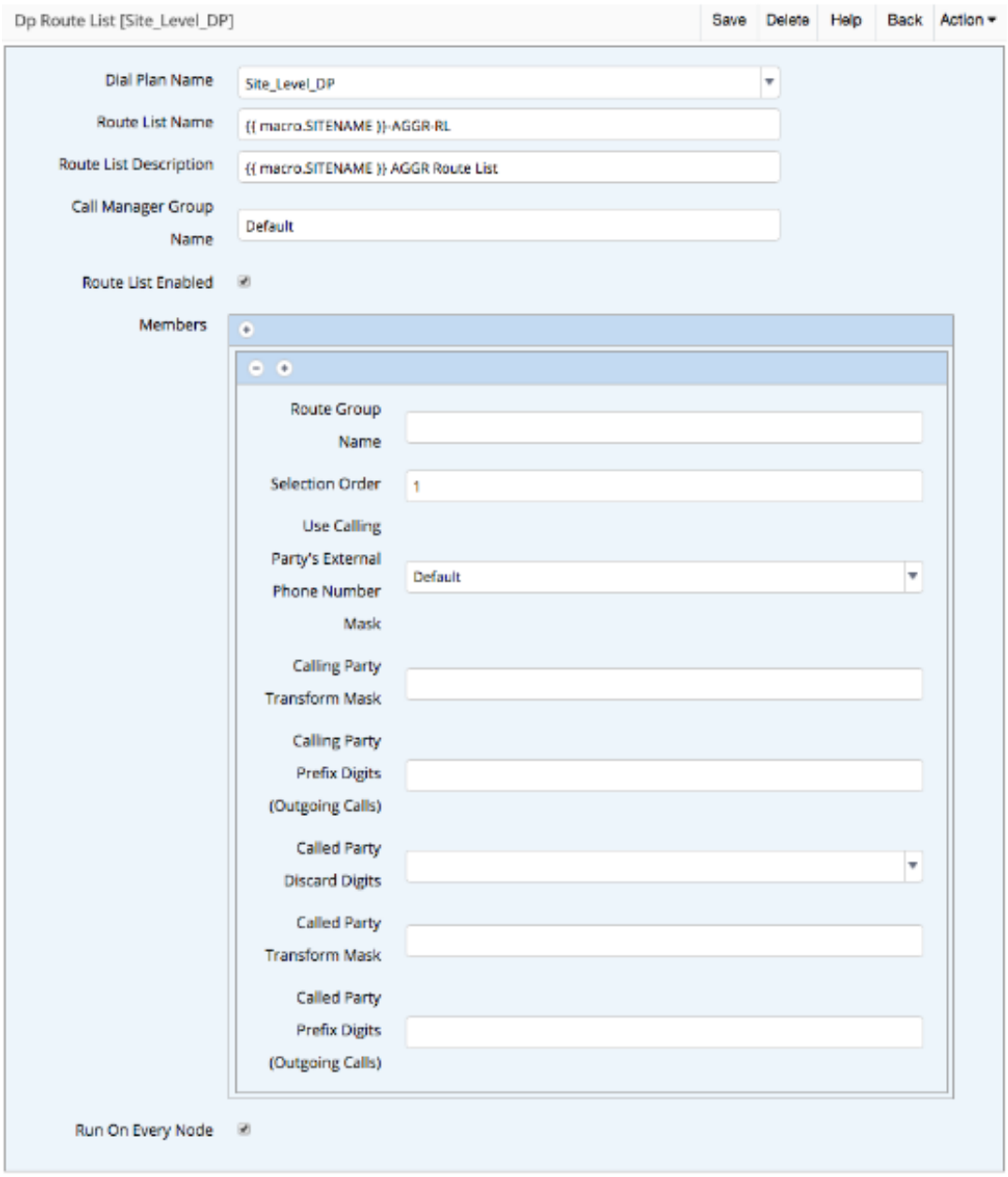
Media Resource Group List fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Media Resource Group List Name**: Free text field to enter a unique name for the Media Resource Group List
- **Media Resource Groups**: Array of media resource groups to assign to the Media Resource Group List. In this example binding the customer level MRG.

Route List Model

The Route List dial plan model allows the administrator to define an unlimited number of Route Lists.





Route List fields:

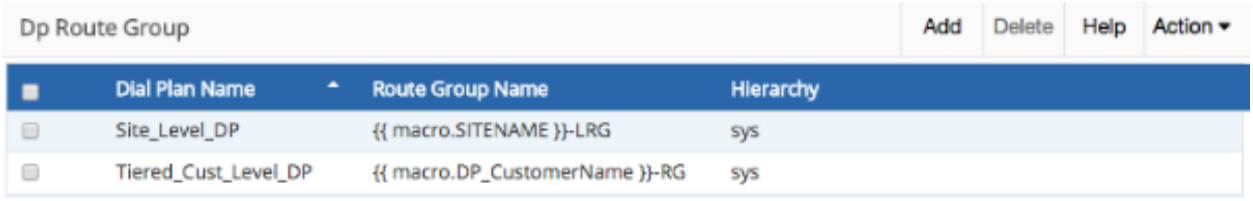
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.

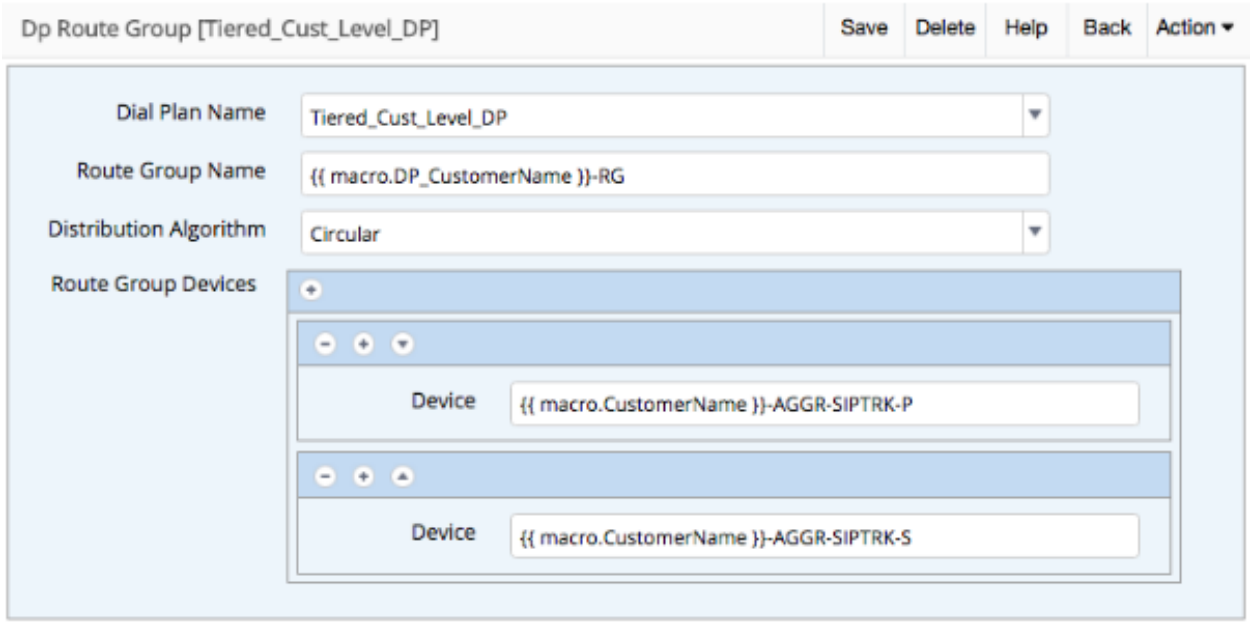
- **Route List Name**: Free text field to enter a unique name for the Route List
- **Route List Description**: Meaningful description of the Route List.
- **Call Manager Group Name: Free text field to designate the proper Call Manager** Group
- **Route list Enabled**: Check box to set the Route List Enabled field in Call Manager.
- **Members**: Array to enter member elements to the route list.
  - **Route Groups Name**: Free text field to assign a route group to the Route List.
  - **Selection Order**: The order in which the Route Groups will be placed in the Route List.
  - Use Calling Party's External Phone Number Mask: Drop-down providing Call Manager available options:
    - Default
    - On
    - Off
  - **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
  - **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
  - **Called Party Discard Digits**: Drop-down providing Call Manager available options:
    - None
    - PreDot
    - PreDot Trailing-#

  Note that more discard instructions may be added at market demand.
  - **Called Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
  - **Called Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Called Party Prefix Digit data

Route Group Model

The Route Group dial plan model allows the administrator to define an unlimited number of Route Groups.



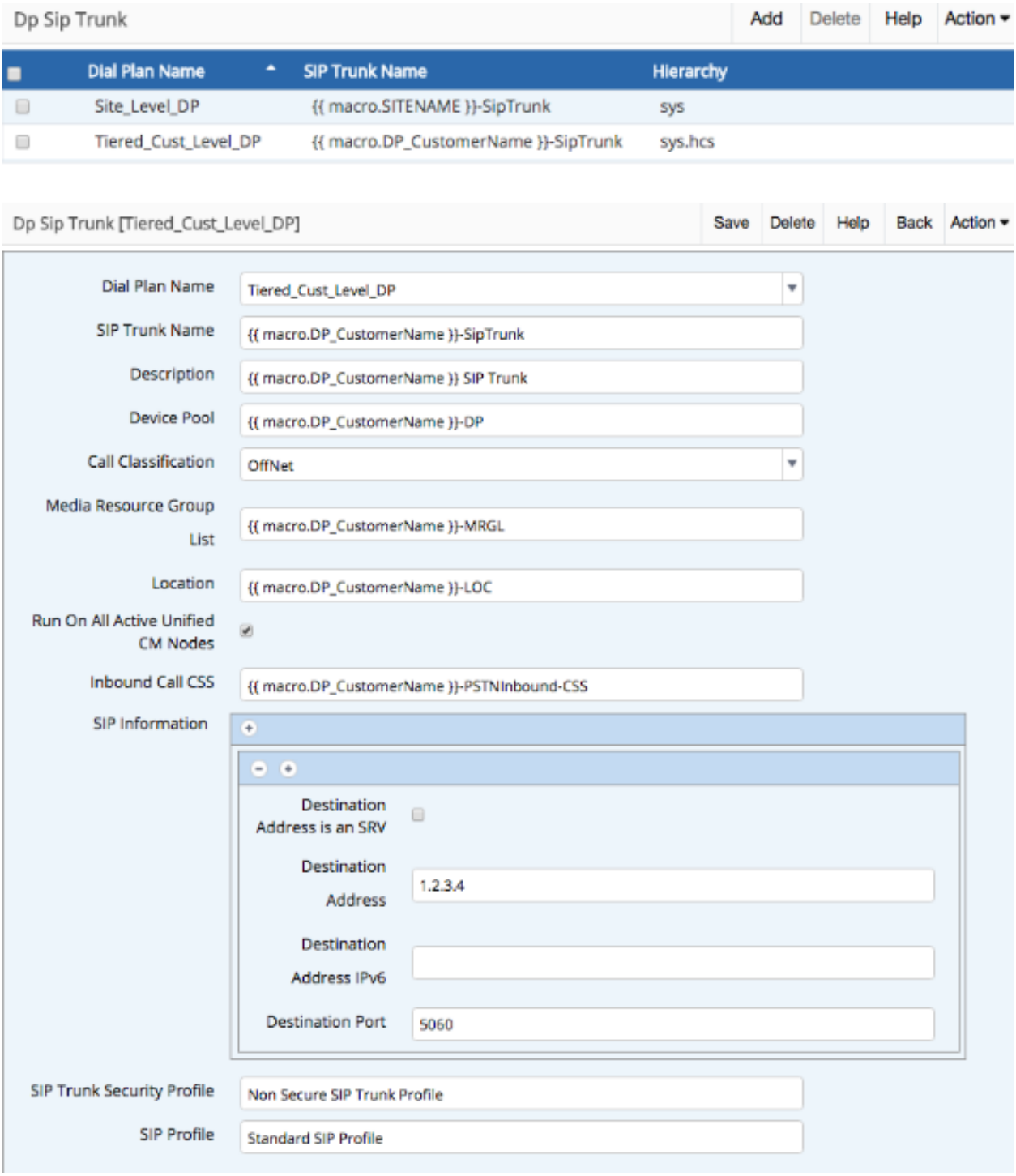


Route Group fields:

- **Dial Plan** Name: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Route Group** Name: Free text field to enter a unique name for the Route Group
- **Distribution Algorithm**: Drop-down providing the Call Manager options:
  - Top Down
  - Circular
  - Longest Idle Time
  - Broadcast
- **Route Group Devices**: Array to add devices to the route group. In this example a primary and secondary SIP trunk to aggregation.

SIP Trunk Model

The SIP Trunk dial plan model allows the administrator to define an unlimited number of SIP Trunks.



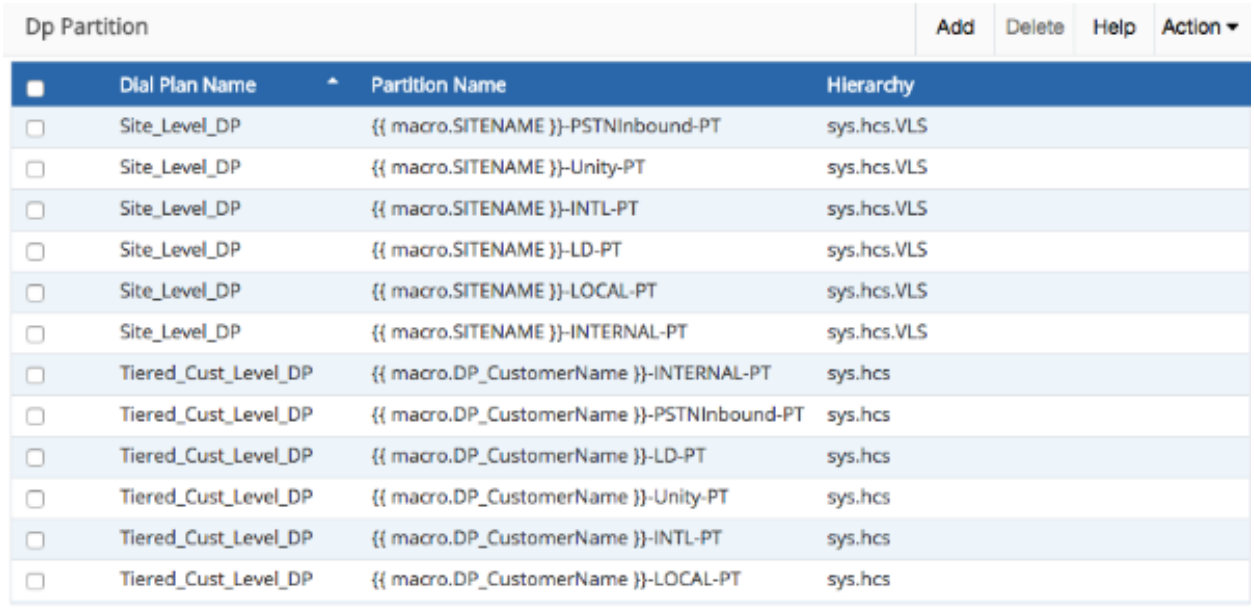
SIP Trunk fields:

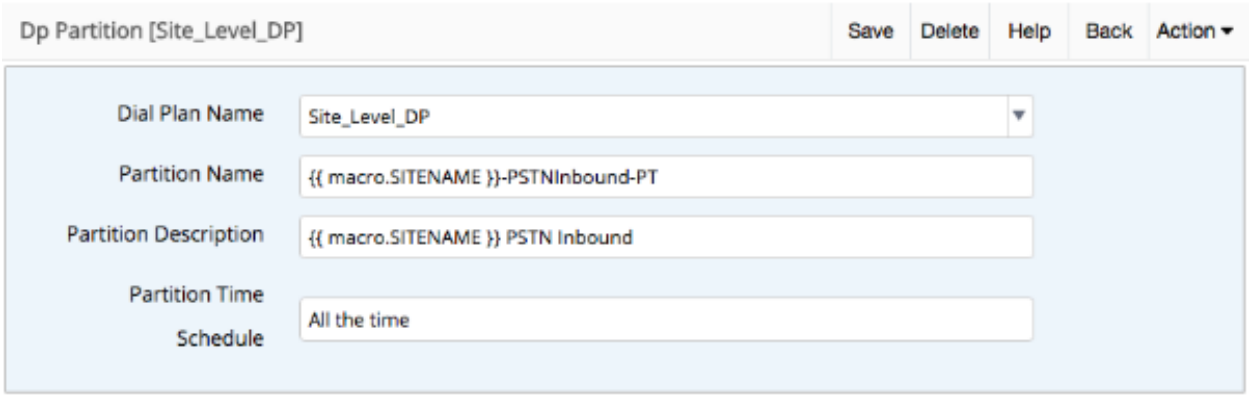
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **SIP Trunk Name**: Free text field to enter a unique name for the SIP Trunk
- **Description**: Meaningful description of the SIP Trunk.
- **Device Pool**: Free text field to enter the proper device pool for the trunk

- **Call Classification**: Drop-down providing Call Manager options:
  - Offnet
  - OnNet
  - Use System Default
- **Media Resource Group List**: Free text field to enter the proper MRGL for the SIP Trunk.
- **Location**: Free text field to enter the proper Location for the SIP Trunk.
- **Run On All Active CM Nodes**: Check box to set the run on all nodes option.
- **Inbound Call CSS**: Free text field to enter the proper CSS for SIP Trunks per dial plan.
- **SIP Information**: Array to add multiple SIP IP Destination:
  - **Destination Address**: The IPv4 IP address of the destination.
  - **Destination Address IPv6**: The IPv6 of the destination.
  - **Destination Port**: The TCP/IP port for the SIP Trunk instance.
- **SIP Trunk Security Profile**: Free text field to enter a valid SIP Trunk Security Profile.
- **SIP Profile**: Free text field to enter a valid SIP Profile.

Partition Model

The Partition dial plan model allows the administrator to define an unlimited number of Partitions.





Partition fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Partition Name**: Free text field to enter a unique name for the Partition.
- **Partition Description**: Meaningful description of the Partition.
- **Partition Time Schedule**: Time schedule for the Partition if required per dial plan. May be left blank.

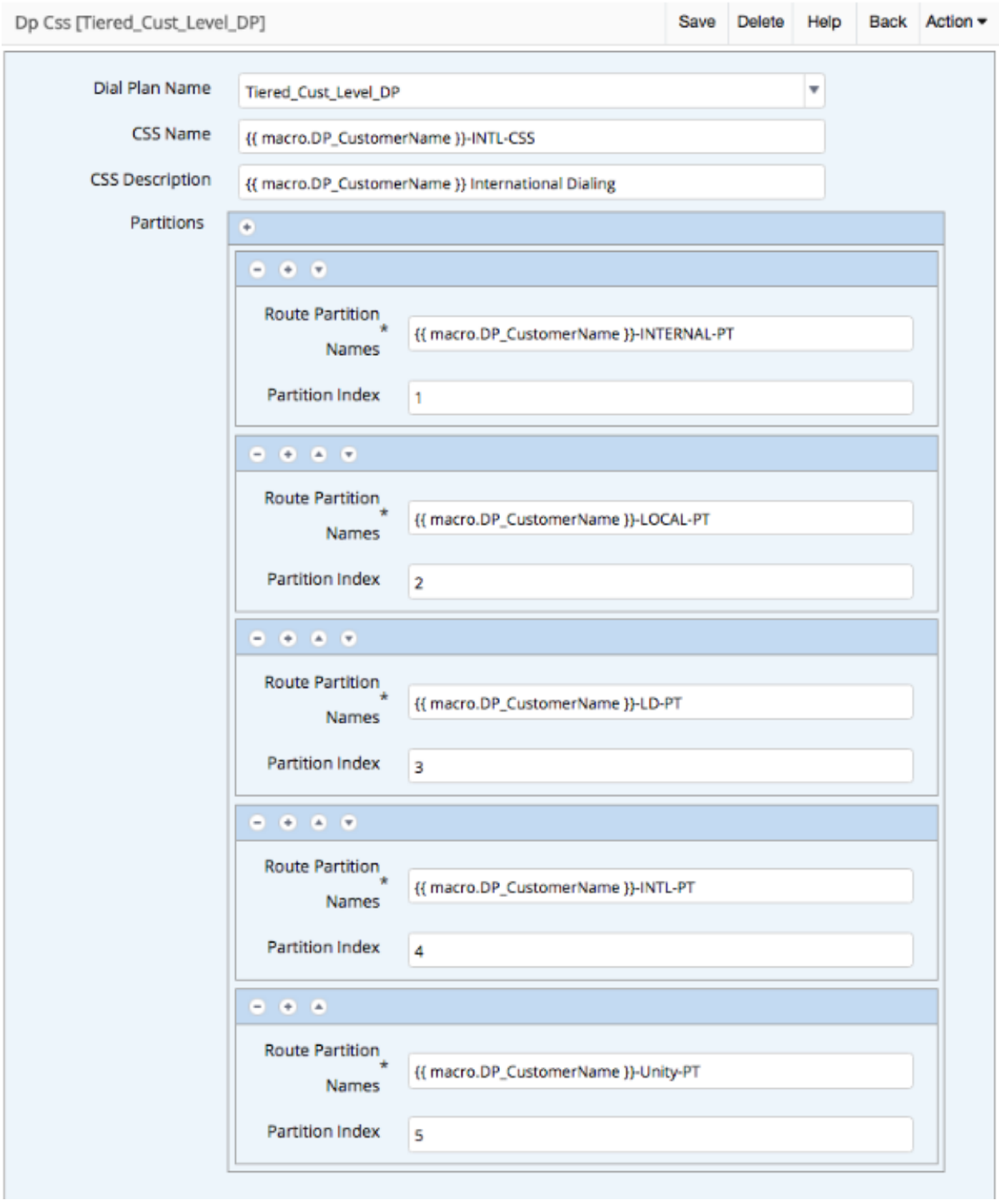
Calling Search Space Model

The Calling Search Space (CSS) dial plan model allows the administrator to define an unlimited number of CSS.

Dp Css

Add | Delete | Help | Action

Dial Plan Name	CSS Name	Hierarchy
Site_Level_DP	{{ macro.SITENAME }}-PSTNInbound-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-LD-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-LOCAL-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-CSS	sys.hcs.VLS
Site_Level_DP	{{ macro.SITENAME }}-INTL-CSS	sys.hcs.VLS
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-PSTNInbound-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTL-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LD-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-INTERNAL-CSS	sys.hcs
Tiered_Cust_Level_DP	{{ macro.DP_CustomerName }}-LOCAL-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-LD-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-INTL-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-INTERNAL-CSS	sys.hcs
Tiered_Site_Level_DP	{{ macro.SITENAME }}-LOCAL-CSS	sys.hcs



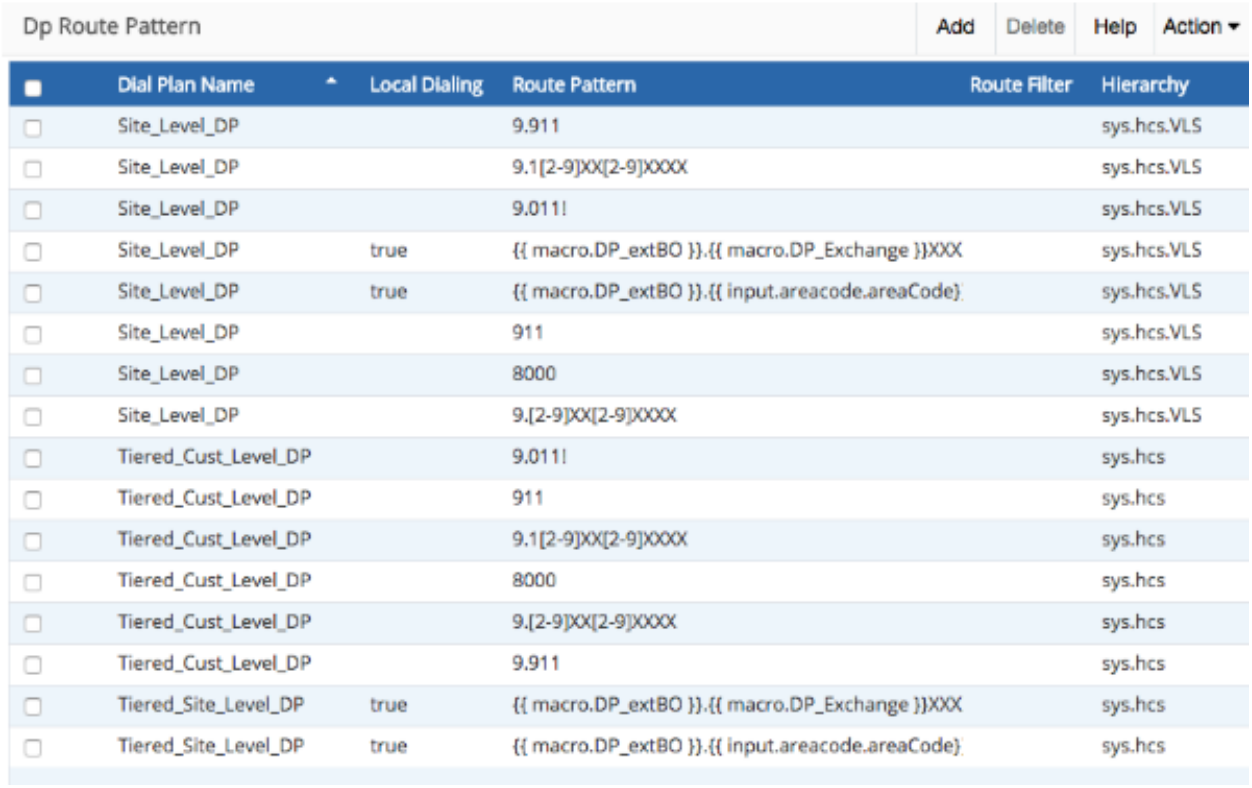
CSS fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **CSS Name**: Free text field to enter a unique name for the CSS.
- **CSS Description**: Meaningful description of the CSS.

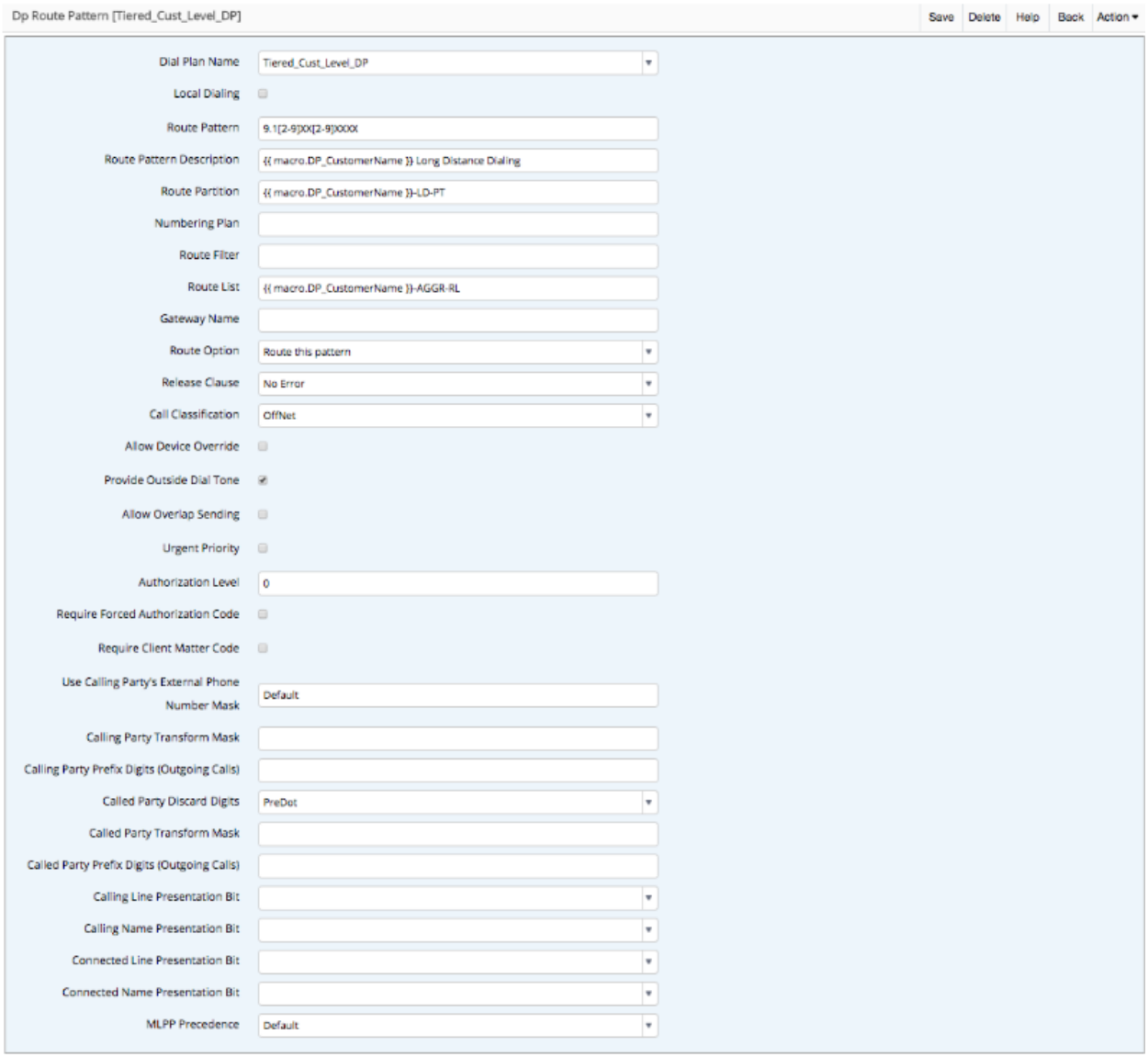
- **Partitions**: Array to add Partitions associated in order to the CSS.
  - **Route Partition Name**: Free text field to enter valid Partition name
  - **Partition Index**: Free text field to enter the numeric id for Partition order.

Route Pattern Model

The Route Pattern dial plan model allows the administrator to define an unlimited number of Route Patterns. “Local Dialing” flag will be covered in a following section.



Dial Plan Name	Local Dialing	Route Pattern	Route Filter	Hierarchy
Site_Level_DP		9.911		sys.hcs.VLS
Site_Level_DP		9.1[2-9]XX[2-9]XXXX		sys.hcs.VLS
Site_Level_DP		9.011!		sys.hcs.VLS
Site_Level_DP	true	{{ macro.DP_extBO }}.{{ macro.DP_Exchange }}XXX		sys.hcs.VLS
Site_Level_DP	true	{{ macro.DP_extBO }}.{{ input.areacode.areaCode}		sys.hcs.VLS
Site_Level_DP		911		sys.hcs.VLS
Site_Level_DP		8000		sys.hcs.VLS
Site_Level_DP		9.[2-9]XX[2-9]XXXX		sys.hcs.VLS
Tiered_Cust_Level_DP		9.011!		sys.hcs
Tiered_Cust_Level_DP		911		sys.hcs
Tiered_Cust_Level_DP		9.1[2-9]XX[2-9]XXXX		sys.hcs
Tiered_Cust_Level_DP		8000		sys.hcs
Tiered_Cust_Level_DP		9.[2-9]XX[2-9]XXXX		sys.hcs
Tiered_Cust_Level_DP		9.911		sys.hcs
Tiered_Site_Level_DP	true	{{ macro.DP_extBO }}.{{ macro.DP_Exchange }}XXX		sys.hcs
Tiered_Site_Level_DP	true	{{ macro.DP_extBO }}.{{ input.areacode.areaCode}		sys.hcs



Route Pattern fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Local Dialing**: Check box to identify special patterns.
- **Route Pattern**: Free text field to enter a common Call Manager routing pattern.
- **Route Pattern Description**: Meaningful description of the Route Pattern.
- **Route Partition**: Free text field to enter a valid CUCM Partition.
- **Numbering Plan**: Free text field to enter a valid CUCM Numbering Plan if IDP is utilized.
- **Route Filter**: Free text field to enter a valid route filter name.
- **Route List**: Free text field to enter a valid route list name.
- **Gateway Name**: Free text field to enter a valid gateway name.
- **Route Option**: Drop-down providing Call Manager option:

  - Route this pattern
  - Block this pattern
- **Release Clause**: Drop-down providing Call Manager option:
  - No Error
  - Unallocated Number
  - Call Rejected
  - Number Changed
  - Invalid Number Format
  - Precedence Level Exceeded
- **Call Classification**: Drop-down providing Call Manager option:
  - Offnet
  - OnNet
- **Allow Device Override**: Check box to enable device override.
- **Provide Outside Dial Tone**: Check box to enable Outside Dial Tone.
- **Allow Overlap Sending**: Check box to enable Overlap Sending.
- **Urgent Priority**: Check box to enable Urgent Priority.
- **Authorization Level**: Free text box to enter Authorization Level as numeric value.
- **Require Forced Authorization Code**: Check box to enable Forced Authorization Code.
- **Require Client Matter Code**: Check box to enable Client Matter Code.
- **Use Calling Party's External Phone Number Mask**: Drop-down providing Call Manager available options:
  - Default
  - On
  - Off
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Called Party Discard Digits**: Drop-down providing Call Manager available options:
  - None
  - PreDot
  - PreDot Trailing-#

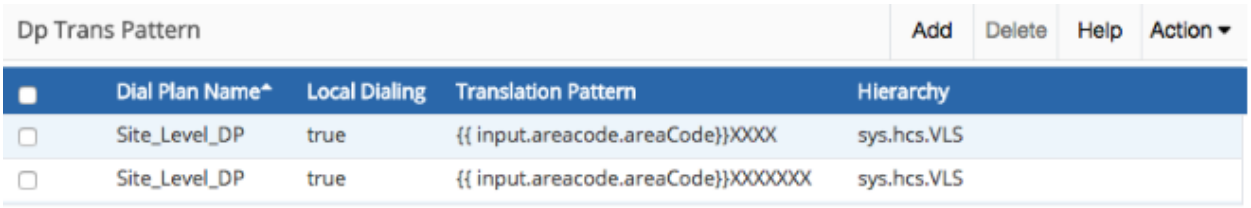
Note that more discard instructions may be added at market demand.

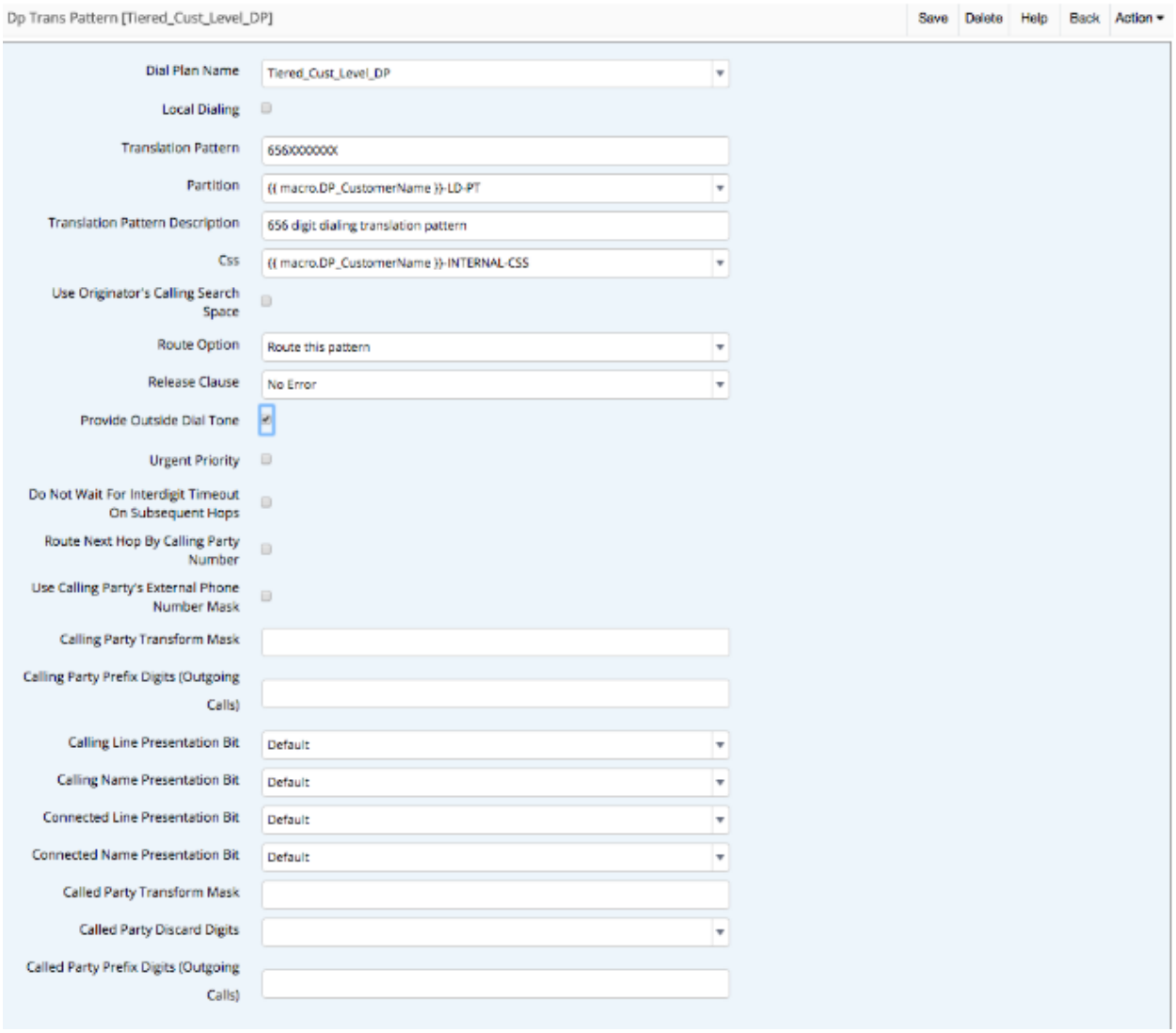
- **Called Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Called Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Called Party Prefix Digit data.
- **Calling Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default

  - Allowed
  - Restricted
- **Calling Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **MLPP Precedence**: Drop-down providing Call Manager available options:
  - Default
  - Executive Override
  - Flash
  - Flash Override
  - Immediate
  - Priority
  - Routine

Translation Pattern Model

The Translation Pattern dial plan model allows the administrator to define an unlimited number of Translation Patterns. “Local Dialing” flag will be covered in the following section.





Translation Pattern fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Local Dialing**: Check box to identify special patterns.
- **Translation Pattern**: Free text field to enter a common Call Manager translation pattern.
- **Partition**: Free text field to enter a valid partition for the Translation Pattern.
- **Translation Pattern Description**: Meaningful description of the Translation Pattern.

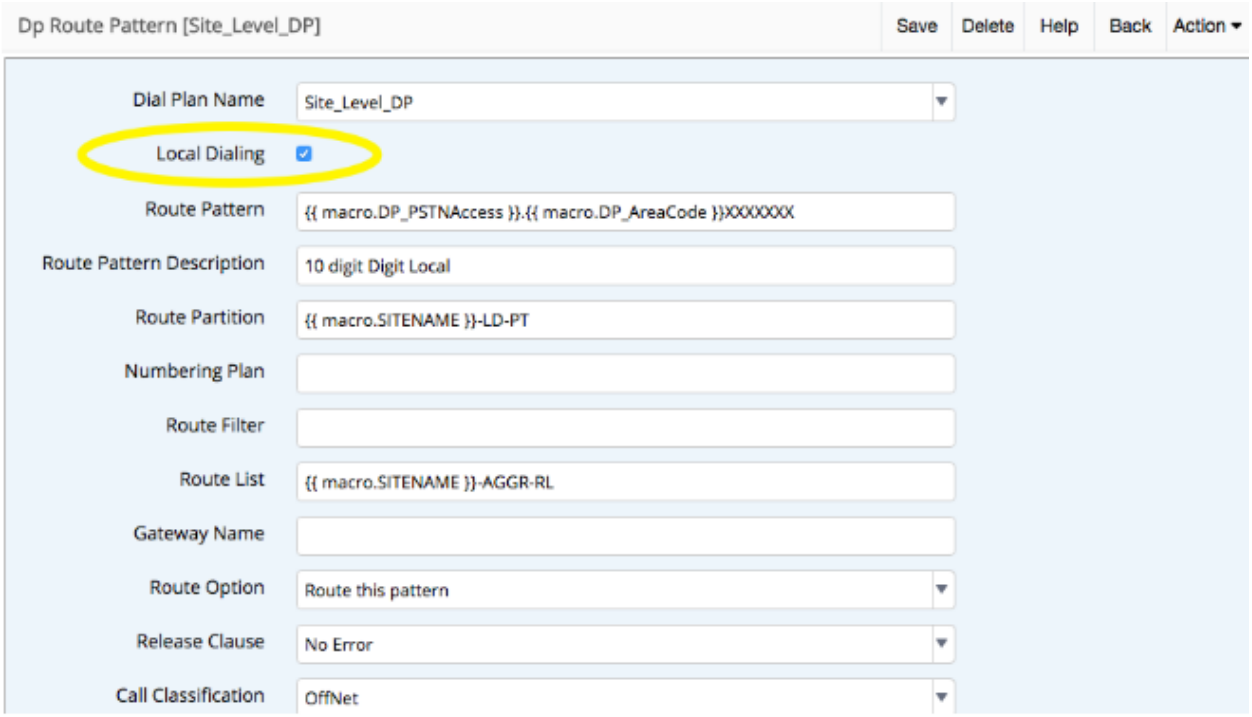
- **Css**: Free text field to assign a valid CSS per the dial plan.
- **Route Option**: Drop-down providing Call Manager options:
  - Route this pattern
  - Block this pattern
- **Release Clause**: Drop-down providing Call Manager options:
  - No Error
  - Unallocated Number
  - Call Rejected
  - Number Changed
  - Invalid Number Format
  - Precedence Level Exceeded
- **Provide Outside Dial Tone**: Check box to enable Outside Dial Tone.
- **Urgent Priority**: Check box to enable Urgent Priority.
- **Do Not Wait For Interdigit Timeout On Subsequent Hops**: Check box to bypass interdigit timeout.
- **Route Next Hop By Calling Party Number**: Check box to enable Route Next Hop By Calling Party Number.
- **Use Calling Party's External Phone Number Mask**: Check box to enable use of Calling Party's External Phone Number Mask.
- **Use Originator's Calling Search Space**: Check box to enable Originator's Calling Search Space.
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Calling Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed

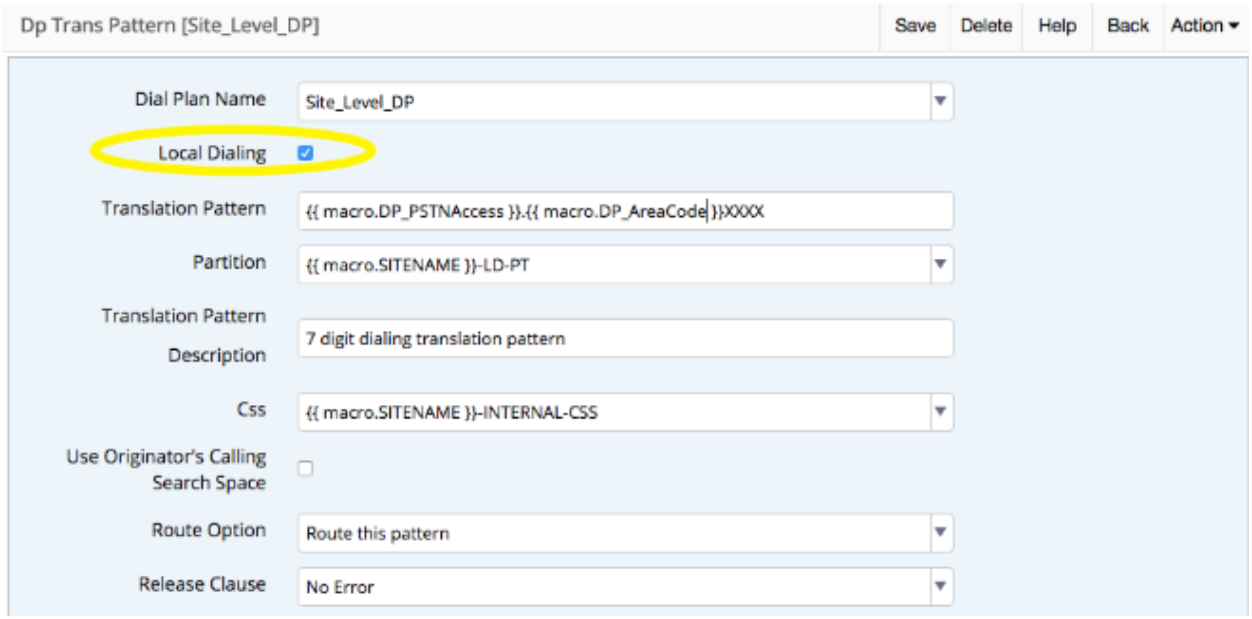
  - Restricted

- **Called Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data.
- **Called Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Called Party Prefix Digit data.

Route Pattern and Translation Pattern 'Local'

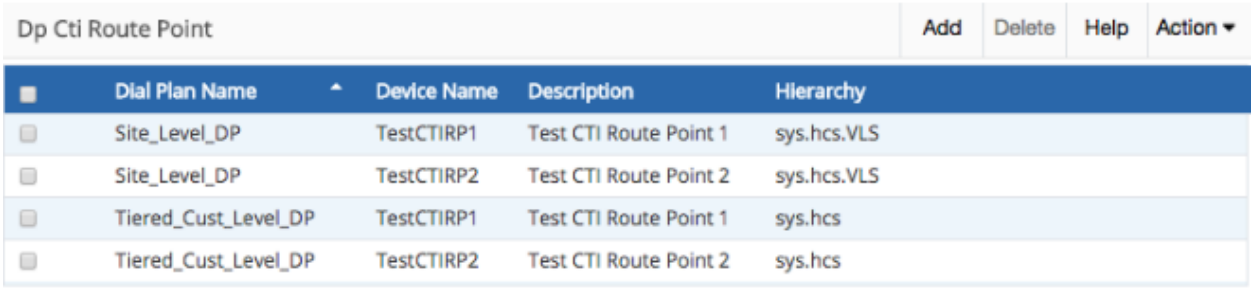
The Translation/Route Pattern local designation in dial plan model allows the administrator to define patterns as local or looping patterns from the Site/Customer dial plan input sheet. The dial plan input sheets allow for creating a list of local area code/exchange that can be referenced via macro values to create site or customer level unique patterns.

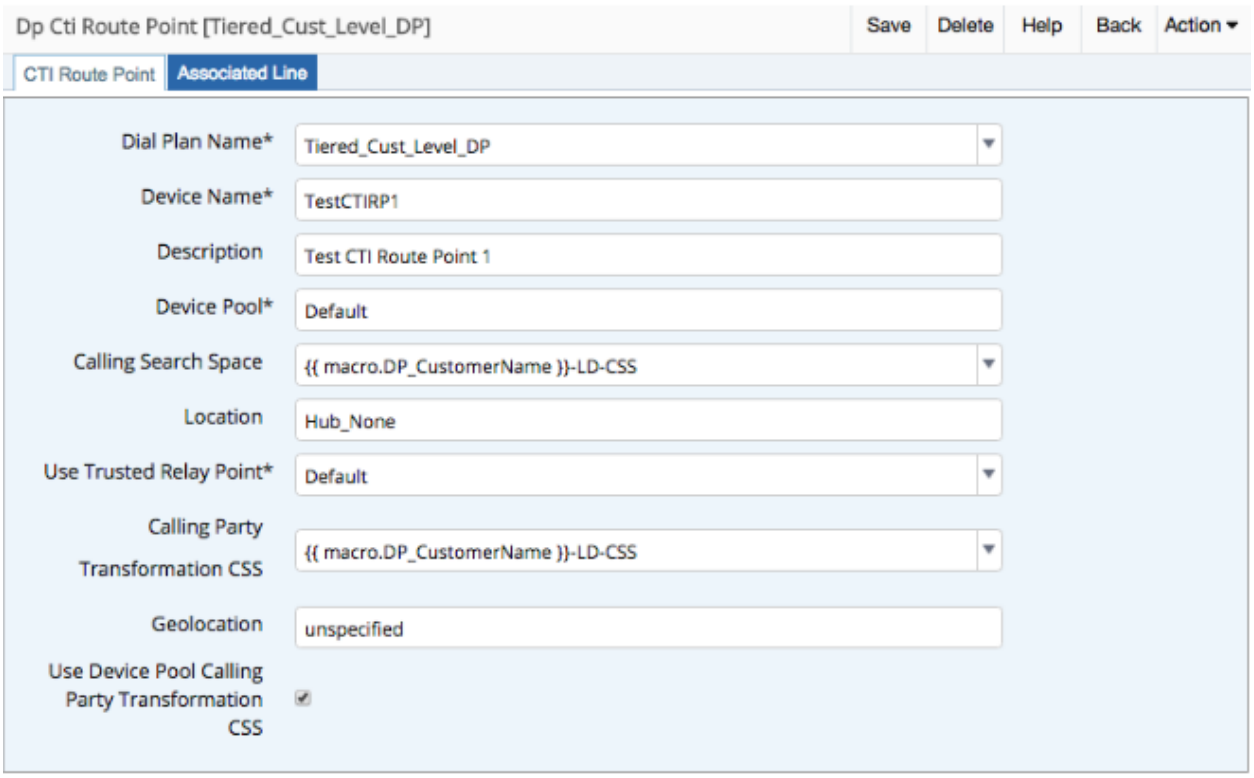




CTI Route Points

The CTI Route Point dial plan model allows the administrator to define an unlimited number of CTI Route points with an associated line.

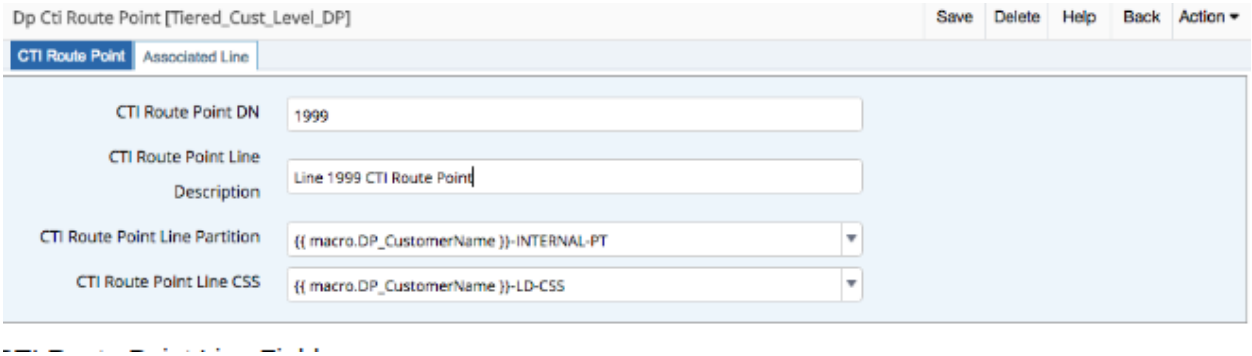




CTI Route Point Device fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Device Name**: The unique device name assigned to the CTI Route Point.
- **Description**: Meaningful description of the CTI Route Point.
- **Device Pool**: Free text field to enter the proper device pool for the CTI Route Point.
- **Css**: Drop-down field that provides a list of CSS from the dial plan css model.
- **Location**: Free text field to assign a valid Call Manager Location
- **Use Trusted Relay Point**: Drop-down with values:
  - Default
  - Off
  - On

- **Calling Party Transformation CSS**: Drop-down field that provides a list of CSS from the dial plan css model.
- **Geolocation**: Free text field to enter a geolocation if necessary.
- **Use Device Pool Calling Party Transformation CSS**: Check box to enable Use Device Pool Calling Party Transformation CSS.

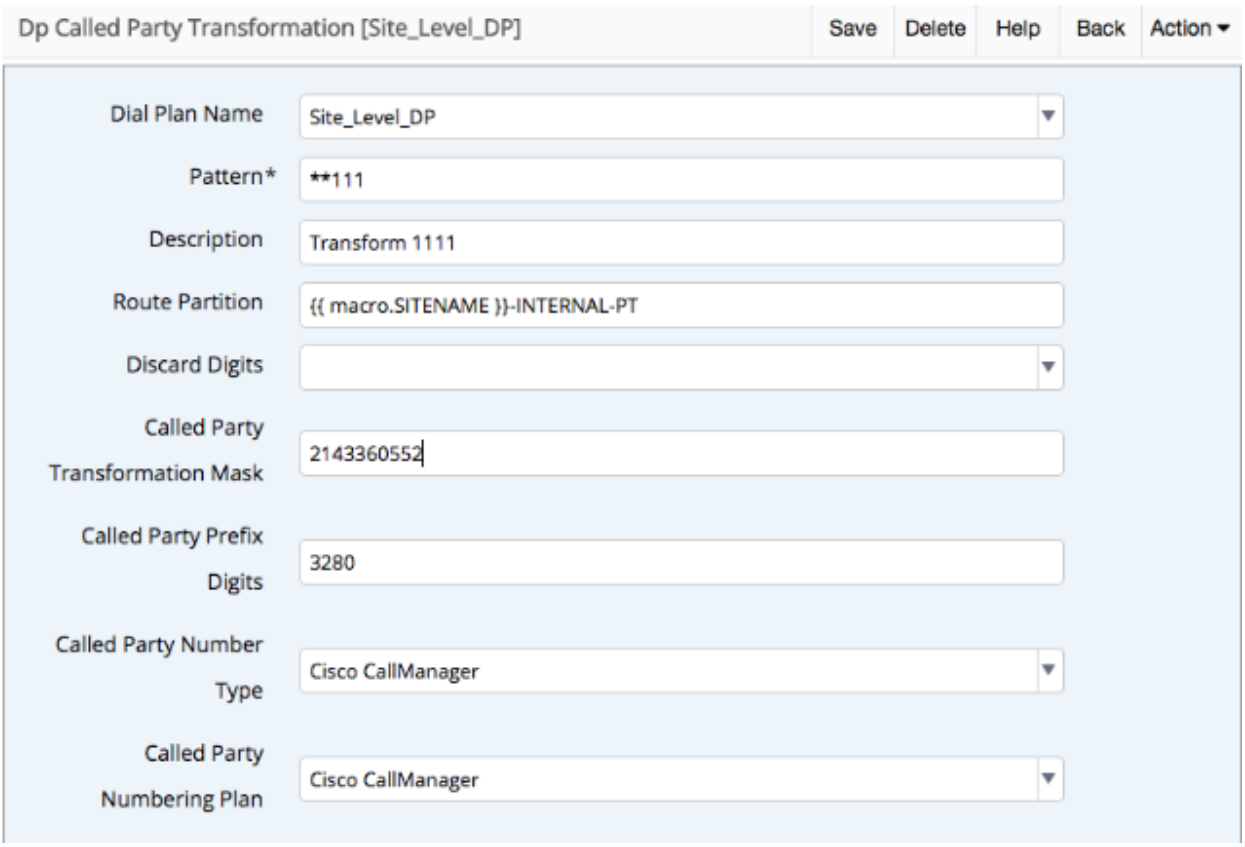


CTI Route Point Line Fields:

- **CTI Route Point DN**: The back end system will take the input from this field and create the Internal Number Inventory entry marked as used, then create a CUCM Line with the input number then finally associate the newly created line to the CTI Route Point.
- **CTI Route Point Line Description**: Meaningful description of the CTI Route Point Line.
- **CTI Route Point Line Partition**: Drop-down field that provides a list of Partitions from the dial plan partitions model.
- **CTI Route Point Line CSS**: Drop-down field that provides a list of CSS from the dial plan css model.

Called Party Transformation Model

The Called Party Transformation dial plan model allows the administrator to define an unlimited number of Called Party Transformations.



Called Party Transformation fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Pattern**: Free text field to allow entry in standard Call Manager patterns.
- **Description**: Meaningful description of the Called Party Transformation.
- **Route Partition**: Free text field for entry of a valid Call Manager Partition.
- **Called Party Discard Digits**: Drop-down providing Call Manager available options:
  - PreDot
  - PreDot Trailing-#

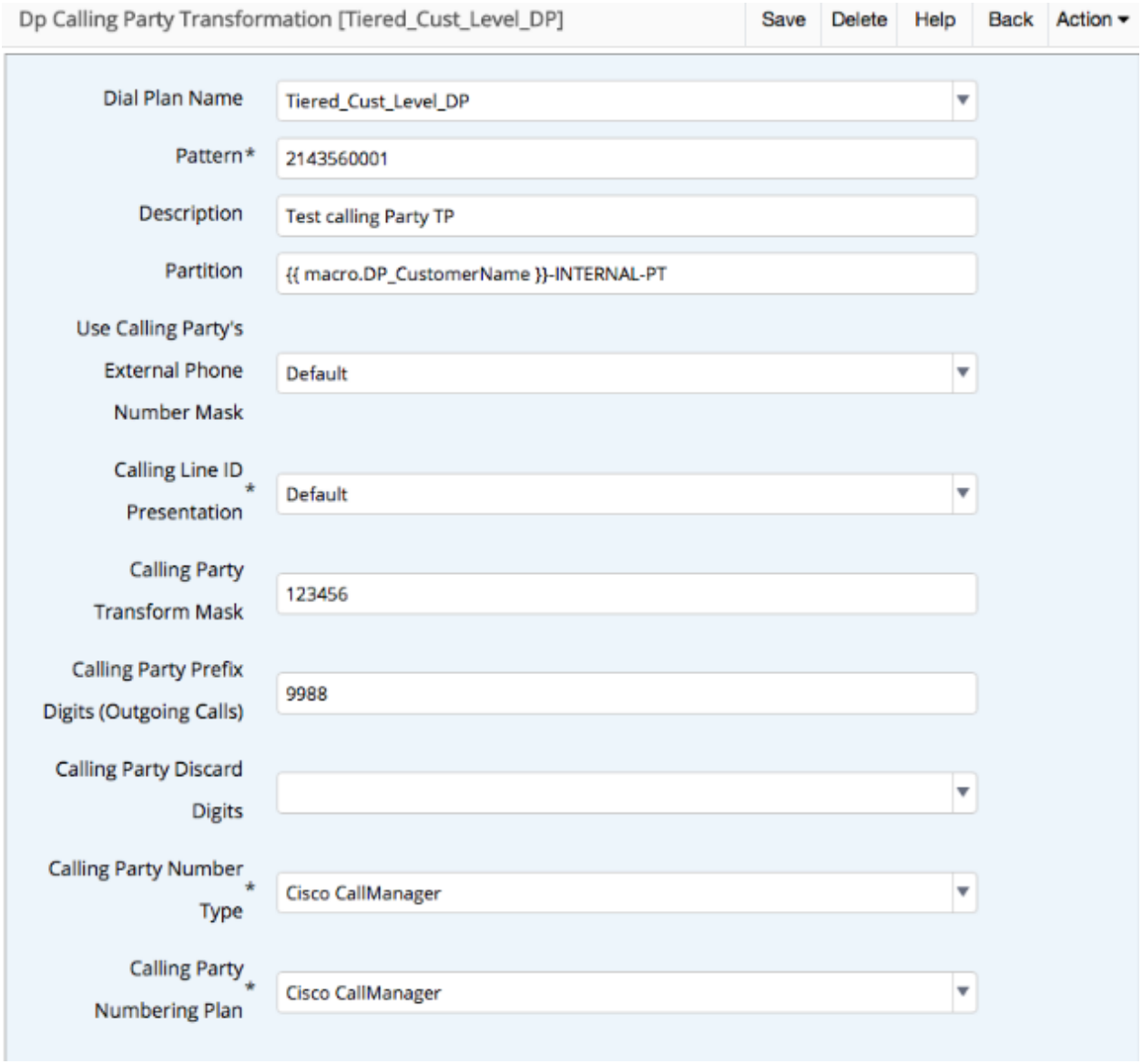
Note that more discard instructions may be added at market demand.

- **Called Party Transformation Mask**: Free text field for entry of transformation mask.
- **Called Party Prefix Digits**: Free text field for entry of prefix digits.
- **Called Party Number Type**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - Unknown
  - National
  - International
  - Subscriber

- **Called Party Numbering Plan**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - ISDN
  - National Standard
  - Private
  - Unknown

Calling Party Transformation Model

The Calling Party Transformation dial plan model allows the administrator to define an unlimited number of Calling Party Transformations.



Calling Party Transformation fields:

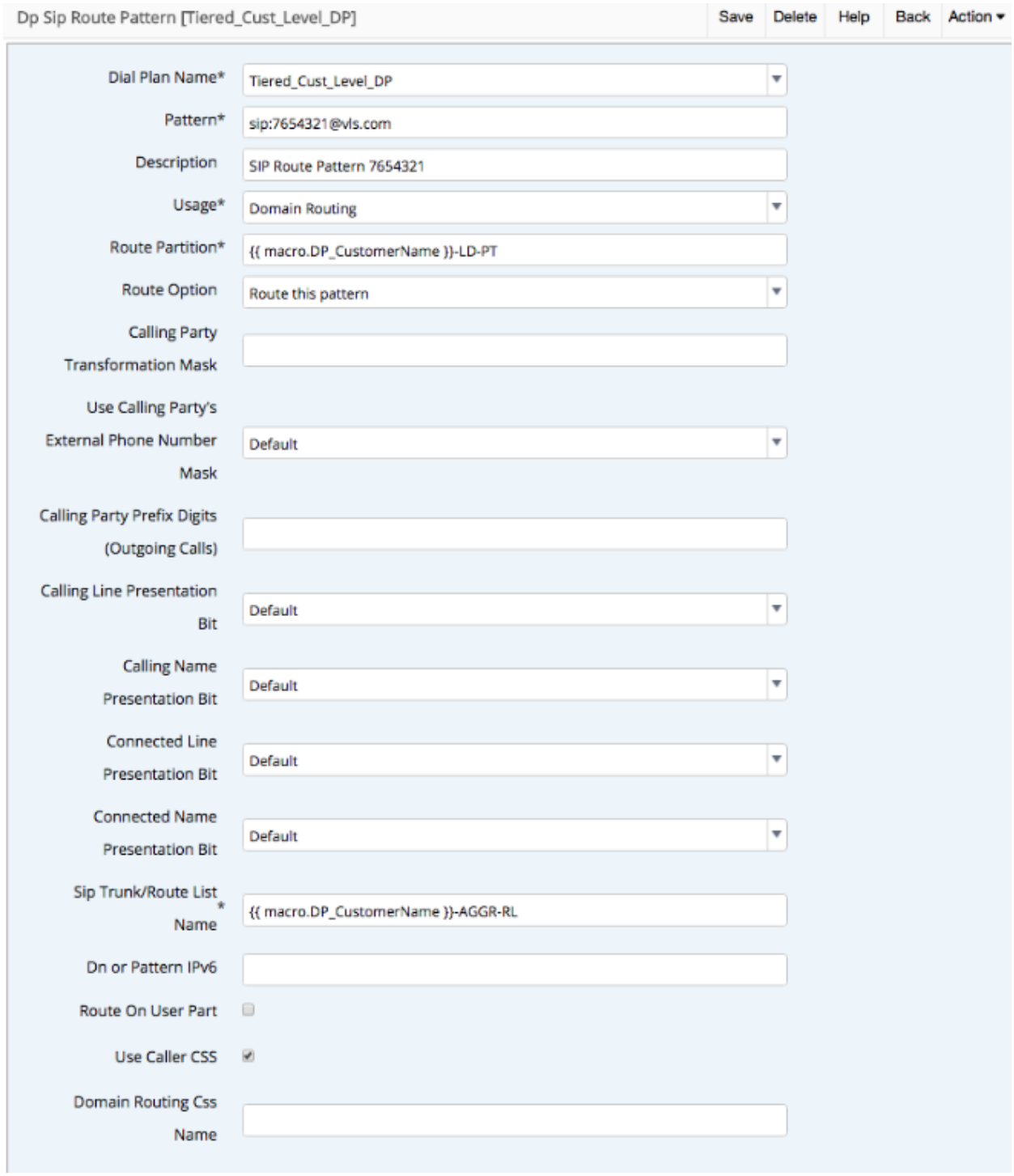
- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Pattern**: Free text field to allow entry of standard Call Manager patterns.
- **Description**: Meaningful description of the Called Party Transformation.
- **Partition**: Free text field for entry of a valid Call Manager Partition.
- **Use Calling Party's External Phone Number Mask**: Drop-down providing Call Manager available options:
  - Default
  - On
  - Off
- **Calling Line ID Presentation**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Called Party Discard Digits**: Drop-down providing Call Manager available options:
  - PreDot

Note that more discard instructions may be added at market demand.

- **Called Party Number Type**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - Unknown
  - National
  - International
  - Subscriber
- **Called Party Numbering Plan**: Drop-down providing Call Manager options:
  - Cisco CallManager
  - ISDN
  - National Standard
  - Private
  - Unknown

SIP Route Pattern Model

The SIP Route Pattern dial plan model allows the administrator to define an unlimited number of SIP Route Patterns.



SIP Route Pattern fields:

- **Dial Plan Name**: Drop-down driven unique name given to the entire dial plan as a whole. This name appears in every dial plan model type.
- **Pattern**: Free text field to allow entry in standard Call Manager patterns uri patterns.
- **Description**: Meaningful description of the SIP Route Pattern.
- **Usage**: Drop-own providing Call Manager options:

  - Domain Routing
- **Route Partition**: Free text field for entry of a valid Call Manager Partition.
- **Route Option**: Drop-down providing Call Manager options:
  - Route this pattern
  - Block this pattern
- **Calling Party Transform Mask**: Free text field to enter common Call Manager Transform Mask data
- **Use Calling Party's External Phone Number Mask**: Drop-down providing Call Manager available options:
  - Default
  - On
  - Off
- **Calling Party Prefix Digits (Outgoing Calls)**: Free text field to enter common Call Manager Calling Party Prefix Digit data.
- **Calling Line ID Presentation**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Calling Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Line Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted
- **Connected Name Presentation Bit**: Drop-down providing Call Manager available options:
  - Default
  - Allowed
  - Restricted

- **Sip Trunk/Route List Name**: Free text field for entry of a valid SIP Trunk or Route List Name.
- **Dn or Pattern IPv6**: Free text field for entry of Dn or Pattern IPv6.
- **Route On User Part**: Check box to enable Route On User Part.
- **Use Caller CSS**: Checkk box to enable use of Caller CSS.
- **Domain Routing Css Name**: Free text field for entry of a domain routing CSS.

26.1.8. Dial Plan Model Bulk Loader

Individual dial plans are meant to be established in the system with a bulk loader. Reference Bulk Loaders will be provided by VOSS staff for use in customer deployments. The key to dial plan for use with the tooling is the Dial Plan Name. This is the top entry in the dial plan model loader. Once a name is established it will carry down through the rest of the fields pertaining to the dial plan name.

Example of the dial plan model bulk loader:

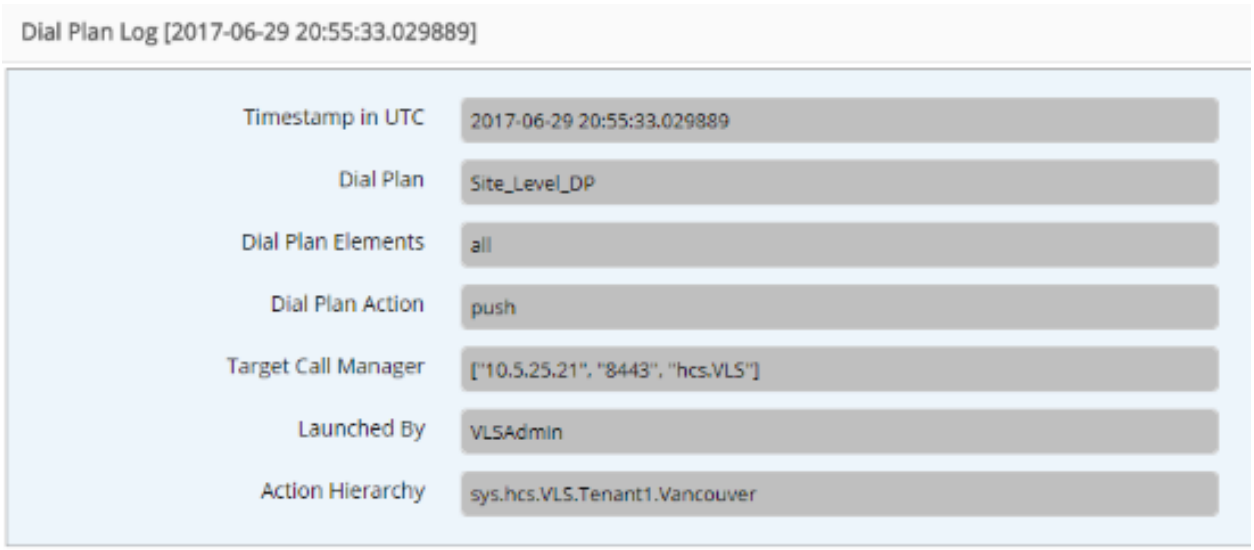
	A	B	C	D	E	F	G	H	I	
1	##	Dial Plan Name								
2		entity: data/DP_DialPlan; parallel: False; parallel_transaction_limit: ; template:								
3		hierarchy	action	search_fields	device	template	ndl	pkid	dpName	
4		# Base							# DP_DialPlan	
5	# Comment	# Hierarchy Node	# Action	# Search Fields	# Device	# CFT Template	# Network Device List	# Unique Identifier	# Dial Plan Name	
6		sys.hcs	Add						Tiered_Cust_Level_DP	Global Dial Plan E
7	##									
8	##									
9	##	Device Pool - Region - Location - SRST Refernce								
10		entity: data/DP_DP-Reg-Loc; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template:								
11		hierarchy	action	search_fields	device	template	ndl	pkid	dpName	
12		# Base							# Device Pool	
13	# Comment	# Hierarchy Node	# Action	# Search Fields	# Device	# CFT Template	# Network Device List	# Unique Identifier	# Dial Plan Name	
14	0	sys.hcs	Add						Tiered_Cust_Level_DP	{{ macro.DP_Cust
15	##									
16	##									
17	##	Time Periods								
18		entity: data/DP_TimePeriod; hierarchy: sys; parallel: False; parallel_transaction_limit: ; template:								
19		hierarchy	action	search_fields	device	template	ndl	pkid	dpName	
20		# Base							# Time Period	
21	# Comment	# Hierarchy Node	# Action	# Search Fields	# Device	# CFT Template	# Network Device List	# Unique Identifier	# Dial Plan Name	#
22	0	sys.hcs	Add						Tiered_Cust_Level_DP	01:00
23	0	sys.hcs	Add						Tiered_Cust_Level_DP	07:00
24	0	sys.hcs	Add						Tiered_Cust_Level_DP	No Office Hours

26.1.9. Dial Plan Log

Logs that will record any dial plan push/remove actions within the system. The information is read only and informational.

Dial Plan Log

Timestamp in UTC	Dial Plan	Dial Plan Action	Dial Plan Elements	Launched By	Action Hierarchy	Hierarchy
2017-06-29 20:05:57.931482	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:39:03.092865	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:44:48.719970	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:47:13.973042	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:48:13.449928	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:53:32.707848	Site_Level_DP	remove	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver
2017-06-29 20:55:33.029889	Site_Level_DP	push	all	VLSAdmin	sys.hcs.VLS.Tenant1.Vancouver	sys.hcs.VLS.Tenant1.Vancouver



Log fields:

- Timestamp in UTS: The timestamp of the time the dial plan action was launched
- Dial Plan: The dial plan model applied
- Dial Plan Elements: Point to all or subset of dial plan elements.
- Dial Plan Action: Push or Remove
- Target Call Manager: The URI to the destination Call Manager
- Launched By: The administrator who submitted the request
- Action Hierarchy: The hierarchy level at which the action was launched.

26.1.10. Dial Plan Use Checklist

- Load Dial Plan Models for Global Values via bulk loader or JSON
- Load Dial Plan Models for Site Values via bulk loader or JSON
- Set Dial Plan Input Data for Global or Site level values. Only the fields that are referenced via Macro in the dial plan model must be populated.
- Push Global dial plan data to Call Manager using the Dial Plan Maintenance Tool. Be sure to check that the tool is run at the appropriate hierarchy level.
- Push Site level dial plan data at Call Manager using the Dial Plan Maintenance Tool. Be sure to check that the tool is run at the appropriate hierarchy level.
- Should any changes need to be made to the pushed dial plans, the tool does allow for removal in reverse order then a re-push once the dial plan models are updated.
- Set Site Defaults via the site default profile tool.

26.2. Unity SIP Integration

26.2.1. Introduction

The Unity SIP Integration tooling provisions complete SIP integration between redundantly deployed Cisco Call Managers (CUCM) and Cisco Unity Connection (CUC) servers. This integration tooling can be used to define the primary only integration that the legacy Voicemail Service provides.

The integration tooling provides a repeatable process to manage the integration of CUCM and CUC, while also providing the ability to:

- Define the dial plan used for integration so that the administrator deploying the integration does not need to have dial plan knowledge.
- Override the dial plan input mechanism mentioned above for advanced deployment.
- Deploy CUCM and CUC SIP integration in full redundancy supporting optional tenants.

Important: Contact your dedicated VOSS support representative for details on how to set up and configure the Unity SIP Integration feature.

Note: If this feature is not exposed in the Admin GUI menu layout, refer to the Optional Features Appendix: Unity SIP Integration - Menu Layout Changes and Access Profile Changes.

Unity SIP Integration Scope

The Unity SIP Integration tooling provides support for:

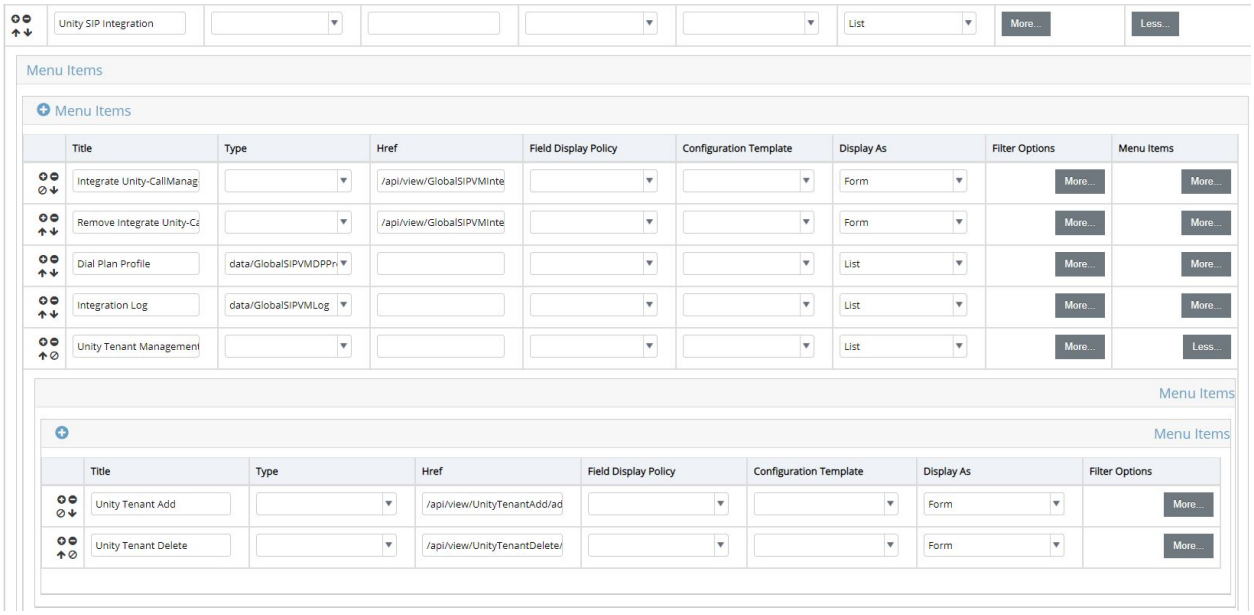
- Dual trunks to Unity publisher/subscriber
- Multiple SIP server destinations to CUCMs (SIP redundancy)
- Specifically defined number of Unity port build per Unity node
- Dynamic creation of CUCM route list/route group or the ability to update if they already exist
- Creation of Unity tenants for shared architectural deployments
- Creation of Unity integration utilizing tenants
- Support for multi-cluster deployments

26.2.2. Menu Layout Changes

1. Login as an administrator with sufficient rights to change menu layouts.
2. Click **Role Based Access > Menu Layouts**.
3. Select the required menu.
4. Configure the menu layout as shown below under **Unity SIP Integration**.
5. Click **Save**.

Title	Type	Href	Display As
Unity SIP Integration			List
Integrate Unity-CallManager		/api/view/GlobalSIPVMIntegration/add	Form
Remove Integrate Unity-Call Manager		/api/view/GlobalSIPVMIntegration Delete/add	Form
Dial Plan Profile	data/GlobalSIPVMDPProfile		List
Integration Log	data/GlobalSIPVMLog		List
Unity Tenant Management			List
• Unity Tenant Add		/api/view/UnityTenantAdd/add	Form
• Unity Tenant Delete		/api/view/UnityTenantDelete/add	Form

See also **Unity SIP Integration Menu Layout** illustration:



26.2.3. Access Profile Changes

1. Login as an administrator with sufficient rights to change access profiles.
2. Click **Role Based Access > Access Profiles**.
3. Select the required administrator name, for example ProviderAdminAP.
4. Configure the provider access profiles as shown in step 5.
5. Under **Type Specific Permissions** add the following new **Permitted Type** entries and **Permitted Operations**:

- Permitted Type: view/UnityTenantAdd
- Permitted Operations: Create
- Permitted Type: view/UnityTenantDelete
- Permitted Operations: Create
- Permitted Type: view/GlobalSIPVMIntegration
- Permitted Operations: Create, Field Display Policy, Read, Tag
- Permitted Type: view/GlobalSIPVMIntegrationDelete
- Permitted Operations: Create
- Permitted Type: data/GlobalSIPVMDPProfile
- Permitted Operations: Create, Delete, Read, Tag, Update
- Permitted Type: data/GlobalSIPVMLog
- Permitted Operations: Read, Tag

6. Click **Save**.

26.2.4. Unity SIP Integration

The Unity SIP Integration feature can be used in place of your existing voicemail service. A list of menus items is available to carry out the Unity SIP Integration tasks. Unity SIP Integration provides SIP integration for both CUCM and CUC.

A typical workflow would be that one or more integration dial plan profiles are set up for use, and then a SIP Unity Integration is pushed to CUCM and CUC.

Menu Name	Description and Notes
Integrate Unity-CallManager	The main tool used to push integration between CUCM and CUC.
Remove Integrate Unity- Call-Manager	This allows you to remove the complete integration out of the target CUCM and CUC.
Dial Plan Profile	This allows an advanced administrator to define all of the dial plan elements that make up the CUC integration, for example device pools, route group, route list, CSSs, and so on.
Integration Log	This log is populated with information about when the integration was pushed, as well as other details, so that it can be pulled back out again.
Unity Tenant Management	A “tenant” is basically a small voicemail setup for a sub-company within your larger Connection server. In other words if you had companies sharing a single connection server for voicemail services, you can set each one up as a separate “tenant” in your install which effectively isolates them from one another. Note that a Unity server containing user data without tenants cannot have tenants added after the fact.
Unity Tenant Add	This allows you to add a unity tenant to the Unity server.
Unity Tenant Delete	This allows you to remove a unity tenant from the Unity server.

26.2.5. Integrate Unity-Call Manager

This option allows you to create a SIP Integration between Cisco Unified Call Manager (CUCM) and Cisco Unity Connection (CUC).

Base

Note: Prior to completing this form, the **Provisioning Target Call Manager**, the **Provisioning Target Unity**, and the **Voicemail Service Dial Plan Profile** must be set. Based on these selections, other key values are auto populated on the form.

Complete, at minimum, the mandatory fields (red border):

UC Publisher Application Selection

- **Provisioning Target Call Manager** - Choose from the drop-down list.
- **Provisioning Target Unity** - Choose from the drop-down list.

Deployment Options

- **Voicemail Service Dial Plan Profile** - Choose from the drop-down list.
- **Dial Plan Advanced Mode** - Select this check box to unlock the fields for dial plan elements. You then have the ability to update those values 'live'.

  Clear the check box to return the dial plan elements to the default voicemail dial plan profile values. This check box can be hidden from lower level administrators.
- **Provision CUCM-Unity in Redundant Mode** - Clear this check box for the feature to function in single mode, that is to operate in a similar way to the original voicemail service (Publisher only and no Subscriber trunk).

  Select this check box to provision in redundant mode. In this mode, you can configure ports on both the Publisher and Subscriber Unity nodes, as well as build a trunk to both Publisher and Subscriber.
- **Unity Tenant(s) Present** - If the selected 'Provisioning Target Unity' server (see under **UC Publisher Application Selection** above) has tenants on it, this check box is automatically selected.

CUCM Global

- **SIP Profile** - To assign the configured settings in this SIP profile to the associated device.
- **SIP Trunk Security Profile** - To assign a single security profile to multiple SIP trunks in order to apply the configured settings to the SIP trunks.

These fields are auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.

Unity Port Group

Complete, at minimum, the mandatory fields (red border):

- **Phone System** - Choose from the drop-down. The phone system settings identify the phone system with which Unity Connection integrates and regulate certain phone system features (integration configuration settings are located in the port groups that belong to the phone system.)

- **SIP Server Authentication Username** - Enter the user name that Unity Connection uses to authenticate with the SIP server (SIP integrations only).
- **SIP Server Authentication Password** - Enter the password that Unity Connection uses to authenticate with the SIP server (SIP integrations only.
- **Repeat SIP Server Authentication Password** - Repeat the SIP Server Authentication Password entered above.
- **SIP Security Profile (IP Port)** - Select the SIP security profile that Unity Connection uses. Default setting = 5060.
- **Primary CUCM IPv4 Address or Host Name** - Enter the IP address (or host name) of the PIMG/TIMG unit that the port group connects to.
- **Redundant SIP Servers**
  - **Call Manager Server IP or Host Name** -

Unity Ports

Complete, at minimum, the mandatory fields (red border):

- **Publisher Server**

  This field is auto populated based on the **Provisioning Target Unity** chosen under **Deployment Options**.
- **Publisher Port Count** -
- **Subscriber Server** -
- **Subscriber Port Count** -

CUCM Voicemail Pilot

Complete, at minimum, the mandatory fields (red border):

- **Pilot Number** - Enter a number to identify the voicemail pilot number.
- **Calling Search Space** - Enter an appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this pilot number.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Default Voice Mail Pilot for the System** - Select this check box if you want to replace the current default pilot number, and make this pilot number the default Voice Mail Pilot for the system.

CUCM Voicemail Profile

Complete the following fields as required:

- **Name** - Enter a name to identify the voicemail profile.
- **Description** - Enter the description of the profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (), angle brackets (<>), dollar sign ($), single-quote(‘), open parenthesis [(], close parenthesis [)], slash (/), colon (:), semi-colon (;), equal sign (=), at sign (@), tilde (~), brackets ({ }), or apostrophe (‘).

- **Pilot** - Choose the appropriate voicemail pilot number that is defined in the Voice Mail Pilot Configuration or Use **Default**. This field is auto populated based on the **Pilot Number** entered under **CUCM Voicemail Pilot**.
- **Voice Mail Box Mask** - Specify the mask that is used to format the voice mail box number for auto-registered phones. When a call is forwarded to a voice-messaging system from a directory line on an auto-registered phone, CUCM applies this mask to the number that is configured in the Voice Mail Box field for that directory line.
- **Make this the default Voice Mail Profile for the System** - Select this check box to replace your current default profile, and make this the default profile name.

CUCM Route List

Complete the following fields as required:

- **Name** - Enter a name for this route list. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Run On All Active Unified CM Nodes** - Select this check box to enable the active route list to run on every node.
- **Call Manager Group** - Choose a CUCM group. The route list registers with the first CUCM in the group, which is its primary Cisco Unified CM.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.

CUCM Route Group

Complete the following fields as required:

- **Name** - Enter a name for this route group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.

  This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Distribution Algorithm** - Choose a distribution algorithm from the drop-down:
  - **Top Down** - If you choose this distribution algorithm, CUCM distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member.
  - **Circular** - If you choose this distribution algorithm, CUCM distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which CUCM most recently extended a call. If the nth member is the last member of a route group, CUCM distributes a call starting from the top of the route group.

  Default = Circular.

CUCM to CUC Publisher SIP Trunk

Complete, at minimum, the mandatory fields (red border):

- **Device Name** - Enter a device name.
- **Trunk Device Pool** - This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Destination IP Address** - Choose from the drop-down list.

CUCM to CUC Subscriber SIP Trunk

This tab is only visible if the **Provision CUCM-Unity in Redundant Mode** check box on the **Base** tab is selected.

Complete, at minimum, the mandatory fields (red border):

- **Device Name** - Enter a unique device name.
- **Trunk Device Pool** - This field is auto populated based on the **Voicemail Service Dial Plan Profile** chosen under **Deployment Options**.
- **Destination IP Address** - Choose from the drop-down list.

26.2.6. Dial Plan Profile

This allows an advanced administrator to define all of the dial plan elements that make up the CUC integration.

Mandatory fields include; SIP Profile, SIP Trunk Security Profile, Device Pool, Route Group, Route List, SIP Trunk Inbound CSS, Call Manager Group and Voicemail Pilot CSS.

This form can be filled with static (exact) values if you want to deploy these same values over and over at Store level. This option is typically not used and is displayed for illustrative purposes only.

At the Provider hierarchy, macros are used to make the profile portable across several customers. For example, if you had two or three different versions of dial plans, then you would have two or three versions of this profile. The lower level administrators could then apply the profiles as required.

Note: You can only add a SIP integration once a Dial Plan Profile has been configured.

26.2.7. Remove Integrate Unity-CallManager

This tool (**Unity SIP Integration > Remove Integrate Unity-CallManager**) takes the complete selected SIP integration back out of the Cisco Unified Call Manager (CUCM) and Cisco Unity Connection (CUC).

From the **Integration Label** drop-down, choose the integration that you want to remove and click **Save**.

26.2.8. Unity Tenant Management

Unity Tenant Management assists in creating groups of objects in Unity Connection that provide a basic “tenant services” application. In short it allows you to create a tenant, which includes numerous interrelated

database objects in Connection that work together to provide basic directory segmentation features to allow for isolated groups of users and handlers within your Connection server.

You can add or delete unity tenants.

26.2.9. Unity Tenant Add

1. Choose **Unity Tenant Management > Unity Tenant Add** to open the **Unity Tenant Add** form.
2. Complete, at minimum, the following mandatory fields:
   - **Target Unity Server** - .
   - **Unity Tenant Name (Alias)** - The alias is used as a prefix for all objects created in the tenant - used to make sure all objects in Connection are uniquely named.
   - **SMTP Domain** - a unique SMTP Domain name.
   - **Tenant Desciption** - .
3. Click **Save**.

26.2.10. Unity Tenant Delete

1. Choose **Unity Tenant Management > Unity Tenant Delete** to open the **Unity Tenant Delete** form.
2. From the **Unity Tenant Name (Alias)** drop-down, choose the tenant to delete.
3. Click **Save** to remove the tenant.

26.2.11. Integration Log

This tool (**Unity SIP Integration > Integration Log**) will be populated with all the details relevant to the SIP Integration.

This includes when the integration was pushed, and other details so that the integration can be pushed back out again if required.

26.3. Phone Based Registration

26.3.1. Phone Based Registration: Overview

This document describes the installation, configuration, operation and troubleshooting procedures for the VOSS-4-UC Phone Based Registration Add-On.

The VOSS-4-UC Phone Based Registration Add-on feature allows an administrator to pre-provision Cisco Phones for UC Subscribers with rich and detailed configuration without requiring knowledge of the Phone MAC address in advance.

Given a pre-configured phone, the PBR Add-On allows an end user to access an Auto Registered phone to Register their pre-configured device via the Phone Services menus.

Phone Based Registration Feature Reference

- *Architecture*
- *Pre-Requisites*
- *Expose access to Phone Based Registration feature*
- *Create a restricted API Role and Admin user*
- *Install the Phone Based Registration Web Service*
- *Configure the Phone Based Registration Add-On*
- *Setup a Cisco Unified CM for Phone Based Registration*
- *High Level Overview of Phone Based Provisioning*

26.3.2. Architecture

Phone Based Registration Feature Reference

The VOSS-4-UC Phone Based Registration Add-on is implemented as a Cisco Unified IP Phone Services Application.

This operates a web service on the VOSS-4-UC platform that is installed on all unified nodes in a VOSS-4-UC Cluster as follows:

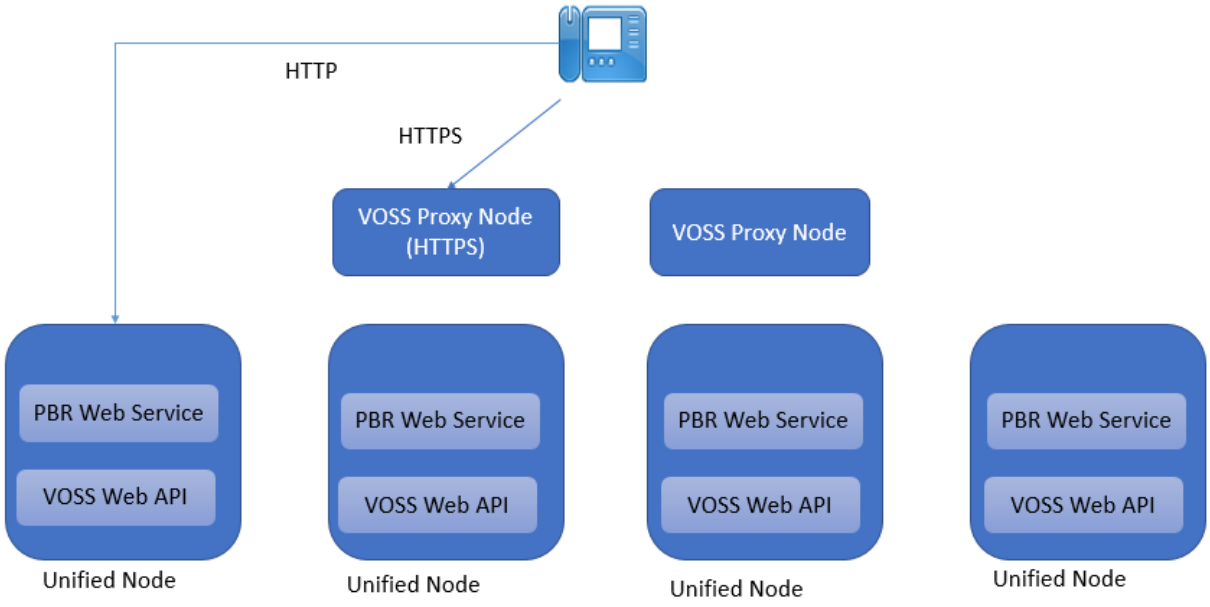


Figure 1: Phone Based Registration Network Connectivity

26.3.3. Pre-Requisites

Phone Based Registration Feature Reference

The following pre-requisites are required to install and operate the Phone Based Registration Add-On.

Network Connectivity

The VOSS-4-UC Phone Based Registration Add-On requires that Auto Registered Phones can connect to the VOSS-4-UC Proxy Nodes and Unified nodes.

Source Node	Destination Node	Transport	Port	Protocol
Phone	VOSS-4-UC Proxy Nodes	TCP	443	HTTPS
Phone	VOSS-4-UC Unified Nodes	TCP	8412	HTTP

Table 1: Phone Based Registration Network ports

Note that either HTTP or HTTPS is used on a per customer basis. The choice depends on:

- Security requirements, e.g. HTTPS only.
- Device support (some older devices do not support HTTPS – refer to the Cisco IP Phone security guide for list of devices that support secure communications.

Certificates for HTTPS

When using HTTPS for connectivity the VOSS-4-UC certificate must be installed on Cisco Call Managers that make use of the Phone Based Registration Service.

The VOSS-4-UC Platform certificate needs to be copied from the VOSS-4-UC server and uploaded to CUCM.

1. Log in to VOSS-4-UC using Firefox or Chrome. In the URL click on the 'Lock' symbol and choose to view the Certificate. Find the 'Copy To' or 'Export' option depending on your browser and save the certificate file to your PC.
2. Log in to VOSS-4-UC using the "Cisco Unified OS Administration" login. Browse to **Security > Certificate Management** and upload the Certificate with the Certificate Purpose set to 'tomcat-trust'. Restart the Cisco service as per the instructions.

The CUCM Hostname configured on CUCM under **System > Server** must be able to resolve via DNS otherwise the Phones will not authenticate. If the Hostname does not resolve then change the hostname to the IP Address instead.

26.3.4. Expose access to Phone Based Registration feature

Phone Based Registration Feature Reference

The Phone Based Registration Add-On needs to be added to the menu layouts for Provider and Customer administrators that require access to the feature.

The simplest mechanism to configure the menu layouts and access profiles for Phone Based Registration is to export the existing menu layouts and access profiles for the appropriate roles and submit to VOSS GS team to create a customized version that includes current modifications.

A detailed description of the items to expose can be found in Appendix 1.

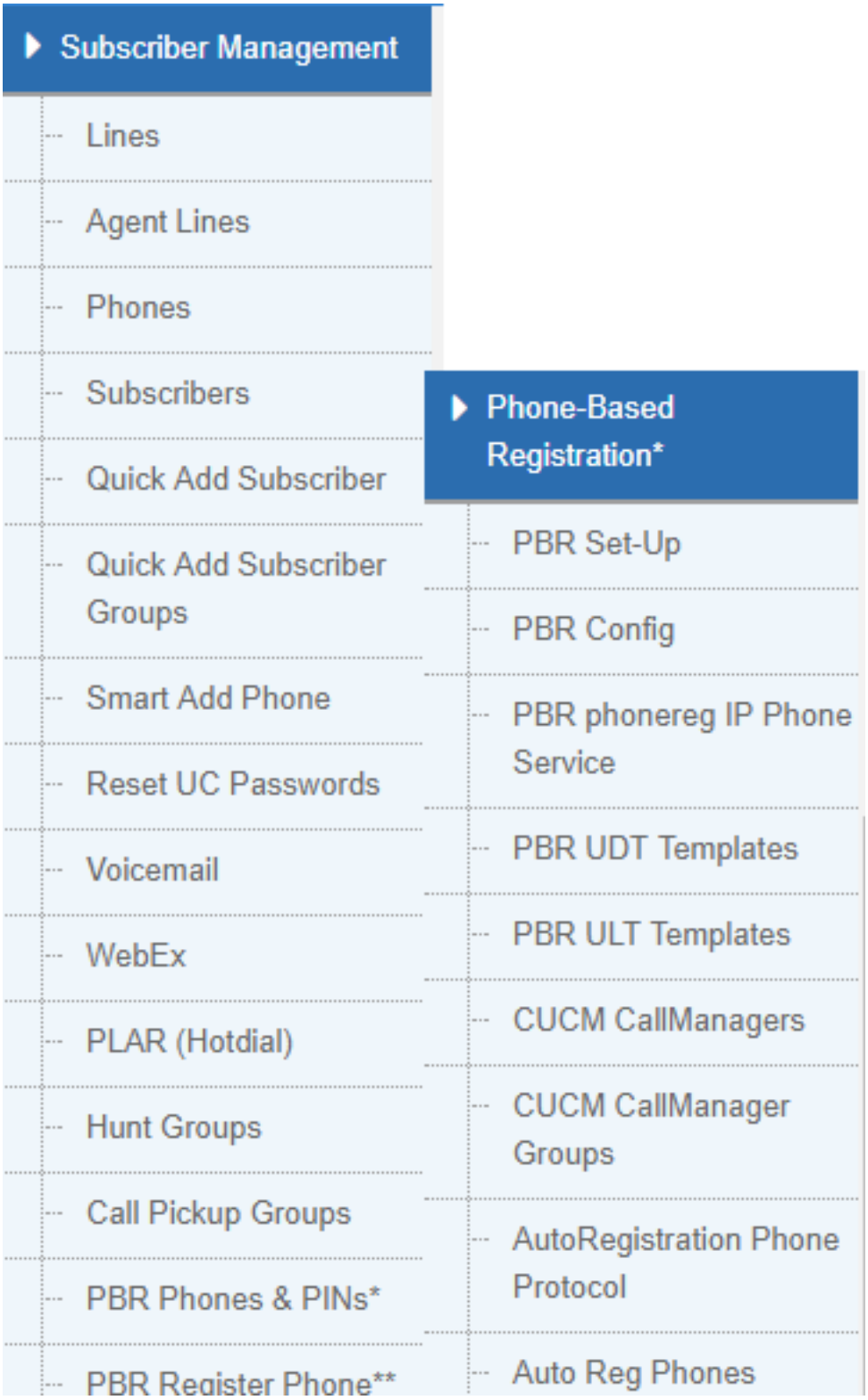


Figure 2: Sample Menu layouts for Phone Based Registration Add-On

26.3.5. Create a restricted API Role and Admin user

Phone Based Registration Feature Reference

The Phone Based Registration Add-On Web service initiates transactions on behalf of the end user that is registering a phone. This requires a limited role to provide the least privilege to this user.

Create a Restricted API Access Role at the Provider Hierarchy

1. Browse to **Role Management**.
2. Click **Roles** and then **Add**.
3. Complete the form as follows:
   a. Name: PBR_RestrictedAPIAccess
   b. Menu Layout: RS_PBR_Restricted_Menu
   c. Access Profile: RS_PBR_RestrictedAPIAccess

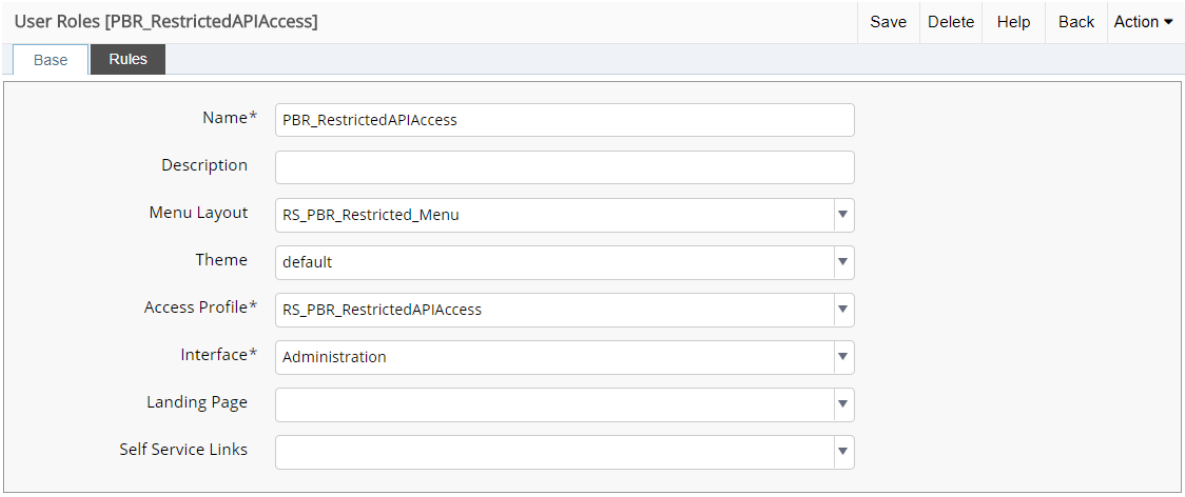


Figure 3: Sample Restricted API Access Role

Create a Restricted API Access User at the Provider Hierarchy

1. Browse to **Admin Users**.
2. Click **Add**.
3. Complete the form and select **PBR_RestrictedAPIAccess** for the role.
4. Note the email address and password.

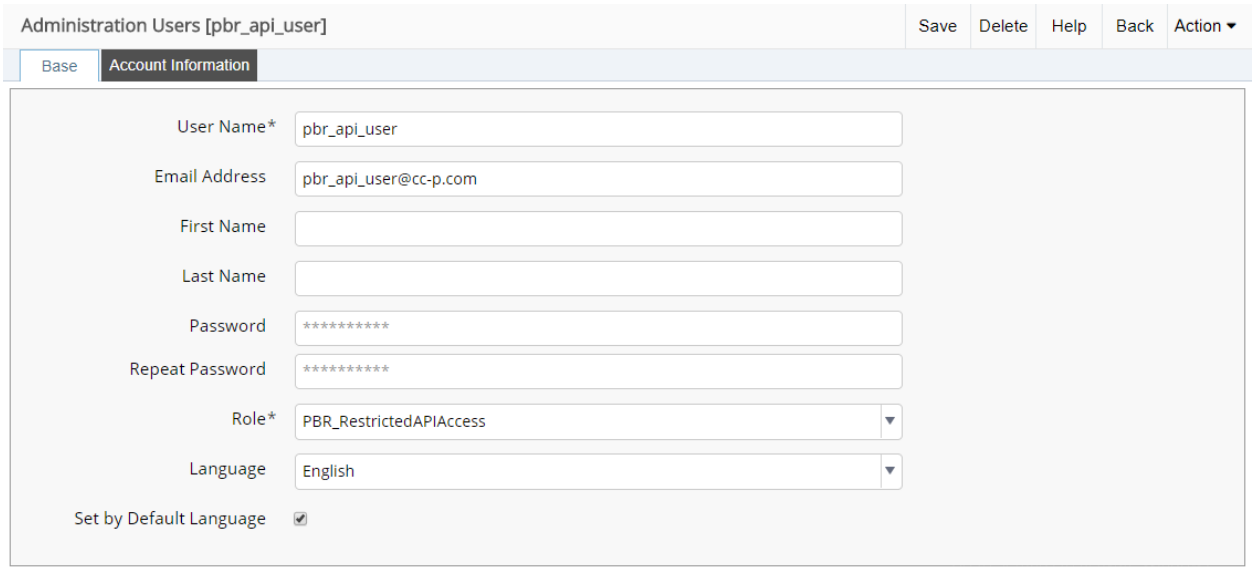


Figure 4: Sample Restricted API Access user

26.3.6. Install the Phone Based Registration Web Service

Phone Based Registration Feature Reference

Note: If phone based registration was not installed prior to a delta bundle upgrade, you will need to download the latest Phone Based Registration install script to all unified nodes before continuing with the installation steps below in order to install the latest version.

This can be located on the secure downloads server under `/software/voss4uc/releases/Release-19.3.3/pbr`

Refer to the accompanying document *MOP-PBR-19.3.3.pdf*.

Note that a full service restart is initiated on initial startup of the PBR web service on each VOSS-4-UC unified node.

- *On a cluster*:
  1. Run the following command on all unified nodes in serial:

     app install media/phone-based-registration_install-19.3.3.script –force
  2. Run the following command on the primary node:

     cluster provision –force
- *On a standalone system*:
  1. Run the following command on the unified node:

     app install media/phone-based-registration_install-19.3.3.script –force
  2. Run the following command:

     system provision –force

The PBR web service is assigned the same web weights as the `selfservice` and `voss-deviceapi` service. For example, when running **web weight list** from a web proxy, the output should be similar to the example below:

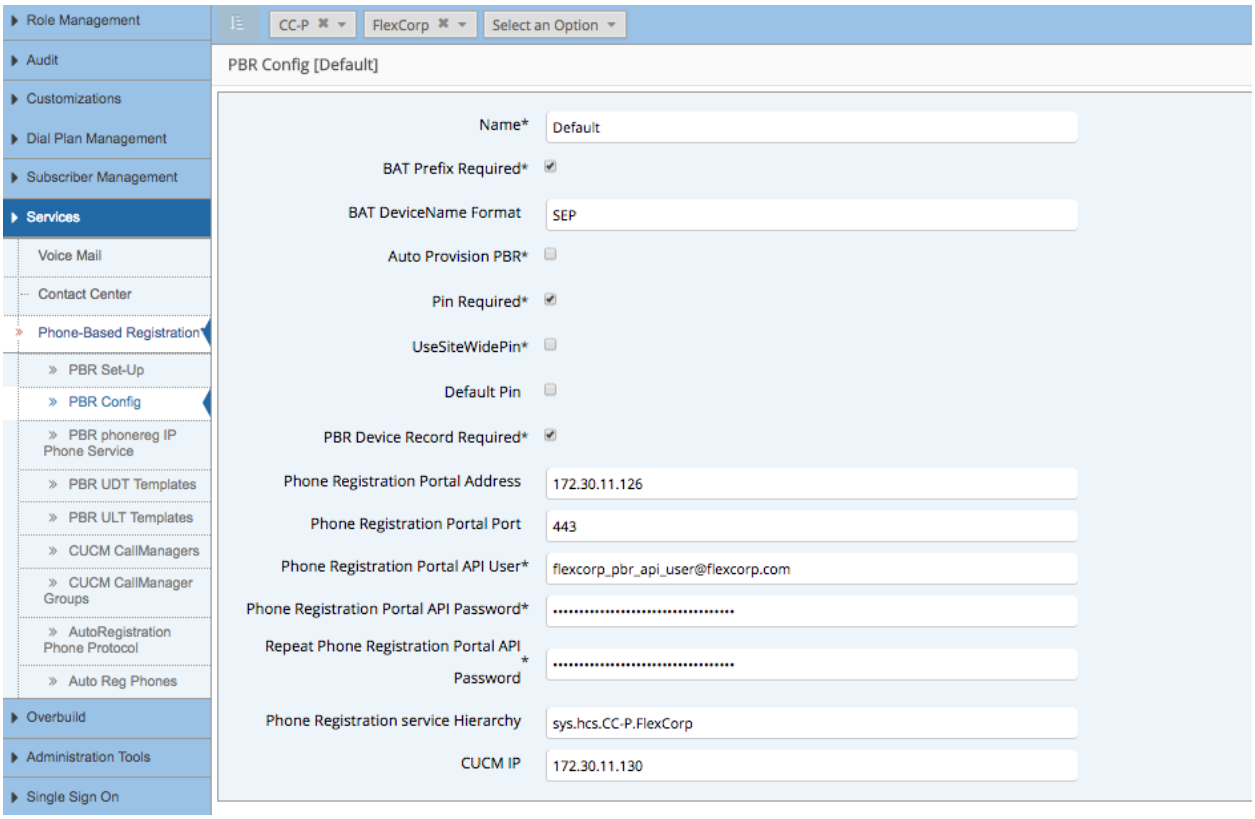
```
platform@VOSS-WP-1:~$ web weight list
Default service weights

  upstreamservers:
    phonebasedreg:
        phoneservices:
            192.168.100.10:443: 0
            192.168.100.3:443: 1
            192.168.100.4:443: 1
            192.168.100.5:443: 1
            192.168.100.6:443: 1
            192.168.100.9:443: 0
    voss-deviceapi:
        selfservice:
            192.168.100.10:443: 0
            192.168.100.3:443: 1
            192.168.100.4:443: 1
            192.168.100.5:443: 1
            192.168.100.6:443: 1
            192.168.100.9:443: 0
        voss-deviceapi:
            192.168.100.10:443: 0
            192.168.100.3:443: 1
            192.168.100.4:443: 1
            192.168.100.5:443: 1
            192.168.100.6:443: 1
            192.168.100.9:443: 0
```

26.3.7. Configure the Phone Based Registration Add-On

Phone Based Registration Feature Reference

The Phone Based Registration Add-On supports a number of configuration parameters that manage how the service operates in a specific provider or customer environment. This configuration is implemented using the **Services > Phone Based Registration > PBR Config** menu item.

- A single PBR config record MUST be created globally at provider level.
- A PBR config record must be created for each customer that will utilize the phone based registration add-on.
- The config at the provider level is there to enable the PBR web service to make initial connection to VOSS-4-UC API.
- The config at customer level defines the specific connection parameters for that customer and eventually will allow per customer VOSS-4-UC user to be used.



Configuration is on VOSS-4-UC user interface:

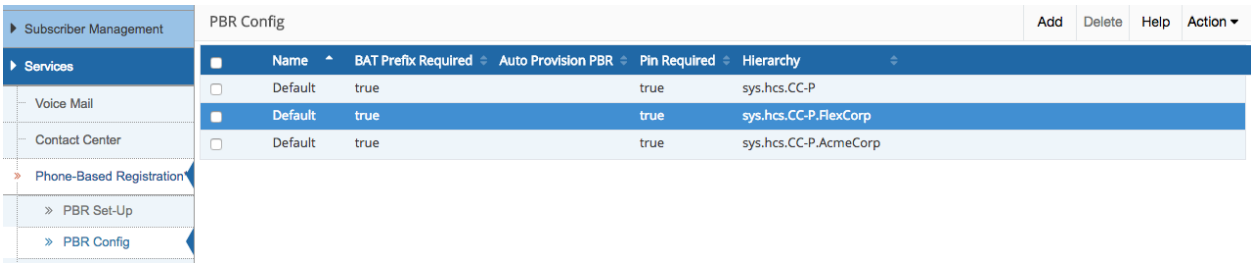


Figure 5: Sample PBR Config record

When configuring the PBR service for a specific hierarchy the following considerations are important:

1. VOSS recommends that PBR configuration should only allow the replacement of phones with fake MACs with device name prefix starting with BAT.

   This ensures that it is never possible for a user to replace a phone that is in active use.

   Select the **BAT Prefix Required** check box.

2. Is the use of PBR Device records required in this environment?

   a. The PBR device record provides a mechanism for administrators to explicitly specify that a device is eligible for phone based registration.

      Select the **PBR Device Record Required** check box if this is desired.

   b. The PBR device record allows the administrator to specify a PIN that should be used when performing phone based registration for a specific phone or for all phones at a site.

      Select the **Pin Required** check box.

c. The PBR device record can be used to guarantee that the correct device is replaced in environments where Directory numbers are not unique within a Unified CM cluster, e.g. multiple Directory numbers are configured with same DN but located in different partitions.

   In this case, clear the **UseSiteWidePIN** check box.

Phone Based Registration Portal Port:

- This should be port 443 for HTTPS based connectivity
- This can be port 80 for HTTP based connectivity

Phone Based Registration Portal Address:

- When using HTTPS, this is the IP address or hostname of a VOSS-4-UC proxy node in a cluster.
- When using HTTP, this is the IP address or hostname of the primary VOSS-4-UC unified node in a cluster.
- This address and the port below must be accessible from the phone network.

Phone Based Registration Portal API User Credentials:

- Phone Based Registration Portal API User:
  - This is the user that was configured in the previous section of documentation. Please specify the email address.
- Phone Based Registration Portal API Password:
  - The password of the PBR API user:

Note that this information is required for both the Provider level config and the config for any customers.

Phone Based Registration Service Hierarchy:

- If the config record is defined at Provider level, then this should be the Provider hierarchy, e.g. sys.hcs.CC-P.
- If the config record is defined at the customer level, then this should be the customer hierarchy, e.g. sys.hcs.CC-P.FlexCorp)

CUCM IP:

- This should be the IP address of Unified CM that is accessible to VOSS-4-UC using HTTPS SOAP requests.

By default, VOSS-4-UC requires a PBR device record per device, but in some cases, it could be sufficient to use a single pin per site:

1. In this case, select the **UseSiteWidePIN** check box.
2. This provides limited security to ensure that a PIN is still required to register a phone, but reduces the operational burden by eliminating the need to provision a PBR device record for each phone.

Additional options:

- Auto Provision PBR device record. This feature is experimental and should **not be selected**.
- Use default PIN. This feature is experimental and should **not be selected**.
- BAT devicename format: This should be left to default.

Important: After saving the above configuration in VOSS-4-UC, you must restart the services by running the following CLI command on the primary node:

cluster run app start phone-based-registration

26.3.8. Setup a Cisco Unified CM for Phone Based Registration

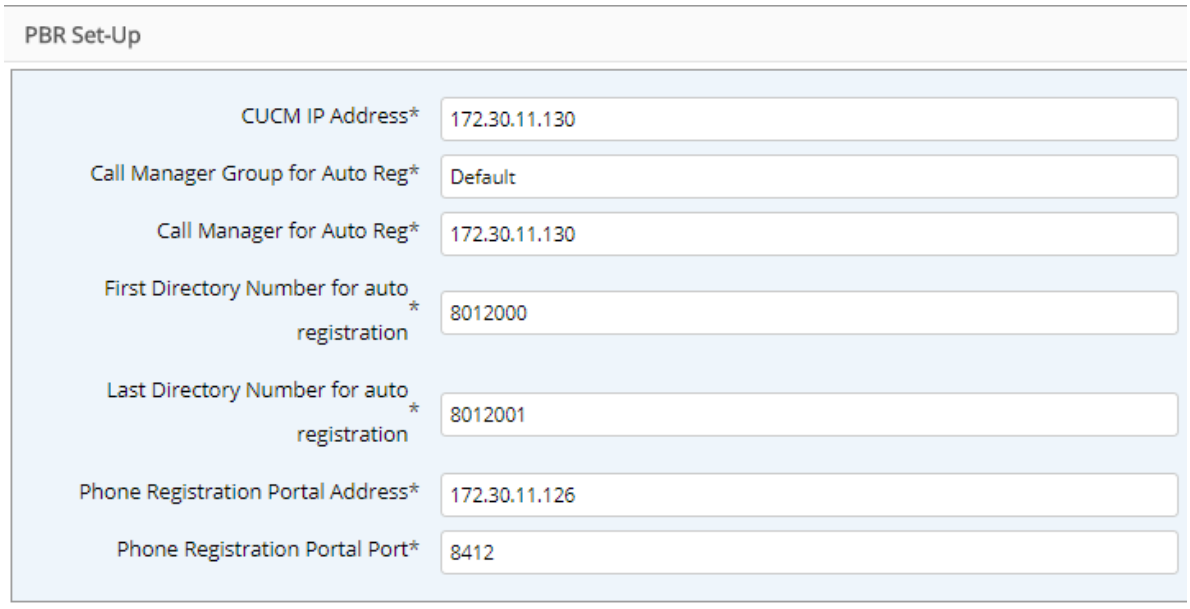
Phone Based Registration Feature Reference

Using PBR Setup feature to configure a Cisco Unified CM

The PBR Setup feature automates the configuration of Unified CM for AutoRegistration and Phone Based Registration.

In VOSS-4-UC, browse to **Services > Phone Based Registration > PBR Setup**. The following input is required:

- **Call Manager IP**: IP Address of the publisher for the Unified CM Cluster.
- **Call Manager Group**: Name of Unified CM Group for AutoReg.
- **Call Manager Name**:
  - Name of the Call Manager for AutoReg.
  - Confirm by checking the value of name field at **Services > Phone Based Registration > CUCM Call Managers**.
  - This must either be the IP address of the Unified CM OR a hostname that can be resolved in DNS.
- **First and Last Directory Number for Autoreg**: A valid range of DNs to be used for Auto Registration.
- **PBR Portal Address**: The IP Address of VOSS cluster UN1 .
- **PBR Portal Port**: 8412.



VOSS recommends that initial configuration of the Unified CM is performed using the PBR Setup workflow described above. In cases where there is existing auto registration config on the Unified CM, it may be required to do this manually.

The VOSS-4-UC Phone Based Registration Add-On requires the following functionality to be configured on Cisco Unified CMs that manage phones that may be registered by this feature:

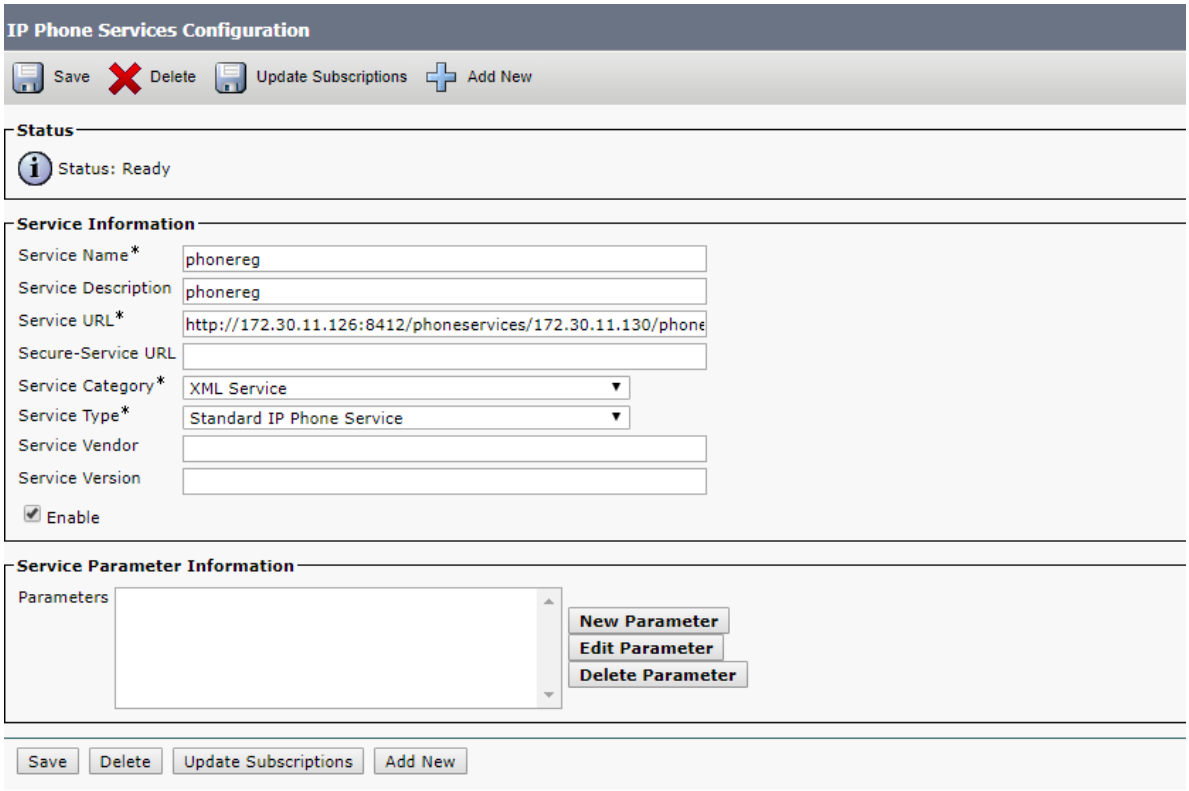
1. Configure the Unified CM to allow AutoRegistration of new phones. This is standard auto registration config for Unified CM.
2. When a phone Auto Registers the phonereg phone service should be configured for the phone. This is achieved by specifying a Universal Device Template for Auto Reg that subscribes to the phonereg phone service.

Screenshots of the relevant configuration on Unified CM are provided to assist with understanding how the service is implemented and as background for a Cisco expert that may need to fine tune the Unified CM config.

3. Setup the phonereg Phone Service:

   Browse to **Device > Device Settings > Phone Services**.

   172.30.11.126



   Service URL:

   Depending on whether HTTPS or HTTP is used the service URL may be different:

   - HTTP (Service URL):

     ```
     http://{VOSS_IP}:{PBR_PORT}/phoneservices/{UnifiedCM_IP}/phonereg/menu?device=
     ↪#DEVICENAME#
     ```

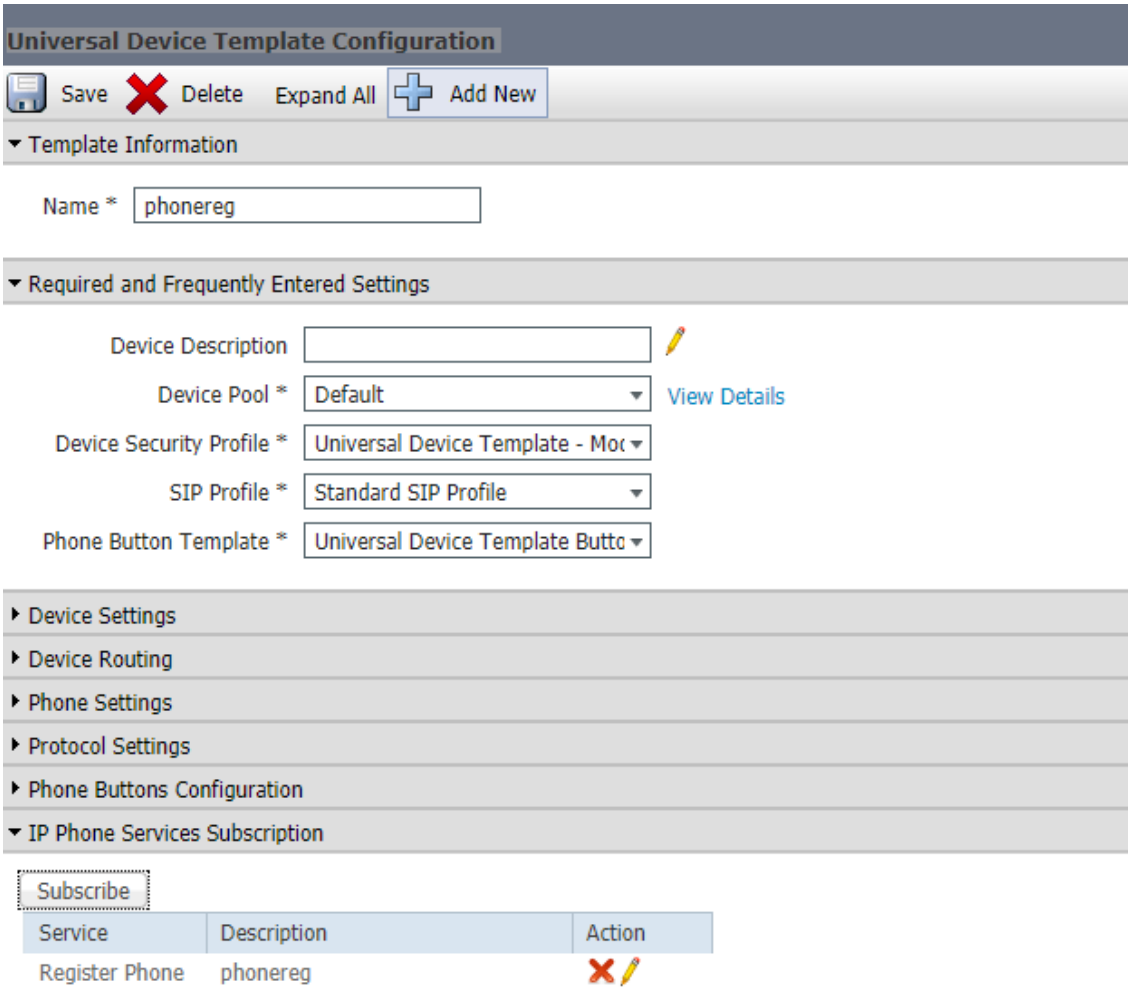
   - HTTPS (Secure-Service URL):

     ```
     https://{VOSS_IP}:443/phoneservices/{UnifiedCM_IP}/phonereg/menu?device=
     ↪#DEVICENAME#
     ```

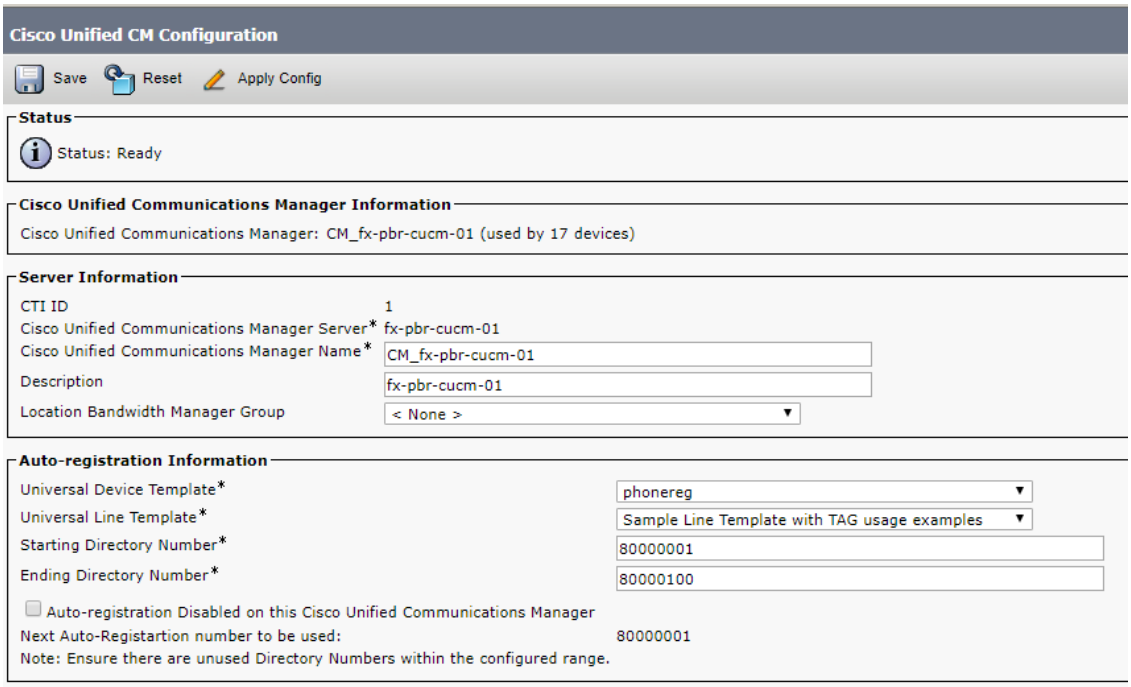
For HTTPS-only, both Secure Services URL and Service URL must be populated with the HTTPS URL.

Note: The port must always be specified explicitly.

4. Configure phonereg Universal Device Template:
   a. Browse to **User Management > User/Phone Add > Universal Device** Template.
   b. Note the subscription to the phonereg Phone Service.



5. Unified CM for Auto Registration:
   a. Browse to **System > Cisco Unified CM**.
   b. Note the phonereg Universal device template.



26.3.9. High Level Overview of Phone Based Provisioning

Phone Based Registration Feature Reference

Setup a phone for Phone Based Registration

In this case we provision a phone with a fake MAC address, e.g. BAT000008012005 using bulk loaders or the VOSS-4-UC Admin portal. An optional Phone Based Registration (PBR) device record can be provisioned that provides the following functionality:

1. Configure a PIN code that can be used to authenticate requests to register phones with Phone Based Registration.
2. Assist with unique identification of device to replace where directory numbers are not unique within a Call Manager Cluster.

Register a phone with Phone Based Registration

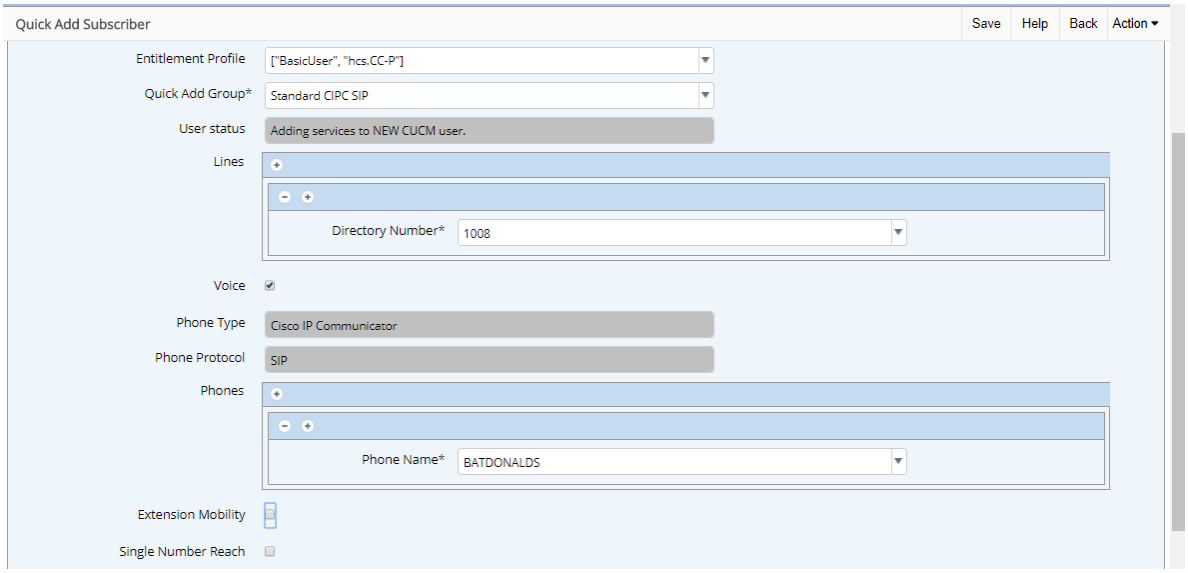
Assuming the Phone is correctly setup the following steps are required to register a phone with the Phone Based Registration Add-On.

1. Auto Register a physical phone with Cisco Call Manager.
2. Access the Phone Services Menu on the Auto Registered Phone.
3. Select Register Phone menu option.
4. Enter extension and PIN (if required).
5. Submit request.

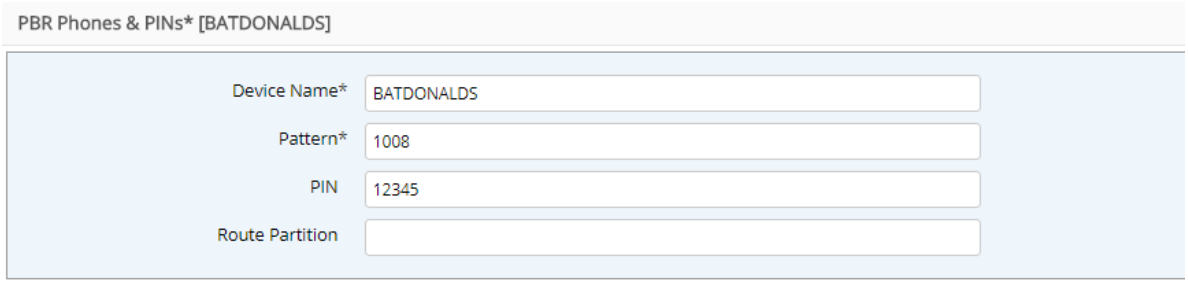
This initiates a request to VOSS-4-UC to replace the configuration of the Auto Registered Phone with the rich settings defined for the pre-provisioned device with fake MAC.

26.3.10. Detail Phone Based Provisioning Steps

1. Provision a phone with a fake MAC Address:
   a. In this case we'll use Quick Add Subscriber, but VOSS-4-UC Phone Management or Advanced Subscriber features can also be used.
   b. The fake MAC address must have a BAT prefix, e.g. BATABCABCABCABC.



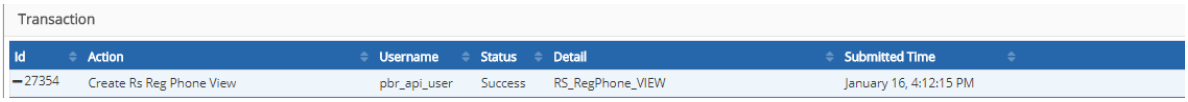
2. Provision a PBR Device Record for the phone with a PIN:
   a. Browse to **Subscriber Management > PBR Phones and PINS > Add**.
   b. Specify the Device Name of the pre-provisioned device with the fake MAC.
   c. Route Partition is not required unless Site-Wide PIN.

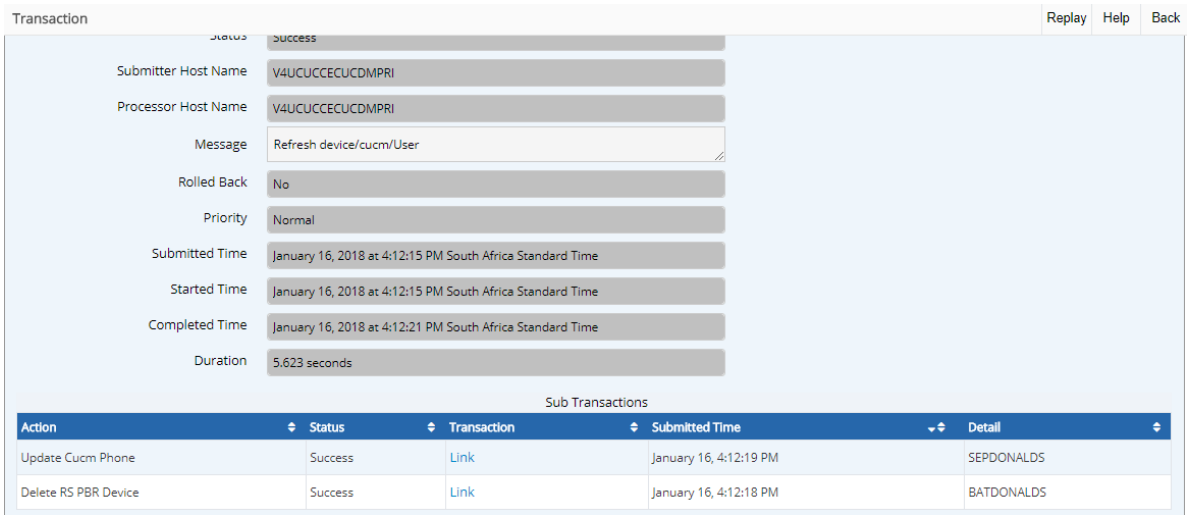


3. Auto Register the Phone on CUCM:

4. Select Phone Services and then Register Phone:
    a. Enter Extension and PIN.
    b. Submit.

5. The Phone screen should now show Registering Phone.
6. The VOSS-4-UC Transaction log should now show a Register Phone Transaction.

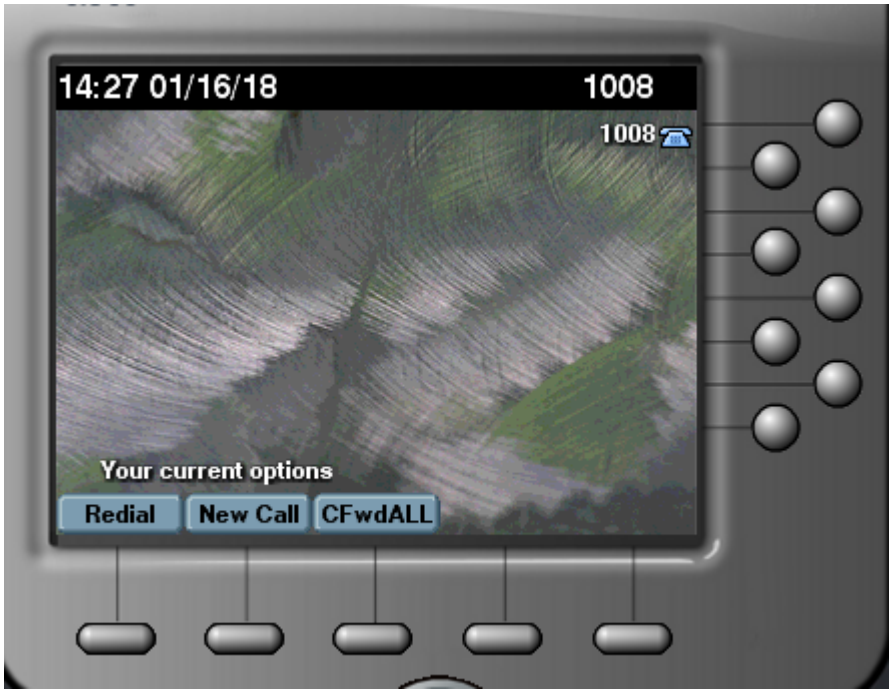




Note:

- The PBR Device Record is deleted (if you need to re-register this phone then a new record is required).
- The device name of the pre-provisioned phone (BATDONALDS) is updated to match the name of the autoregistered phone.

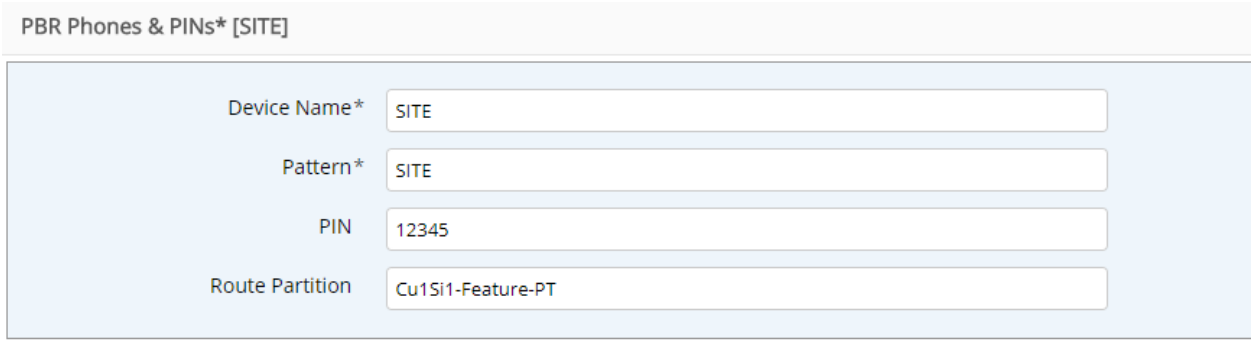
7. Upon completion of the transaction the phone should reboot and show the device configuration of the pre-provisioned phone.



26.3.11. Provisioning PBR Device Records with Site Wide PINs

Site wide PINS are useful when PINs are required for either security or to address use-cases where DNs are not unique.

However, the operational overhead of provisioning a device record per unique device is not acceptable. In this case, create a single PBR device record at each site:



Note:

- When using Site wide PINS the Device Name and Pattern must be hardcoded to use SITE. This is case sensitive.
- When using Site wide PINS the administrator must specify the route partition for the site.

26.3.12. Menu Layout and Access Profiles

1. Phone-Based Registration Sub-menu under Services:
    - Add “PBR Set-Up”
        - Title: PBR Set-Up
        - Type: view/RS_SetupReg_VIEW
        - Display As Form
    - Add “PBR Config”
        - Title: PBR Config
        - Type: data/RS_PBR_Config
        - Display as list
    - Add “PBR phonereg IP Phone Service”
        - Title: PBR phonereg IP Phone Service
        - Type: device/cucm/IpPhoneServices
    - Add “PBR UDT Templates”
        - Title: PBR UDT Templates
        - Type: device/cucm/UniversalDeviceTemplate

- Add “PBR ULT Templates”
  - Title: PBR ULT Templates
  - Type device/cucm/UniversalLineTemplate
- Add “CUCM CallManagers”
  - Title: CUCM CallManagers
  - Type: device/cucm/CallManager
- Add “CUCM CallManager Groups”
  - Title: CUCM CallManager Groups
  - Type: device/cucm/CallManagerGroup
- Add “AutoRegistration Phone Protocol”
  - Title: AutoRegistration Phone Protocol
  - Type: device/cucm/ServiceParameter
  - Filter: AutoRegistrationPhoneProtocol
    - Filter By - Name
    - Filter Type - Equals
    - Filter String - AutoRegistrationPhoneProtocol
    - Ignore Case - false
- Add “Auto Reg Phones”
  - Title: Auto Reg Phones
  - Type: relation/SubscriberPhone
  - Filter: Auto
    - Filter By - BAT Phone Template
    - Filter Type - Equals
    - Filter String - Auto
    - Ignore Case - false

2. Under Subscriber Management Advanced Functions add:
   - Add “PBR Phones & PINs”
     - Type: data/RS_PBR_Device
     - Title: PBR Phones & PINs
   - Add “PBR Register Phone”
     - Title: PBR Register Phone
     - Type: view/RS_RegPhone_VIEW
     - Display As: Form
3. Add the PBR Views to the Access Profile for Provider Admin (expose all operations):
   - view/RS_RegPhone_VIEW
   - view/RS_SetupReg_VIEW

- data/RS_PBR_Config
- data/RS_PBR_Device

26.4. Phone Services

26.4.1. Introduction to Phone Services

The Phone Services feature provides a XML-based interface to user settings that can be utilized via the Cisco IP Phones. If the feature is enabled, the following services become available for users to interact with via their IP Phones using the Telephone User Interface (TUI):

- Speed Dials - Provides the user with the ability to manage and use their speed dials for the phones/extension mobility profile.
- Call Forward - Provides the user with the ability to manage call forward destinations per line for key call forward options (all, busy, no answer).
- Corporate Directory - Provides the ability to view, search, and initiate calls from the users within VOSS-4-UC.

These will appear alongside other Phone Services that are setup in the system.

The Phone Service feature requires network connectivity between the phones and the VOSS-4-UC Proxy server instance. The feature supports HTTP only from the phones.

The Phone Services feature has been tested to support the following phone types:

- 78XX, 88XX, 89XX, and 99XX
- Other Cisco phone models may work, however these have not been validated and will not be supported if there are issues. So use with any other phone models should be tested carefully in your lab prior to use in production if desired.

See also:

- *Phone Services Feature Setup*
- *Manage Phone Services*

26.4.2. Phone Services Feature Setup

Introduction to Phone Services

To enable and setup Phone Services, the following steps are required:

1. Pre-requisites

Prior to setting up the Phone Services Feature, make sure that the phone based registration web service has already been installed, see *Install the Phone Based Registration Web Service*.

2. Configure a Local Admin for use by the Feature

Configure a local admin user in the system at the provider level to be used by the Phone Services feature to initiate transactions in VOSS-4-UC. VOSS suggests this user is used just for phone services and not used to login to the system or for other admin purposes. The permissions required for this user are included in the access profile **RS_PBR_RestrictedAPIAccess**, which is on the system by default. You may need to create a role with the relevant settings to assign to the user being created. This user and password will be used in the next step.

Note: Consider a credential policy for this user that does not expire the password to avoid needing to change the password and update the various configurations setup in Step 3 for the new password.

---

3. Enable the PBR instance for UCM Clusters

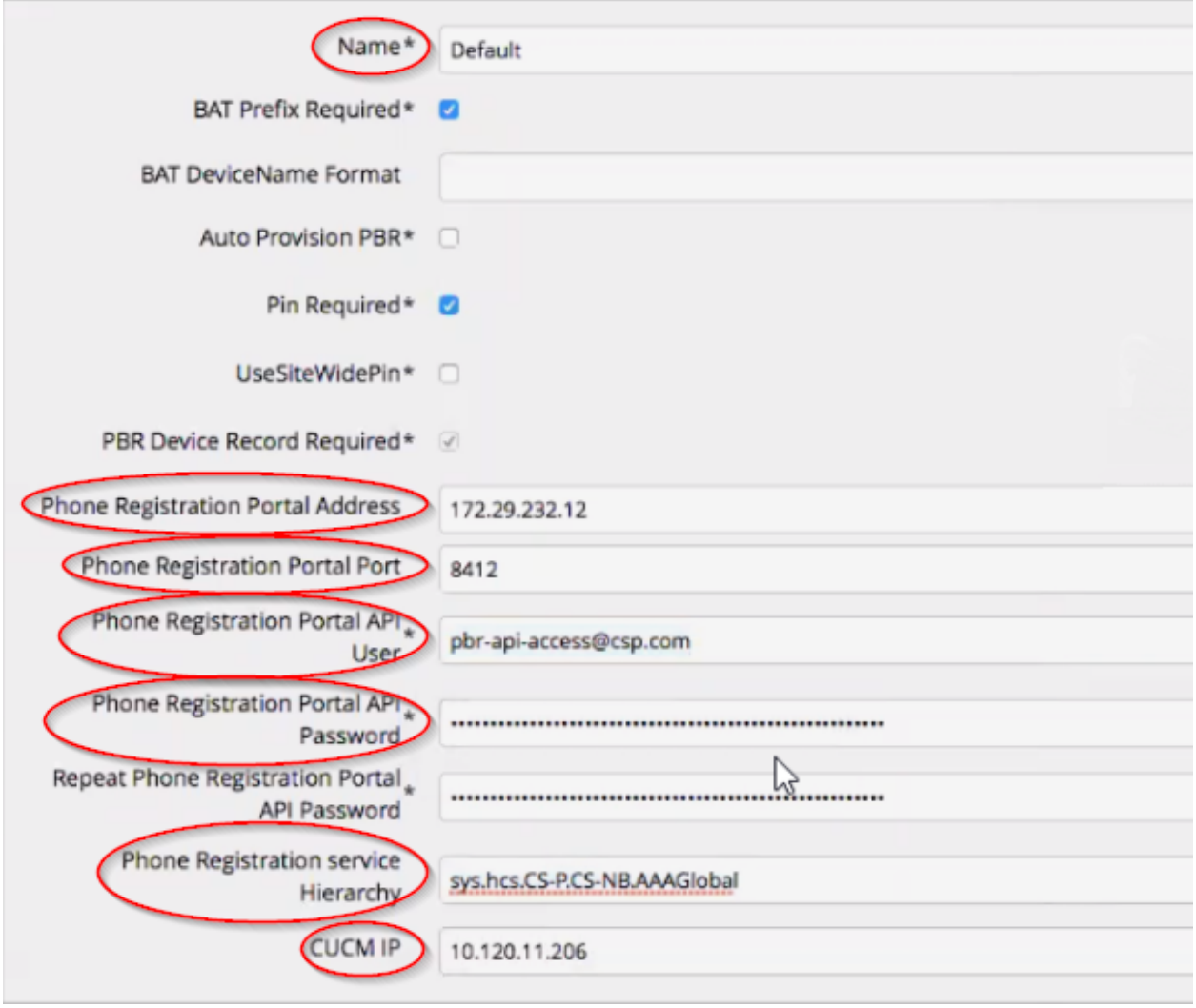
If you have already configured Phone-based Registration then some of these steps might already be complete. Configuration parameters are accessed from the **Services > Phone Based Registration > PBR Config** menu item.

- Setup the required PBR Configuration instances in VOSS-4-UC. This may require you to add the correct model (**data/RS_PBR_Config**) to the access profile and menu layouts for the roles that require access to enable/configure phone services.
- An instance of the model at the Provider level is required (with the Unified CM IP value blank if you don't have a Unified CM at the Provider level). This instance will enable the basic Phone Services capability on the system.
- An instance of the model at the hierarchy level of the Unified CM Cluster that requires the feature to be supported. **In the case of a multi-cluster setup, multiple instances may be required at the same hierarchy (one instance per Unified CM)**.

The following fields and settings are required for Phone Services (see also illustration below - values are examples only). The other settings on the form are not required for Phone Services.

- **Name** - Unique name for this instance.
- **Phone Registration Portal Address** - this is the IP address of the VOSS-4-UC Proxy that the phones will communicate with. This needs to be the address visible to the phones (could be across a NAT boundary).
- **Phone Registration Portal Port** - This must be port `8412`.
- **Phone Registration Portal API User** - This user ID is hard coded for Phone Services: `pbr-api-access@[providername].com`.
- **Phone Registration Portal API Password** - The password for the user setup in Step 2.
- **Phone Registration Service Hierarchy** - This field is populated based on the hierarchy breadcrumb when you click the add button. If it is wrong, navigate back to the list view and change the breadcrumb to the correct hierarchy.
  - If the config record is defined at provider level, then this must be the provider hierarchy, for example `sys.hcs.CS-P`.
  - If the config record is defined at the customer level, then this must be the customer hierarchy, for example `sys.hcs.CS-P.CS-NB.AAAGlobal`.

- **CUCM IP** - This should be the IP address of the Unified CM Publisher that is accessible to VOSS-4-UC using HTTP SOAP requests. Optional if this is the initial provider level record and there is not a Unified CM at that level.



To make the setup of multiple instances of this record easier in a system with more than one cluster, you can include a configuration template in your menu layout populated with the values for the shared settings then the form will pre-populate with them, e.g. Portal address, Portal port, API User, and API Password.

Note: Depending on your network setup, in the event of a proxy failure, e.g. a data center DR Failover scenario, the Phone Services hostname/IP address may need to be changed to the proxy in the DR data center.

Important:

- After saving the above configuration in VOSS-4-UC, you must restart the services by running the following CLI command on the primary node (if not already done):

  cluster run app start phone-based-registration

- The **Services Provisioning** value under **Enterprise Parameters Configuration - Parameter Name**

on the associated Unified CM **must** be set to **Both**.

4. Create Unified CM IP Phone Service for Phones to Access the Feature

There are two ways of setting up the service that controls which devices the service appears on:

- Regular service - the service must be subscribed individually to specific phones on which the service must appear:

  Enable check box = Selected

- Enterprise-wide subscription - the service will appear on all phones in the system:

  Enterprise Subscription check box = Selected.

Typically an enterprise-wide subscription would be the easiest as it means not managing the service subscriptions by device. However, if more granular control is required then managing it as a normal service and subscribing as needed is possible.

The IP Phone Service provides the details of the VOSS-4-UC Service which is how the IP Phones access the feature. The service needs to be setup into the Unified CM for the phones to use it.

Choose **Device > Device Settings > Phone Services**.

The following are the settings for the service. The service can be configured via VOSS-4-UC if the IP Phone Services device model is included in your menus (or via bulk loader). Otherwise it can be configured directly in the Cisco Unified CM:

- **Service Name**: VOSS-4-UC Phone Services (or preferred name that will appear in the Phone's services menu)
- **Service Description**: VOSS-4-UC Phone Services
- **Service Category**: XML Service
- **Service Type**: Standard IP Phone Service
- **Service Vendor**: VOSS
- **ServiceURL**:

```
http://<VOSS-4-UC-Address>:8412/phoneservices/<UnifiedCMAddress>/menu
  ?name=#DEVICENAME#
  &corp_dir=true
  &corp_dir_format=UN-LN-FN
  &refresh=true
```

Where `<VOSS-4-UC-Address>` - is the address that the phones will use to reach VOSS-4-UC (typically the primary proxy server - consider any NAT setup in your network). You may consider using/validating a DNS SRV address here for redundancy in the event of a proxy failure. `<UnifiedCMAddress>` - is the address of Unified CM as known to VOSS-4-UC - consider any NAT setup in your network.

Note: This is an example ServiceURL only, showing the corporate directory format set to "UN-LN-FN" (Username, Lastname, Firstname). See parameters below, and replace the value following the '=' sign with the value you require.

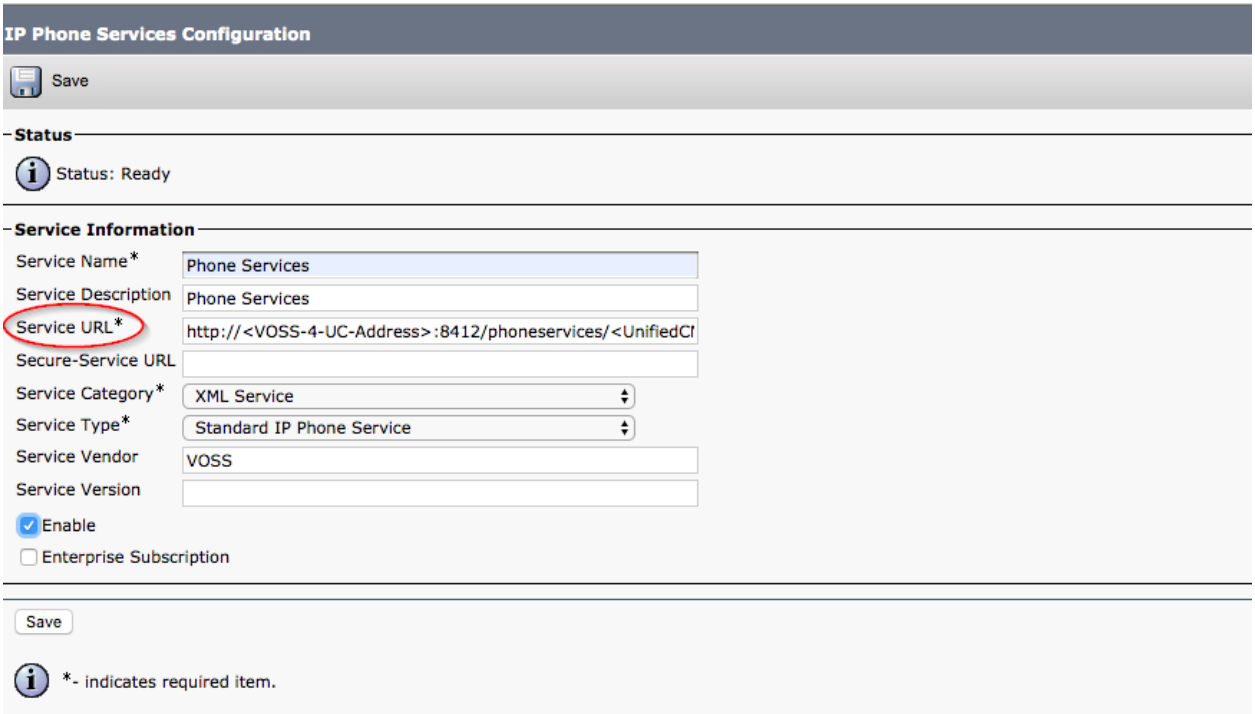
- `corp_dir` - this parameter is enabled (true) by default. It can be disabled if necessary by adding it to the URL as "corp_dir=false". When enabled, the "Corp Dir" menu item is added to the list of services. The corporate directory consists of all directory numbers located at the customer hierarchy or lower,

and displays a maximum of 50 numbers only. The numbers can be filtered by adding first name and last name.

- `corp_dir_format` - this parameter determines the format of the corporate directory, and can have one of the following values:
  - "UN-LN-FN" = Username, Lastname, Firstname
  - "LN-FN-UN" = Lastname, Firstname, Username
  - "LN-FN" = Lastname, Firstname
  - "FN-LN" = Firstname, Lastname
  - "UN" = Username

  If the parameter is omitted from the URL, the default corporate directory format will be "UN-LN-FN", i.e. Username, Lastname, Firstname.
- `refresh` - this parameter is used to control whether the service will retrieve the latest setting from the underlying Unified CM when the service is used.

  For example, when opening the call forward option, it would retrieve the latest call forward all setting from the Unified CM. This can be useful if the **CFWD ALL** softkey is also used on the phone. If the softkey is not being used and changes are only in VOSS-4-UC then `refresh=false` (which is the default if excluded) can be used to make the service quicker.



5. Connectivity between Phones and VOSS-4-UC

For the Phone Services feature to work, the network needs to support connectivity between the Phones and the VOSS-4-UC Proxy server. This could be across a NAT boundary or a firewall that requires the appropriate configuration to allow the traffic. From a firewall perspective, the connectivity is via HTTP and the port is `8412`. As noted above, consider the user/validating of a DNS SRV entry for the VOSS-4-UC proxy address for redundancy, otherwise if IP address or static hostname is used the service and rules may need updating in the event of a DR scenario or proxy failure.

See also:

- *Manage Phone Services*

26.4.3. Manage Phone Services

Note: This feature will only be available once correctly configured in VOSS-4-UC as well as the associated Unified CM (see *Phone Services Feature Setup*).

After initial configuration, an end user will be able to manage the following phone services directly from the phone (if configured in VOSS-4-UC):

- Speed Dials
- Call Forward - View Call Forward Settings, Set Call Fwd All(CFA), Set Call Fwd Busy(CFB), Set Call Forward NoAnswer(CFNA)
- Corporate Directory

Manage (add, edit or delete) a service directly from the Telephone User Interface (TUI).

The services all work in a similar way as shown in the following example with speed dials:

1. Select **Services > Speed Dial**.
2. Click **Manage**.
3. Click **Add**, **Edit** or **Delete** and follow the prompts.
4. Click **Submit** to initiate the transaction (only relevant to **Add** and **Edit**).

See also:

- *Introduction to Phone Services*
- *Phone Services Feature Setup*

Index